Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

SEMANA 1: LÓGICA

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

1. Lógica

La lógica le proporciona a las matemáticas un lenguaje claro y un método preciso para demostrar teoremas a partir de axiomas. Por ejemplo:

axiomas de Euclides, definiciones, nociones primarias de geometría clásica
$+$
lógica
$=$
teoremas 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.
Sin la lógica los axiomas serían un montón de verdades aceptadas, pero nada más. La lógica, sin embargo, les da sentido y permite concluir nueva verdades (teoremas) que antes no conocíamos. Un ejemplo de teorema: la suma de los ángulos interiores de cualquier triángulo siempre es de 180°.
Al ser la lógica el punto de partida de las matemáticas, en ella se deben introducir nociones primarias tales como proposición, valor de verdad, conectivo lógico.

1.1. Proposiciones y valor de verdad

Definición 1.1 (Proposición lógica). *Una proposición debe interpretarse como un enunciado que siempre toma uno de los valores de verdad posibles: verdadero (V) o falso (F).*

Por ejemplo, en el contexto de la aritmética, "2+1=5" corresponde efectivamente a una proposición. Más aún, su valor de verdad es F.
Típicamente notaremos a las proposiciones con letras minúsculas: p, q, r, etc.

Algunos ejemplos:

- "Estoy estudiando ingeniería".
- "$1 \geq 0$".
- "Está lloviendo en Valdivia".

1.2. Conectivos lógicos

Los conectivos lógicos sirven para construir nuevas proposiciones a partir de proposiciones ya conocidas. El valor de verdad de la nueva proposición dependerá del valor de verdad de las proposiciones que la forman. Esta dependencia se explicita a través de una tabla de verdad.

Definición 1.2 (Negación). *La proposición $\overline{p}$ se lee "no p" y es aquella cuyo valor de verdad es siempre distinto al de p. Por ejemplo, la negación de "mi hermano ya cumplió quince años" es "mi hermano aún no cumple quince años". Esto se explicita a través de la siguiente tabla de verdad.*

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

Definición 1.3 (O lógico o disyunción). *La proposición $p \vee q$ se lee "p o q". Decimos que $p \vee q$ es verdad, o que "se tiene $p \vee q$", cuando al menos una de las dos proposiciones, o bien p o bien q, es verdadera. Por ejemplo, la proposición "mañana lloverá o mañana no lloverá" es verdadera. En otras palabras, tal como se aprecia en la siguiente tabla de verdad, si alguien afirma que se tiene $p \vee q$ lo que nos está diciendo es que nunca son simultáneamente falsas.*

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

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 alguien afirma que se tiene $p \wedge q$, lo que nos 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). *Todos estaremos de acuerdo en considerar verdadera la proposición "si el señor K está en California entonces el señor K está en Estados Unidos". ¿Por qué?*
Porque a uno no le importa dónde está el señor K: podría estar en Texas o en China. **Lo único importante** *es que, si efectivamente "está en Californa", entonces podemos concluir, con esa sola información, que "está en Estados Unidos".*
La proposición $p \Rightarrow q$ se lee "p implica q" o "si p entonces q". Para estudiar su valor de verdad nos debemos concentrar en el caso de que la hipótesis p sea verdadera. Ahí tenemos que determinar si basta con esa información para concluir que q es verdadera. En resumen: si alguien afirma que se tiene $p \Rightarrow q$, debemos concluir que si p es verdad entonces **necesariamente** *q será verdad. Todo esto se explicita a través de la siguiente tabla.*

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

Definición 1.6 (Equivalencia). *Decimos que la proposición p es equivalente con la proposición q (o que "p si y sólo si q"), y escribimos $p \iff q$, cuando basta con conocer el valor de verdad de una para saber el valor de verdad de la otra ya que éste siempre es el mismo.*
Por ejemplo "el paralelógramo dibujado en la pared tiene todos sus ángulos iguales" es equivalente con la proposición "las diagonales del paralelógramo dibujado en la pared miden lo mismo". O bien ambas son verdaderas o bien ambas son falsas.

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

1.3. Tautologías

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

Tres ejemplos bastante razonables:

Ejemplos:

$$p \vee \overline{p}$$
$$p \Rightarrow p \vee q$$
$$(p \iff q) \iff (q \iff p)$$

Demostraremos, desarrollando una tabla de verdad, que la primera proposición es tautología.

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

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 análogo a lo que hacemos cuando reemplazamos el término $(x - x)$ por el símbolo 0.

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

Por ejemplo, $p \wedge \overline{p}$. Son todas equivalentes a la proposición F.
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 demostrar la condición de tautología de algunas de ellas usando tablas de verdad, como ejercicio.

Proposición 1.1 (Tautologías importantes).

1. $(p \wedge \overline{p}) \iff F \quad (p \wedge V) \iff p \quad (p \wedge F) \iff F$
   $(p \vee \overline{p}) \iff V \quad (p \vee V) \iff V \quad (p \vee F) \iff p$
2. *Caracterización de la implicancia.* $(p \Rightarrow q) \iff (\overline{p} \vee q)$
3. *Leyes de De Morgan.*
   a. $\overline{(p \wedge q)} \iff (\overline{p} \vee \overline{q})$
   b. $\overline{(p \vee q)} \iff (\overline{p} \wedge \overline{q})$

4. *Doble negación.* $\overline{\overline{p}} \iff p$

5. *Conmutatividad.*

   5.1. $(p \vee q) \iff (q \vee p)$
   5.2. $(p \wedge q) \iff (q \wedge p)$

6. *Asociatividad.*

   6.1. $(p \vee (q \vee r)) \iff ((p \vee q) \vee r)$
   6.2. $(p \wedge (q \wedge r)) \iff ((p \wedge q) \wedge r)$

7. *Distributividad.*

   7.1. $(p \wedge (q \vee r)) \iff ((p \wedge q) \vee (p \wedge r))$
   7.2. $(p \vee (q \wedge r)) \iff ((p \vee q) \wedge (p \vee r))$
   7.3. $((q \vee r) \wedge p) \iff ((q \wedge p) \vee (r \wedge p))$
   7.4. $((q \wedge r) \vee p) \iff ((q \vee p) \wedge (r \vee p))$

Cuatro tautologías muy importantes

Estas cuatro tautologías se prueban *usando tablas de verdad*. Son particularmente útiles para demostrar teoremas.
Cada una de ellas da lugar a una técnica de demostración: equivalencia dividida en dos partes, transitividad, contrarrecíproca, reducción al absurdo. En las partes que siguen ilustraremos el uso de estas técnicas. Verás este símbolo cada vez que lo hagamos.

Proposición 1.2.

1. *Equivalencia dividida en dos partes.* $(p \iff q) \iff (p \Rightarrow q \wedge q \Rightarrow p)$

2. *Transitividad.* $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$

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

4. *Reducción al absurdo.* $\overline{(p \Rightarrow q)} \iff (p \wedge \overline{q})$

Verificación simbólica y exploratoria

Cuando queremos verificar de manera simbólica que cierta proposición es tautología evitaremos usar tablas de verdad y sólo nos permitiremos usar (como conocidas) las tautologías básicas que aparecen en las secciones anteriores. Demostremos de manera simbólica entonces que:

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

En efecto:

$$\begin{aligned}
(p \iff q) &\iff (p \Rightarrow q) \wedge (q \Rightarrow p) \\
&\iff (\overline{p} \vee q) \wedge (\overline{q} \vee p) \\
&\iff [(\overline{p} \vee q) \wedge \overline{q}] \vee [(\overline{p} \vee q) \wedge p] \\
&\iff [(\overline{p} \wedge \overline{q}) \vee (q \wedge \overline{q})] \vee [(\overline{p} \wedge p) \vee (q \wedge p)] \\
&\iff [(\overline{p} \wedge \overline{q}) \vee F] \vee [F \vee (q \wedge p)] \\
&\iff (\overline{p} \wedge \overline{q}) \vee (p \wedge q)
\end{aligned}$$

En las demostraciones exploratorias se acepta "explorar" la tabla de verdad deshechando los casos "fáciles". 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. **Lo que debemos hacer** es concluir que $(p \Rightarrow \overline{r})$ es verdadera.

Caso 1. p es falsa. Este caso es fácil: obviamente se tiene que $(p \Rightarrow \overline{r})$ es verdadera.

Caso 2. p es verdadera. Como asumimos que $(p \Rightarrow \overline{q})$ es verdadera, se tiene que tener q 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.

1.4. Función proposicional y cuantificadores

Definición 1.9 (Función proposicional). *Una función proposicional p es una expresión descrita en función de algún parámetro x que satisface lo siguiente: cada vez que x* **se reemplaza** *por una cadena de símbolos, $p(x)$ se transforma en una proposición.*

Ejemplos:

- $p(x)$ = "x es un jugador de fútbol" es una función proposicional. Notar que $p($`Marcelo Salas`$)$ es verdadera mientras que $p($`Nicolás Massu`$)$ es falsa.
- $q(x)$ = "$x-5 \leq 0$", también es una función proposicional. $q(2)$ es verdadera, pero $q(6)$ es falsa.

Observación: En adelante, usaremos $p(x)$ de dos formas distintas:

- Para referirnos a la función proposicional misma y mostrar que x es la variable que reemplazamos por cadenas de símbolos para obtener proposiciones lógicas.
- Para referirnos, cuando x es algo en particular, a la proposición que se forma de haber hecho el reemplazo en la función proposicional.

Cuantificador universal

Definición 1.10 (Cuantificador universal). *La proposición $(\forall x)p(x)$, que se lee "para todo x $p(x)$", es verdadera siempre y cuando $p(x)$ sea verdadera para cualquier cadena de símbolos que se reemplace en x.*

Veamos un ejemplo:

Ejemplo:

- Usando el ejemplo anterior, $p(x)$ = "x es un jugador de fútbol", ¿será verdadera $(\forall x)p(x)$.

  Claramente, como vimos que $p($`Nicolás Massu`$)$ es falsa, no es cierto que al reemplazar x por cualquier cadena de símbolos lo resultante sea una proposición verdadera.

  Luego $(\forall x)p(x)$ es falsa.

A continuación veamos ejemplos de proposiciones construidas usando el cuantificador universal y cómo se verifica la veracidad de dichas proposiciones.

Ejemplo:

- $(\forall x)(p(x) \vee \overline{p(x)})$ es verdadera. Verifiquemos que es verdadera, por pasos.

  Sea x arbitrario (este es el modo en que se considera el "$\forall x$").

  p.d.q (por demostrar que): $p(x) \vee \overline{p(x)}$ es verdadera.

  En efecto:

  Caso 1. $p(x)$ es verdadera. Como $V \vee \overline{p(x)}$ es verdadera, se concluye.

  Caso 2. $p(x)$ es falsa. En este caso $\overline{p(x)}$ es verdadera. Como $(F \vee V) \iff V$, se concluye.

- $(\forall x)[p(x) \Rightarrow (p(x) \vee q(x))]$ es verdadera. Demostrémoslo.

  Sea x arbitrario

  Hipótesis: $p(x)$ es verdadera.

  p.d.q: $p(x) \vee q(x)$ es verdadera.

  En efecto: como $p(x)$ es verdadera, usamos que $V \vee q(x)$ es verdadera para concluir.

- $[(\forall x)p(x) \vee (\forall x)q(x)] \Rightarrow [(\forall x)(p(x) \vee q(x)]$ es verdadera.

  Hipótesis: $(\forall x)p(x) \vee (\forall x)q(x)$ es verdadera

  p.d.q: $(\forall x)(p(x) \vee q(x))$ es verdadera

  En efecto: sea x arbitrario.

  Caso 1. $p(x)$ es verdadera. En este caso $(p(x) \vee q(x))$ es verdadera.

  Caso 2. $p(x)$ es falsa. En este caso, por hipótesis, $q(x)$ **tiene que ser verdadera**. Se deduce que $(p(x) \vee q(x))$ es verdadera.

Cuantificador existencial

Definición 1.11 (Cuantificador existencial). *La proposición $(\exists x)p(x)$, que se lee "existe x, tal que $p(x)$", es verdadera cuando se puede encontrar por lo menos una cadena de símbolos que hace $p(x)$ verdadero.*

Ejemplo:

- Retomando el ejemplo anterior, con $p(x) =$ "x es un jugador de fútbol". ¿Se tendrá que $(\exists x)p(x)$?.

  Tenemos que hay al menos un x que hace a $p(x)$ verdadera, por ejemplo $x =$ `Matías Fernández` cumple claramente que $p($`Matías Fernández`$)$ es verdadera.

  Así, $(\exists x)p(x)$ es verdadera.

Relación entre cuantificadores

A continuación veremos la relación que existe entre los dos cuantificadores antes definidos. Dicha relación se debe a la negación.

Resulta que $(\exists x)p(x)$ es falsa si y sólo si $\overline{p(x)}$ no es verdadera para ninguna cadena de símbolos x, es decir, si y sólo si $(\forall x)\overline{p(x)}$ es verdadera. Así, hemos hallado la

Proposición 1.3 (Negación del cuantificador existencial). *La siguiente proposición es una tautología*

$$\overline{(\exists x)p(x)} \iff (\forall x)\overline{p(x)}.$$

Existencia y unicidad

Hay un cuantificador más que se utiliza con frecuencia:

Definición 1.12 (Existencia y unicidad). *La proposición $(\exists! x)p(x)$, que se lee "existe un único x tal que $p(x)$", es verdadera cuando hay exactamente una cadena de símbolos hace verdadero $p(x)$.*

Un ejemplo:

Ejemplo:

Nuevamente, considerando nuestra función proposicional $p(x) =$ "x es un jugador de fútbol". ¿Cuál será el valor de verdad de $(\exists! x)p(x)$?

Podemos notar que tanto $x_1 =$ `Marcelo Salas` y $x_2 =$ `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, $(\exists! x)p(x)$ es falsa.

Observación: Notemos que $\exists!$ **no** es un cuantificador nuevo, en el sentido de que puede ser definido en función de los dos cuantificadores anteriores. Es decir la siguiente proposición es verdadera.

$$(\exists! x)p(x) \iff \underbrace{[(\exists x)p(x)]}_{\text{Existencia}} \wedge \underbrace{[(\forall x)(\forall y)((p(x) \wedge p(y)) \Rightarrow (x = y))]}_{\text{Unicidad}}$$

Ejemplo importante: Equivalencia dividida en dos partes

Veremos ahora una técnica de demostración que se basa en una de las tautologías importantes que vimos antes. Supongamos que queremos demostrar que

$$\underbrace{(\forall x)(p(x) \wedge q(x))}_{p} \iff \underbrace{[(\forall x)p(x) \wedge (\forall x)q(x)]}_{q}$$

es verdadera.
Lo que haremos es usar la Tautología 1,

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

En donde el rol de p y q está descrito arriba. Ésta nos permite dividir la demostración en dos partes, ya que en lugar de verificar que $(p \iff q)$ es verdadera, podemos verificar que $(p \Rightarrow q) \wedge (q \Rightarrow p)$ es verdadera.
Esto, a su vez lo hacemos verificando que $(p \Rightarrow q)$ es verdadera y luego que $(q \Rightarrow p)$ también lo es.
$\Rightarrow$)
Hipótesis: $(\forall x)(p(x) \wedge q(x))$ es verdadera.
p.d.q: $(\forall x)p(x) \wedge (\forall x)q(x)$ es verdadera.

En efecto: **Sea** x **arbitrario**. Por hipótesis se tiene tanto $p(x)$ como $q(x)$ son verdaderas. En particular $p(x)$ lo es. Es decir, probamos que $(\forall x)p(x)$ es verdadera. Análogamente se tiene que también $(\forall x)q(x)$ es verdadera.
$\Leftarrow$)
Hipótesis: $(\forall x)p(x) \wedge (\forall x)q(x)$ es verdadera.
p.d.q: $(\forall x)(p(x) \wedge q(x))$ es verdadera.

En efecto: **Sea** x_0 **arbitrario**. Como por hipótesis $(\forall x)p(x))$ es verdadera **se tiene que** $p(x_0)$ **es verdadera**. Como por hipótesis $(\forall x)q(x)$ es verdadera **se tiene** $q(x_0)$ también lo es. □

Observación: Convenciones en el desarrollo de un argumento En la demostración anterior la expresión "... es verdadera ..." aparece una gran cantidad de veces. Por ejemplo en

> Hipótesis: $(\forall x)(p(x) \wedge q(x))$ es verdadera.
> p.d.q: $(\forall x)p(x) \wedge (\forall x)q(x)$ es verdadera.

Esto no siempre es necesario pues se subentiende que al decir que la hipótesis es p estamos asumiendo que p es verdadera.
Del mismo modo, si declaramos que queremos demostrar q se subentiende que deseamos demostrar que q es verdadera.
También es posible que después de un razonamiento lleguemos a la conclusión que r es verdadera. Esto suele indicarse con expresiones del tipo "se tiene r" o "y entonces r".

Tomando estas convenciones la última parte del desarrollo anterior queda como sigue.

> Hipótesis: $(\forall x)p(x) \wedge (\forall x)q(x)$
> p.d.q: $(\forall x)(p(x) \wedge q(x))$

En efecto: **Sea** x_0 **arbitrario**. Como por hipótesis $(\forall x)p(x)$, **se tiene** $p(x_0)$. Como por hipótesis $(\forall x)q(x)$, **se tiene** $q(x_0)$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ "25-11" no corresponde a una proposición lógica.

2. ☐ "¿Podrás venir ma nana?" 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 $\bar{p}$ es siempre distinto al de p.

6. ☐ Existen proposiciones lógicas p tales que $\bar{p}$ 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 simultáneamente 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. ☐ Si una proposición compuesta es *tautología*, 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 $p \Rightarrow p$.

16. ☐ El valor de verdad de la proposición $p \vee \bar{p}$ es siempre el mismo, sin importar el valor de verdad de p.

17. ☐ Existe un valor de verdad para p, tal que la proposición $p \vee \bar{p}$ es falsa.

18. ☐ El valor de verdad de la proposición $(p \wedge \bar{q}) \vee (p \Rightarrow q)$ puede ser falso.

19. ☐ La negación de la proposición $p \vee \bar{q}$ es $\bar{p} \vee q$.

20. ☐ La negación de la proposición $p \vee \bar{q}$ es $\bar{p} \wedge q$.

21. ☐ La negación de la proposición $p \vee q$ es $\bar{p} \vee \bar{q}$.

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 $p \Rightarrow F$ es siempre falsa.

29. ☐ La proposición $p \Rightarrow \bar{p}$ es siempre falsa.

30. ☐ La proposición $p \Rightarrow q$ es siempre verdadera si el valor de verdad de p es falso.

31. ☐ Si la proposición $p \Rightarrow q$ es verdadera y p también lo es, necesariamente q es verdadera.

32. ☐ Si la proposición $p \Rightarrow (q \Rightarrow r)$ es verdadera y p también lo es, necesariamente r es verdadera.

33. ☐ Si la proposición $(p \Rightarrow q) \Rightarrow r$ es falsa y p es verdadera, necesariamente q es verdadera.

34. ☐ La proposición $p \Leftrightarrow V$ tiene siempre el mismo valor de verdad que p.

35. ☐ La proposición $p \Leftrightarrow F$ es equivalente a la proposición $\bar{p} \vee F$.

36. ☐ La proposición $(p \Leftrightarrow q) \Rightarrow (p \Rightarrow q)$ es una tautología.

37. ☐ Si la proposición $((r \Rightarrow p) \wedge (p \Rightarrow q))$ es verdadera, la proposición $r \Rightarrow q$ también lo es.

38. ☐ La proposición $((\bar{q} \Rightarrow \bar{p}) \wedge (q \Rightarrow r)) \Rightarrow (\bar{r} \Rightarrow \bar{p})$ es una tautología.

39. ☐ La proposición $\overline{(p \Rightarrow q)} \Leftrightarrow (\bar{p} \Rightarrow \bar{q})$ es tautología.

40. ☐ La negación de la proposición $p \Rightarrow q$ es $(p \wedge \bar{q})$.

41. ☐ La negación de la proposición $p \Rightarrow \bar{q}$ es $\bar{p} \Rightarrow q$.

42. ☐ La proposición cuantificada $(\forall x)p(x)$ es verdadera si $p(x)$ es verdadera para cualquier elemento por el que se reemplace x.

43. ☐ Si la proposición $(\forall x)p(x)$ es verdadera, entonces la proposición $(\exists x)p(x)$ es también verdadera.

44. ☐ Si $q(x)$ es una función proposicional y x_0 es tal que $q(x_0)$ es verdadera, entonces la proposición cuantificada $(\exists x)q(x)$ es verdadera.

45. ☐ Es siempre cierto que si la proposición $(\exists x)p(x)$ es verdadera, entonces la proposición $(\exists! x)p(x)$ es verdadera.

46. ☐ Si $p(x)$ es una función proposicional y x_0 es tal que $p(x_0)$ es falsa, entonces la proposición cuantificada $(\forall x)p(x)$ es falsa.

47. ☐ Si las proposiciones $(\forall x)p(x)$ y $(\forall x)q(x)$ son verdaderas, entonces la proposición $(\forall x)(p(x) \wedge q(x))$ es verdadera.

48. ☐ Si la proposición $(\forall x)(p(x) \vee q(x))$ es verdadera, entonces la proposición $(\forall x)p(x) \vee (\forall x)q(x)$ es verdadera.

49. ☐ Si la proposición $(\forall x)p(x) \vee (\forall x)q(x)$ es verdadera, entonces la proposición $(\forall x)(p(x) \vee q(x))$ es verdadera.

50. ☐ La negación de la proposición $(\exists!)p(x)$ es $((\forall x)\overline{p(x)}) \vee ((\exists x)(\exists y)(x \neq y \Rightarrow (\overline{p(x)} \vee \overline{p(y)}))$.

Guía de Ejercicios

1. Demuestre usando tablas de verdad que las siguientes proposiciones vistas en la tutoría, son tautologías:

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

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

(a) $p \vee q$
(b) $p \wedge (q \vee \overline{r})$
(c) $((p \wedge q) \Rightarrow r) \Leftrightarrow (\overline{r} \wedge q)$
(d) $\overline{(\overline{p} \wedge q)} \wedge \overline{(p \vee \overline{r})}$

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

(a) $\overline{p}$
(b) $p \vee q$
(c) $p \wedge q$
(d) $p \Rightarrow q$

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

(a) $p \Rightarrow (p \vee q)$
(b) $(p \Leftrightarrow q) \Leftrightarrow (p \wedge q) \vee (\overline{p} \wedge \overline{q})$
(c) $[(p \Leftrightarrow q) \wedge (q \Leftrightarrow r)] \Rightarrow (p \Leftrightarrow r)$
(d) $\overline{(p \Leftrightarrow q)} \Leftrightarrow (\overline{p} \Leftrightarrow q)$
(e) $[p \wedge \overline{q} \Rightarrow \overline{p}] \Rightarrow (p \Rightarrow q)$

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

(a) $[(p \Rightarrow \overline{q}) \wedge (\overline{r} \vee q) \wedge r] \Rightarrow \overline{p}$
(b) $[p \wedge (p \Rightarrow q)] \Rightarrow q$
(c) $[(p \wedge \overline{q}) \Rightarrow \overline{p}] \Rightarrow (p \Rightarrow q)$
(d) $(p \wedge q \Rightarrow r) \Leftrightarrow (p \wedge \overline{r} \Rightarrow \overline{q})$
(e) $(p \wedge q) \Leftrightarrow [(p \vee q) \wedge (p \Leftrightarrow q)]$

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

(a) $r \Rightarrow q$ es falsa.
(b) $q \Rightarrow \overline{r}$ es falsa.

(c) $p \Rightarrow (q \vee \overline{r})$ es falsa.

(d) $\overline{r} \Leftrightarrow q$ es verdadera y $(p \wedge q) \Rightarrow s$ es falsa

(e) $(r \Rightarrow p) \Rightarrow (p \wedge \overline{q})$ es verdadera y q es verdadera.

7. Sean $p(x), q(x)$ funciones proposicionales. Determinar la negación de las siguientes proposiciones cuantificadas:

(a) $(\exists x)(\forall y)(p(x) \wedge q(y))$

(b) $(\forall x)(\forall y)(p(x) \Rightarrow \overline{q(y)})$

(c) $(\exists! x)p(x)$

(d) $(\forall x)[q(x) \Rightarrow (\exists y)p(y)]$

(e) $(\exists x)(\exists y)(p(x) \Leftrightarrow q(y))$

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. 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.) $(p \vee q \;\Leftrightarrow\; p \wedge r) \Rightarrow ((q \Rightarrow p) \wedge (p \Rightarrow r))$.

(b) (20 min.) $(p \Rightarrow \overline{q}) \wedge (r \Rightarrow q) \;\Rightarrow\; (p \Rightarrow \overline{r})$.

(c) (20 min.) $(p \Rightarrow q) \Rightarrow [\overline{(q \wedge r)} \Rightarrow \overline{(p \wedge r)}]$.

(d) (20 min.) $[(p \Rightarrow \overline{q}) \wedge (\overline{r} \vee q) \wedge r] \Rightarrow \overline{p}$.

P2. 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 $p \vee (q \wedge r) \Leftrightarrow (p \vee r) \wedge q$ puede ser verdadera sin que lo sea la implicancia $p \Rightarrow q$. Es decir, use la información de la hipótesis para sacar conclusiones de los valores de verdad de las proposiciones involucradas.

(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.

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

(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 $(r \Leftrightarrow s)$].

Demuestre que el valor de verdad de la proposición:

$$[(p \wedge r) \vee (q \Rightarrow s)] \Rightarrow [p \vee (r \wedge s)]$$

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

P3. Sean las proposiciones r y s siguientes:

$r:\ (\forall x)(p(x) \Rightarrow q)$

$s:\ ((\forall x)p(x)) \Rightarrow q$

Piense en qué dice cada una en términos intuitivos y cuál es la diferencia entre ambas.

(a) (10 min.) Niegue ambas proposiciones, r y s.

(b) (20 min.) De las dos implicancias, $(r \Rightarrow s)$ y $(s \Rightarrow r)$ determine la que corresponde a una tautología. Justifique su elección.

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

2. Conjuntos

2.1. Introducción

La teoría de conjuntos gira en torno a la función proposicional $x \in A$. Los valores que hacen verdadera la función proposicional $x \in A$ son aquellos **elementos** que forman el **conjunto** A.
La función proposicional "$x \in A$" se lee "x pertenece a A". Su negación, que se denota $x \notin A$, se lee "x no pertenece a A".

Ejemplo:

Si queremos que el conjunto A sea el de los números primos menores que 10 entonces tendríamos que definirlo formalmente así:

$$(\forall x)[(x \in A) \iff (x = 2 \vee x = 3 \vee x = 5 \vee x = 7)].$$

Los conjuntos finitos son fáciles de definir. De hecho, acabamos de mostrar cómo se define el conjunto que se se denota por extensión $A = \{2, 3, 5, 7\}$.
La axiomática de la teoría de conjuntos (que aquí no se estudiará) permite asumir la existencia de un conjunto infinito muy importante: el de los naturales $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Algunos ejemplos de conjuntos

En matemáticas se construyen nuevos conjuntos a partir de conjuntos ya conocidos. Supongamos que ya conocemos el conjunto A. Podemos introducir, $B = \{x \in A | p(x)\}$. Lo que en el fondo estamos definiendo es la función proposicional $x \in B$ así:

$$(\forall x)[(x \in B) \iff (x \in A \wedge p(x))]$$

Por ejemplo, el conjunto de múltiplos de 7 es el conjunto $\{x \in \mathbb{N} | (\frac{x}{7}) \in \mathbb{N}\}$.

Otros ejemplos de conjuntos, con los cuales el lector ya debe estar familiarizado:

Ejemplos:

1. Los reales $\mathbb{R}$.
2. Los enteros $\mathbb{Z}$.
3. Los racionales $\mathbb{Q} = \{x \in \mathbb{R} \mid (\exists p)(\exists q)(p \in \mathbb{Z} \wedge q \in \mathbb{Z} \wedge \ q \neq 0 \wedge x = \frac{p}{q})\}$.
4. Los irracionales $\mathbb{Q}^c = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.
5. Los naturales $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.
6. Los enteros positivos $\mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$

2.2. El conjunto vacío

Definimos ahora el conjunto vacío, el cual notamos ϕ, del siguiente modo:

Definición 2.1 (Conjunto vacío).

$$\phi = \{x \in \mathbb{N} | x \neq x\}.$$

Notar que ϕ no tiene ningún elemento. Es decir $(\forall x)(x \notin \phi)$.

En efecto, sea x arbitrario.

$$(x \in \phi) \iff ((x \in \mathbb{N}) \wedge (x \neq x)) \iff ((x \in \mathbb{N}) \wedge F) \iff F$$

2.3. Igualdad e inclusión

Sean A y B conjuntos. Definimos la igualdad y la inclusión como sigue.

Definición 2.2 (Igualdad e inclusión).

$$A = B \iff (\forall x)(x \in A \iff x \in B)$$
$$A \subseteq B \iff (\forall x)(x \in A \Rightarrow x \in B)$$

Una primera propiedad que probaremos es:

Proposición 2.1. *Sean A y B conjuntos. Se tiene que:*

$$A = B \iff A \subseteq B \wedge B \subseteq A$$

Demostración. Vamos a usar la identidad lógica ya demostrada anteriormente: $(\forall x)(p(x) \wedge q(x)) \iff [(\forall x)p(x)) \wedge (\forall x)p(x)]$.

$$\begin{array}{lll} A = B & \iff & (\forall x)(x \in A \iff x \in B) \\ & \iff & (\forall x)[(x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)] \\ & \iff & (\forall x)(x \in A \Rightarrow x \in B) \wedge (\forall x)(x \in B \Rightarrow x \in A) \\ & \iff & A \subseteq B \wedge B \subseteq A \end{array}$$

Otras propiedades importantes:

Proposición 2.2. *Sean A, B, C conjuntos arbitrarios. Se tiene:*

1. $A = A$
2. $A = B \iff B = A$
3. $(A = B \wedge B = C) \Rightarrow A = C$

4. $A \subseteq A$

5. $(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B$

6. $(A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$

7. $\phi \subseteq A$

DEMOSTRACIÓN. Demostraremos sólo la propiedad 6.
Hipótesis:
(a) $(\forall x)(x \in A \Rightarrow x \in B)$
(b) $(\forall x)(x \in B \Rightarrow x \in C)$

p.d.q: $(\forall x)(x \in A \Rightarrow x \in C)$

En efecto: Sea x arbitrario. Asumamos que $x \in A$. Por (a) se tiene que $x \in B$. Por (b) se tiene que $x \in C$.

2.4. Unión de conjuntos

Operando conjuntos conocidos se pueden definir nuevos conjuntos.Sean A y B conjuntos.
La unión de A con B, que se denota $A \cup B$, es el conjunto que reúne a los elementos que están en A con aquellos que están en B. Formalmente:

Definición 2.3 (Unión).

$$(\forall x)[(x \in A \cup B) \iff (x \in A \vee x \in B)]$$

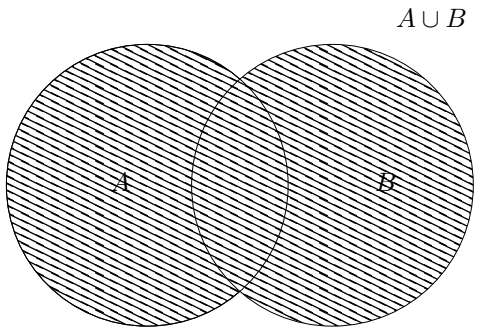

Figura 1: Diagrama de Venn, representando la unión entre A y B (área achurada).

Observación: Diagramas de Venn Un *Diagrama de Venn*, como el presentado en la diapositiva anterior, es una ilustración que muestra la relación matemática o lógica entre conjuntos.
Fueron introducidos por el filósofo y matemático británico John Venn (1834-1923) el año 1881.
Los diagramas de Venn 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).

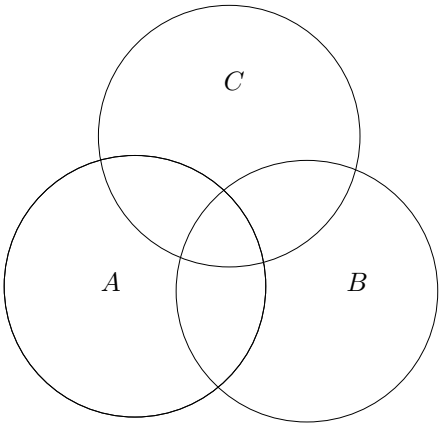

Figura 2: Diagrama de Venn para tres conjuntos.

2.5. Intersección de conjuntos

La intersección de A con B, que se denota $A \cap B$, es el conjunto formado por los elementos que están tanto en A como en B. Formalmente:

Definición 2.4. *Intersección*

$$(\forall x)[(x \in A \cap B) \iff (x \in A \wedge x \in B)]$$

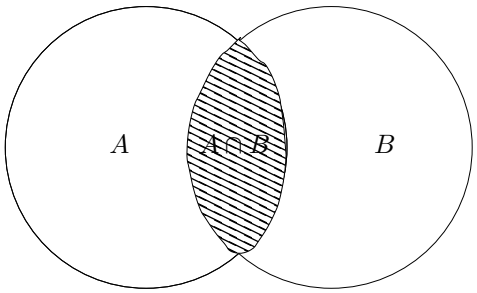

Figura 3: Diagrama de Venn, representando la intersección entre A y B (área achurada).

Una primera propiedad:

Proposición 2.3. *Sean A, B conjuntos tales que $A \subseteq B$. Entonces $A \cup B = B$ y $A \cap B = A$.*

Demostración. Probaremos sólo la primera.
$\subseteq$)
Sea x arbitrario tal que $x \in A \cup B$. Es decir,
Hipótesis: $x \in A \vee x \in B$.

p.d.q: $x \in B$
En efecto:

Caso 1. $x \in A$. Como $A \subseteq B$ se tiene que $x \in B$.
Caso 2. $x \notin A$. Por hipótesis se tiene que tener $x \in B$.
$\supseteq$)
Sea x arbitrario tal que $x \in B$. Obviamente $x \in A \cup B$.

Proposición 2.4. *Sean A, B, C conjuntos, se tiene:*

1. *Conmutatividades*
   - **1.1** $A \cup B = B \cup A$.
   - **1.2** $A \cap B = B \cap A$.
2. *Asociatividades*
   - **2.1** $A \cup (B \cup C) = (A \cup B) \cup C$.
   - **2.2** $A \cap (B \cap C) = (A \cap B) \cap C$.
3. *Distributividades*
   - **3.1** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
   - **3.2** $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
4. **4.1** $A \cap B \subseteq A \subseteq A \cup B$.
   4.2 $A \cap B \subseteq B \subseteq A \cup B$.

Demostración. Notar que las propiedades (1), (2) y (3), son consecuencias directas de las propiedades análogas para $\wedge$ y $\vee$. Queda como ejercicio realizar dichas demostraciones.

2.6. Conjunto universo

Asumiremos la existencia de un universo (conjunto referencia) U en el que viven todos los elementos con los que se va a trabajar. Es decir, U es tal que la proposición $a \in U$ es siempre verdadera.

Con esto, podemos concluir de lo anterior el siguiente:

Corolario 2.1. *Sean A, B conjuntos y sea U el conjunto universo.*

1. $A \cup A = A$
2. $A \cap A = A$
3. $A \cup \phi = A$
4. $A \cap \phi = \phi$
5. $A \cup U = U$
6. $A \cap U = A$

Demostración.
- Como $A \subseteq A$ se tiene que $A \cup A = A$ y que $A \cap A = A$.
- Como $\phi \subseteq A$ se tiene que $\phi \cup A = A$ y que $\phi \cap A = \phi$.
- Como $A \subseteq U$ se tiene que $A \cup U = U$ y que $A \cap U = A$.

Observación: El conjunto universo es un conjunto de **referencia**, es decir habrá veces que tomaremos $U = \mathbb{R}$, u otras $U = \mathbb{Z}$, etc.

2.7. Diferencia y complemento

Supongamos que tenemos un conjunto de referencia U (conjunto universo). Queremos definir el complemento de un conjunto A, que notaremos A^c, como aquel formado por todos los elementos que no están en A. Formalmente:

Definición 2.5 (Conjunto complemento).

$$(\forall x)(x \in A^c \iff x \in U \wedge x \notin A)$$

O sea, $(\forall x)(x \in A^c \iff x \notin A)$.

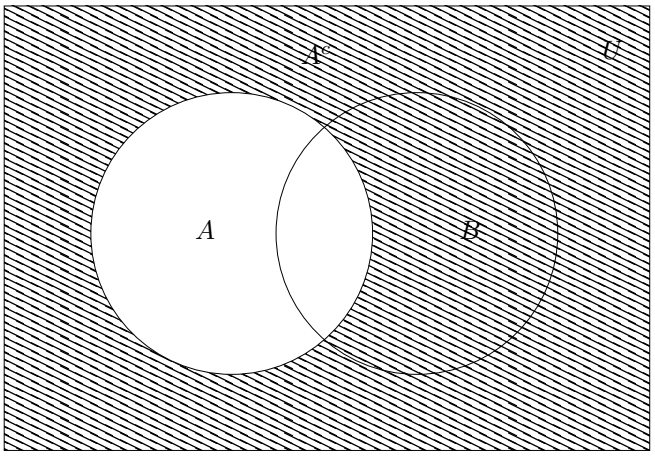

Figura 4: Diagrama de Venn, representando el complemento de A (área achurada).

Ejemplo:

Si viviésemos en el mundo de los números enteros $\mathbb{Z}$ (conjunto universo) entonces consideremos $A = \{x \in \mathbb{Z} |\ x \text{ es par}\}$.
Obviamente $A^c = \{x \in \mathbb{Z} |\ x \text{ es impar}\}$.

Definimos además la diferencia entre A y B, que notamos $A \setminus B$, como el conjunto formado por los elementos que están en A y que no están en B. Formalmente:

Definición 2.6 (Diferencia).

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

Algunas propiedades:

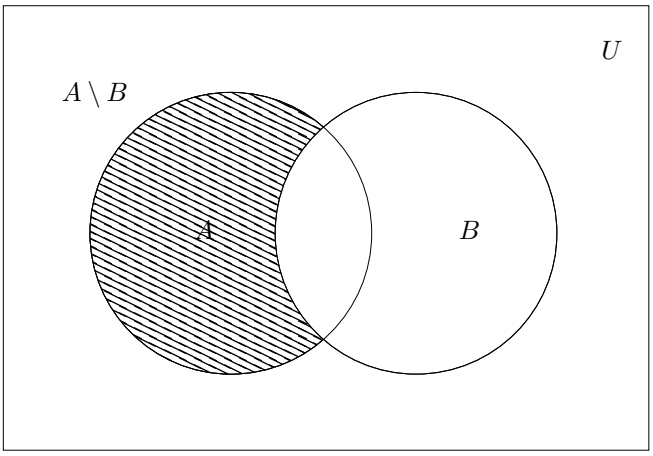

Figura 5: Diagrama de Venn, representando la diferencia entre A y B (área achurada).

Proposición 2.5. *Sean A y B conjuntos.*

1. *Leyes de De Morgan*
   - **1.1.** $(A \cup B)^c = A^c \cap B^c$
   - **1.2.** $(A \cap B)^c = A^c \cup B^c$
2. $(A \subseteq B) \iff (B^c \subseteq A^c)$
3. $(A^c)^c = A$
4. $A \cup A^c = U$
5. $A \cap A^c = \phi$

Demostración. Demostraremos la primera. Sea x arbitrario.

$$\begin{array}{lcl} x \in (A \cup B)^c & \iff & \overline{x \in (A \cup B)} \\ & \iff & \overline{(x \in A) \vee (x \in B)} \\ & \iff & \overline{(x \in A)} \wedge \overline{(x \in B)} \\ & \iff & (x \in A^c) \wedge (x \in B^c) \\ & \iff & x \in (A^c \cap B^c) \end{array}$$

2.8. 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 en A pero no en B, o bien en B pero no en A.

Formalmente:

Definición 2.7. Diferencia simétrica

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

Obviamente, algunas propiedades:

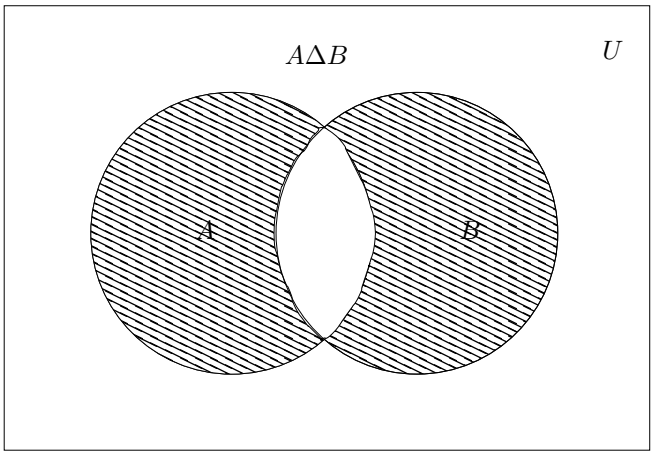

Figura 6: Diagrama de Venn, representando la diferencia simétrica entre A y B (área achurada).

Proposición 2.6. *Sean A, B, C conjuntos.*

1. $A\Delta B = (A \cup B) \setminus (A \cap B)$
2. $A\Delta B = B\Delta A$
3. $(A\Delta B)\Delta C = A\Delta(B\Delta C)$
4. $A\Delta A = \phi$
5. $A\Delta\phi = A$
6. $(A \cap (B\Delta C)) = (A \cap B)\Delta(A \cap C)$

Demostración. Demostraremos la primera.

$$\begin{aligned} A\Delta B &= (A \setminus B) \cup (B \setminus A) \\ &= (A \cap B^c) \cup (B \cap A^c) \\ &= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c] \\ &= [(A \cup B) \cap (B^c \cup B)] \cap [(A \cup A^c) \cap (B^c \cup A^c)] \\ &= [(A \cup B) \cap U] \cap [U \cap (B^c \cup A^c)] \\ &= (A \cup B) \cap (B^c \cup A^c) \\ &= (A \cup B) \cap (B \cap A)^c \\ &= (A \cup B) \setminus (A \cap B). \end{aligned}$$

2.9. Conjunto potencia

Sea A un conjunto. Llamamos conjunto potencia de A, y notamos $\mathcal{P}(A)$, al conjunto de todos los subconjuntos de A. $\mathcal{P}(A)$ también se conoce como el "conjunto de las partes de A". Formalmente:

Definición 2.8 (Conjunto potencia).

$$(\forall X)(X \in \mathcal{P}(A) \iff X \subseteq A)$$

Note que siempre $\phi \in \mathcal{P}(A)$ y $A \in \mathcal{P}(A)$.
Veamos dos ejemplos.

Ejemplo:

Suponga que $A = \{1, 2, 3\}$. En $\mathcal{P}(A)$ están todos los subconjuntos de A. O sea,

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

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

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

Ejemplo importante: Transitividad

A continuación veremos otra técnica de demostración. Supongamos que queremos demostrar que $p \Rightarrow r$. Lo que hacemos es demostrarlo por pasos.
Primero demostramos $p \Rightarrow q_1$. Después $q_1 \Rightarrow q_2$. Después $q_2 \Rightarrow q_3$. Seguimos así hasta que finalmente demostremos $q_n \Rightarrow r$.
Podemos concluir que $p \Rightarrow r$ usando implícitamente la Tautología 2

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

Apliquemos esta técnica para demostrar que para A, B, C conjuntos cualesquiera se tiene:

$$(A\Delta B = A\Delta C) \Rightarrow B = C$$

En efecto,

$$\begin{array}{lll} A\Delta B = A\Delta C & \Rightarrow & A\Delta(A\Delta B) = A\Delta(A\Delta C) \\ & \Rightarrow & (A\Delta A)\Delta B = (A\Delta A)\Delta C \\ & \Rightarrow & \phi\Delta B = \phi\Delta C \\ & \Rightarrow & B = C. \qquad \square \end{array}$$

2.10. Pares Ordenados

Notemos que los conjuntos $\{a, b\}$ y $\{b, a\}$ son idénticos. En efecto, ambos contienen a los mismos elementos. Quisiéramos introducir un objeto que distinga el orden de los elementos.
La solución no es muy difícil. Basta con definir los **pares ordenados** así: $(a, b) = \{\{a\}, \{a, b\}\}$. La propiedad fundamental de los pares ordenados es la siguiente.

Proposición 2.7. *Para todo a, b, x, y se tiene:*

$$(a, b) = (x, y) \iff a = x \wedge b = y$$

Demostración. $\Leftarrow$) Directo.
$\Rightarrow$)
Demostremos primero que $a = x$.
En efecto, como $\{\{a\}, \{a, b\}\} = \{\{x\}, \{x, y\}\}$ se tiene que $\{a\} \in \{\{x\}, \{x, y\}\}$.

Caso 1: $\{a\} = \{x\}$. Se concluye.

Caso 2: $\{a\} \neq \{x\}$. O sea $\{a\} = \{x, y\}$. En este caso se tiene que tener $a = x = y$.

Demostremos ahora que $b = y$.

En efecto, como ya sabemos que $a = x$ la hipótesis nos dice que $\{\{a\}, \{a, b\}\} = \{\{a\}, \{a, y\}\}$.

Caso 1: Si $a = b$, luego $\{a\} = \{a, y\}$, de donde $y = a = b$.

Caso 2: Si $a \neq b$, se tendrá que $\{a, b\} = \{a, y\}$. Luego $b \in \{a, y\}$.
Pero como $a \neq b$, luego $b = y$.

2.11. Producto cartesiano

Sean A, B conjuntos. Se define el producto cartesiano de A con B, que se denota $A \times B$, del siguiente modo:

Definición 2.9 (Producto cartesiano).

$$(\forall x, y)\ [(x, y) \in A \times B \iff x \in A \wedge y \in B]$$

Ejemplo:

Sean $A = \{1, 2, 3\}$ y $B = \{3, 6\}$. Se tiene que

$$A \times B = \{(1, 3), (1, 6), (2, 3), (2, 6), (3, 3), (3, 6)\}$$

Algunas propiedades del producto cartesiano:

Proposición 2.8. *Sean A, A', B, B', C, D conjuntos.*

1. $A' \subseteq A \wedge B' \subseteq B \Rightarrow A' \times B' \subseteq A \times B$
2. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$

Demostración. Demostraremos sólo la primera. Sea $(x, y) \in A' \times B'$. Por definición $x \in A'$ y también $y \in B'$.
Como $A' \subseteq A$ y $B' \subseteq B$ se tiene que $x \in A$ y además $y \in B$. O sea $(x, y) \in A \times B$.

Ejemplo importante: Reducción al absurdo

Veremos otra técnica de demostración más. Supongamos que queremos demostrar que la proposición r es verdadera. Lo que se hace es **asumir que r es falsa y llegar a una contradicción**. ¡¡En otras palabras, lo que se prueba es que en el mundo en que vivimos $\overline{r}$ no puede ser verdadera!!
Si r es una implicancia del tipo $p \Rightarrow q$ entonces, en una demostración por el absurdo, lo que tendríamos que asumir (para llegar a una contradicción) es $\overline{p \Rightarrow q}$.
O sea, $p \wedge \overline{q}$.
Notemos que estamos usando la Tautología 4: $\overline{p \Rightarrow q} \iff p \wedge \overline{q}$.

Veamos, a modo de ejemplo, la siguiente propiedad.

Ejemplo:

Proposición 2.9. *Sean A y B conjuntos. Se tiene que:*

$$A = B \iff A \times B = B \times A$$

DEMOSTRACIÓN. $\Rightarrow$) Directa.

$\Leftarrow$) Reducción al absurdo.
Supongamos que $A \times B = B \times A$ y que al mismo tiempo $A \neq B$. Como $A \neq B$ podemos asumir, sin pérdida de generalidad, la existencia de un $x \in A$ tal que $x \notin B$ (si esto no ocurriese tendría que existir un $x \in B$ tal que $x \notin A$ y la situación sería simétrica).

Sea $y \in B$. Se tiene luego que $(x, y) \in A \times B$ pero $(x, y) \notin B \times A$. Esto contradice el hecho de que $A \times B = B \times A$.

2.12. Cuantificando sobre conjuntos

Dado un conjunto A y una función proposicional $p(x)$, podemos escribir cuantificadores en los que sólo nos interese ver lo que ocurre a los elementos de A. Tenemos así las proposiciones:

Definición 2.10 (Proposiciones cuantificadas sobre conjuntos). *1.* $(\forall x \in A)p(x)$*, que significa que $p(x)$ deber ser cierto para todos los elementos del conjunto A. Notar que esta proposición es equivalente a $(\forall x)(x \in A \Rightarrow p(x))$.*

2. $(\exists x \in A)p(x)$*, que significa que hay al menos un elemento x de A que hace cierto $p(x)$. Notar que esto equivale a $(\exists x)(x \in A \wedge p(x))$.*

3. $(\exists! x \in A)p(x)$*, que significa que hay exactamente un elemento de x de A que hace verdadero $p(x)$.*

Aquí hay dos ideas simultáneas: Existe al menos un $x \in A$ que satisface $p(x)$ (existencia), y que es exactamente uno (unicidad). Claramente esto equivale a $(\exists! x)(x \in A \wedge p(x))$.

El lector puede fácilmente verificar que estos cuantificadores se niegan de la manera usual:

Proposición 2.10.

- $\overline{(\forall x \in A)p(x)} \iff (\exists x \in A)\overline{p(x)}$.
- $\overline{(\exists x \in A)p(x)} \iff (\forall x \in A)\overline{p(x)}$.
- $\overline{(\exists! x \in A)p(x)} \iff [((\forall x \in A)\overline{p(x)}) \vee ((\exists x, y \in A)(p(x) \wedge p(y) \wedge x \neq y))]$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ Una definición formal del conjunto $A = \{1, 2, 3\}$ es $(\forall x)[(x \in A) \Leftrightarrow (x = 1 \vee x = 2 \vee x = 3)]$.

2. ☐ Una definición formal del conjunto $A = \{1, 2, 3\}$ es $(\forall x)[(x \in A) \Leftrightarrow (x = 1 \wedge x = 2 \wedge x = 3)]$.

3. ☐ Dado el conjunto $B = \{x \in A | p(x)\}$, la proposición $x \in B$ está definida por $(\forall x)[(x \in B) \Leftrightarrow (x \in A \vee p(x))]$.

4. ☐ Dado el conjunto $B = \{x \in A | p(x)\}$, la proposición $x \in B$ está definida por $(\forall x)[(x \in B) \Leftrightarrow (x \in A \wedge p(x))]$.

5. ☐ Dado el conjunto $B = \{x \in A | p(x)\}$, la proposición $x \in B$ está definida por $(\forall x)[(x \in B) \Leftrightarrow (x \in A \Rightarrow p(x))]$.

6. ☐ Dado un conjunto $A \neq \mathbb{N}$, se tiene que $\phi = \{x \in \mathbb{N} | x \neq x\} \neq \{x \in A | x \neq x\}$.

7. ☐ Dado un conjunto A, es cierto que $\phi = \{x \in A | x \neq x\}$.

8. ☐ La siguiente proposición lógica es falsa: $(\exists! x)(x \in \phi)$.

9. ☐ La siguiente proposición lógica es verdadera: $(\forall x)(x \notin \phi)$.

10. ☐ La siguiente proposición lógica es falsa: $(\exists x)(x \notin \phi)$.

11. ☐ Dos conjuntos A y B, son iguales si $(\exists x)(x \in A \Leftrightarrow x \in B)$

12. ☐ Dos conjuntos A y B, son iguales si $(\forall x)(x \in A \Leftrightarrow x \in B)$

13. ☐ Dos conjuntos A y B, son iguales si $(\forall x)(x \in A \wedge x \in B)$

14. ☐ Un conjunto A está incluido en un conjunto B si $(\forall x)(x \in B \Rightarrow x \in A)$.

15. ☐ Un conjunto A está incluido en un conjunto B si $(\forall x)(x \notin B \Rightarrow x \notin A)$.

16. ☐ Un conjunto A está incluido en un conjunto B si $(\forall x)(x \in A \Rightarrow x \in B)$.

17. ☐ Dados A, B conjuntos, si $A \subseteq B$ y $B \subseteq A$, no necesariamente se tiene que $A = B$.

18. ☐ Dados A, B conjuntos se tiene que $A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$.

19. ☐ Dados A, B conjuntos, se tiene que $A = B \Leftrightarrow (A \subseteq B \vee B \subseteq A)$.

20. ☐ Dados A, B, C conjuntos, si $A \subseteq B$ y $B \subseteq C$, entonces $B = A$ ó $B = C$.

21. ☐ Dados A, B, C conjuntos, si $A \subseteq B$ y $B \subseteq C$, entonces $B = A = C$.

22. ☐ Dados A, B, C conjuntos, si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$.

23. ☐ Para cualquier conjunto A, se tiene que $\phi \subseteq A$.

24. ☐ Dado un conjunto A, se tiene que $\{\phi\} \subseteq A$.

25. ☐ Dado $A \neq \phi$ conjunto, la proposición $(\exists x)(x \in \phi \Rightarrow x \in A)$ es verdadera.

26. ☐ La unión entre los conjuntos A y B, se define formalmente como: $(\forall x)[(x \in A \cup B) \Leftrightarrow (x \in A \wedge x \in B)]$.

27. ☐ La unión entre los conjuntos A y B, se define formalmente como: $(\forall x)[(x \in A \cup B) \Leftrightarrow (x \in A \vee x \in B)]$.

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: $(\forall x)[(x \in A \cap B) \Leftrightarrow (x \in A \wedge x \in B)]$.

31. ☐ La intersección entre los conjuntos A y B, se define formalmente como: $(\forall x)[(x \in A \cap B) \Leftrightarrow (x \in A \vee x \in B)]$.

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 universo U se define de manera que la proposición $x \in U$ es siempre veradera para los elementos de interés.

34. ☐ Dado un universo U y un conjunto $A \subseteq U$, luego $A^c = U \setminus A$.

35. ☐ Dado un conjunto A, se tiene que $A \cap U = A$.

36. ☐ Dado un conjunto A, se tiene que $A \cap A^c = U$.

37. ☐ Para cualquier par de conjuntos A y B, se tiene que $A^c \cup B^c = U$.

38. ☐ Si dos conjuntos A y B satisfacen que $A \subseteq B$ luego $A^c \subseteq B^c$.

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 $A \subseteq B$ luego $B^c \subseteq A^c$.

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 $A \Delta B = (A \cup B) \setminus (A \cap B) = A^c \Delta B^c$.

47. ☐ Dado un conjunto A, siempre es cierto que $A \in \mathcal{P}(A)$.

48. ☐ Dados A, B conjuntos, se tiene $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

49. ☐ Se tiene que $\mathcal{P}(\phi) = \mathcal{P}(\{\phi\})$.

50. ☐ Se tiene que $\mathcal{P}(\phi) = \{\phi\}$.

51. ☐ Si $A' \subseteq A$ y $B' \subseteq B$, entonces $A' \times A \subseteq B' \times B$.

52. ☐ Si $A' \subseteq A$ y $B' \subseteq B$, entonces $A' \times B' \subseteq A \times B$.

53. ☐ Si A y B son conjuntos tales que $A \times B = B \times A$, entonces necesariamente $A = B$.

54. ☐ La negación de la proposición lógica $(\forall x \in A)p(x)$ es $(\exists x \in A)\overline{p(x)}$.

55. ☐ La negación de la proposición lógica $(\forall x \in A)p(x)$ es $(\exists x \in A^c)\overline{p(x)}$.

56. ☐ La negación de la proposición lógica $(\exists x \in A)p(x)$ es $(\forall x \in A^c)\overline{p(x)}$.

Guía de Ejercicios

1. Demuestre las siguientes propiedades dejadas como ejercicio en las tutorías:

(a) $(A \cap B)^c = A^c \cup B^c$

(b) $(A \subseteq B) \Leftrightarrow (B^c \subseteq A^c)$

(c) $(A^c)^c = A$

(d) $(A \Delta B) \Delta C = A \Delta (B \Delta C)$

(e) $A \Delta \phi = A$

(f) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$

2. Sean $A, B, C \subseteq U$ conjuntos. Emplear los teoremas del álgebra de conjuntos para probar las siguientes igualdades:

(a) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$

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

(c) $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$

(d) $[A \setminus (B \setminus A)] \cup [(B \setminus A) \setminus A] = A \cup B$

(e) $(A \cap B) \setminus (A \cap C) = (A \cap B) \setminus (A^c \cup C)$

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

(a) $A \subseteq B \subseteq C \;\Rightarrow\; C \setminus (B \setminus A) = A \cup (C \setminus B)$.

(b) $B = (A \cap B^c) \cup (A^c \cap B) \Leftrightarrow A = \phi$

(c) $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$

(d) $(A \cup B = A \cap B) \Rightarrow (B \subseteq A \wedge A \subseteq C)$

(e) $(A \cap C = \phi) \Rightarrow (A \setminus B) \setminus C = A \setminus (B \setminus C)$

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

(a) $\mathcal{P}(A)$

(b) $\mathcal{P}(\mathcal{P}(A))$

(c) $A \cap \mathcal{P}(A)$

(d) $\mathcal{P}(A) \cap \mathcal{P}(\phi)$

(e) $(A \times A) \cap \mathcal{P}(\mathcal{P}(A))$
Hint: Recuerde la definición de par ordenado dada en las tutorías.

5. Sean $A, B \subseteq U$ conjuntos. Colocar el signo de inclusión, igualdad o ninguno de ellos, según corresponda entre los conjuntos siguientes (justifique su respuesta):

(a) $A \cap B \square B$

(b) $A^c \square B \setminus A$

(c) $\mathcal{P}(A \cup B) \square \mathcal{P}(A) \cup \mathcal{P}(B)$

(d) $\mathcal{P}(A \cap B) \square \mathcal{P}(A) \cap \mathcal{P}(B)$

(e) $\mathcal{P}(U \setminus A) \square \mathcal{P}(U) \setminus \mathcal{P}(A)$

6. Negar las siguientes proposiciones lógicas:

(a) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})\ x < y$

(b) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\ x \geq y$

(c) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x > 1 \wedge y \leq 1)$

(d) $(\forall \varepsilon \in \mathbb{R}^+)(\exists n_0 \in \mathbb{N})(\forall n > n_0)|a_n| < \varepsilon$

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

(a) $A \times B \neq B \times A$

(b) $A \times (B \times C) \neq (A \times B) \times C$

(c) $A \cup (B \times C) \neq (A \cup B) \times (A \cup C)$

(d) $(A \times B)^c \neq A^c \times B^c$ (Considere un universo apropiado)

(e) $(A \neq B) \wedge (A \times C = B \times C)$

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. Sean A, B, C, D conjuntos. Emplear los teoremas del álgebra de conjuntos para probar que

(a) **(1)** (10 min.) $(B \setminus A) \subseteq C \Leftrightarrow C^c \subseteq (B^c \cup A)$.
(2) (30 min.) $(B \setminus A) \subseteq C \Rightarrow (D \setminus C) \subseteq (D \setminus B) \cup A$.
Hint: Use lo anterior.

(b) (20 min.) $A \cup B = A \cap C \;\Leftrightarrow\; B \subseteq A \wedge A \subseteq C$.

P2. (35 min.) Sean A, B subconjuntos de un mismo universo U. Denotamos $C = (A \cup B)^c$. Probar que

$$(A \Delta B) \Delta C = A \cup B \cup C \;\Leftrightarrow\; A \cap B = \phi.$$

P3. (20 min.) Sea U un conjunto no vacío y $A \subseteq U$. Pruebe que si

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

entonces $A = \phi$.

P4. **(a)** (20 min.) Sean A, B subconjuntos de un mismo universo U. Probar que

$$A \cap B = \phi \;\Leftrightarrow\; \mathcal{P}(A) \cap \mathcal{P}(B) = \{\phi\}.$$

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

(1) $A^c \in \mathcal{F}$
(2) $A \cap B \in \mathcal{F}$
(3) $A \cup B \in \mathcal{F}$
(4) $A \Delta B \in \mathcal{F}$
(5) $\phi \in \mathcal{F} \;\wedge\; U \in \mathcal{F}$.

Importante: Visita regularmente `http://www.dim.uchile.cl/~docencia/algebra` para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

3. Funciones

3.1. 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 3.1 (Función). *Llamaremos función de A en B a cualquier $f \subseteq A \times B$ tal que*

$$(\forall a \in A)(\exists! b \in B) \quad (a, b) \in f$$

Usaremos la notación $f : A \to B$ si es que f es una función de A en B.
Podemos entender una función como una regla de asociación que, dado un elemento cualquiera de A, le asigna un único elemento de B. Gracias a esto, si f es función y $(a, b) \in f$, entonces podemos usar la notación $b = f(a)$. O sea, llamamos $f(a)$ al (único) elemento $b \in B$ tal que $(a, b) \in f$.

Ejemplo:

Consideremos $f = \{(n, p) \in \mathbb{N} \times \mathbb{N} | p = 2n\}$. Esta f resulta ser una función de $\mathbb{N}$ en $\mathbb{N}$, pues el único valor que estamos asociando a cada natural n es el natural $p = 2n$.
Desde ahora, pensaremos en las funciones simplemente como reglas de asociación entre dos conjuntos. Así, la función f que definimos en el párrafo anterior podemos describirla como

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

3.2. Ejemplos de funciones

Veamos otras funciones:

Ejemplos:

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

   f es una 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.

2. 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, intuitivamente sabemos que lo es: a cada número real x le asociamos el número entero más cercano que tenga, que sea menor o igual que él. Por ejemplo $g(11/2) = 5$; $g(3) = 3$ y $g(-3/2) = -2$.

3. Un ejemplo importante, que utilizaremos después, es la llamada función **identidad** de un conjunto A. Ésta es la función $id_A : A \to A$, que se define por $id_A(x) = x$ para cada $x \in A$.

4. 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. 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.

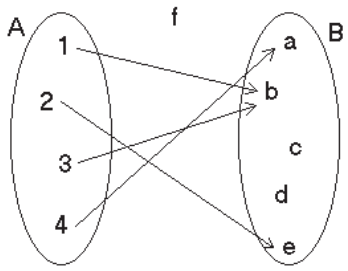

Figura 7: Una función definida mediante diagrama de flechas.

5. 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.

A pesar de que conocemos la definición de qué significa ser 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 $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x^2 + y^2 = 1\}$. Hay dos razones que impiden que f constituya una función de $\mathbb{R}$ en $\mathbb{R}$:

- El valor $f(x)$ no está definido para todos los números reales x. 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 ningún número real al real $x = 2$.

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

Ejemplo:

- Lo más grave, sin embargo, es que existen números reales x a los cuales f les está asociando más de un valor y: 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 $-1 < x < 1$.

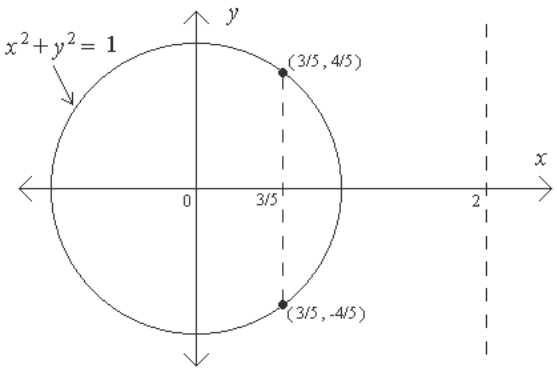

Figura 8: Este diagrama no define una función.

3.3. Igualdad de funciones

Supongamos que $f : A \to B$ es 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 **conjunto de llegada** de f, y lo denotaremos $\mathrm{Rec}(f)$.
Sean $f, g : A \to B$ dos funciones. Una forma de definir igualdad entre funciones es comparar los resultados que ellas dan cuando se les entrega cada uno de los elementos de A. Es decir, definir

$$f = g \iff (\forall a \in A) f(a) = g(a)$$

¿Qué definición de igualdad podemos usar cuando $f : A \to B$ y $g : C \to D$?

Notemos que nuestra definición anterior sólo tiene sentido cuando $A = C$, es decir cuando $\mathrm{Dom}(f) = \mathrm{Dom}(g)$.

¿Tendrá sentido preguntarse si son iguales dos funciones que no parten del mismo conjunto? O sea, no sólo la definición de los valores de la función es relevante para que haya igualdad, sino que también importa cuáles son los dominios y los conjuntos de llegada de las dos funciones.

Así, nuestra definición de igualdad para cualquier par de funciones será la siguiente:

Definición 3.2 (Igualdad de funciones). *Si $f : A \to B$ y $g : C \to D$ son funciones, entonces*

$$f = g \iff \left[\begin{array}{c} \mathrm{Dom}(f) = \mathrm{Dom}(g) \\ \wedge \\ \mathrm{Rec}(f) = \mathrm{Rec}(g) \\ \wedge \\ (\forall x \in \mathrm{Dom}(f)) f(x) = g(x) \end{array}\right]$$

Ejemplo:

[¿son iguales estas funciones?] Consideremos la funciones f y g dadas por

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

Aunque a primera vista ambas funciones nos parecen iguales, esto no es así. Primero debemos notar que nuestra definición de f y g no ha sido todo lo rigurosa que debiera.

¿Cuáles son el dominio y el conjunto de llegada de f y g?

g es una función que está bien definida para cualquier elemento de $\mathbb{R}$, por lo que podemos considerar $\mathrm{Dom}(g) = \mathbb{R}$. Asimismo, tenemos que $\mathrm{Rec}(g) = \mathbb{R}$.
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 de f. Sí podría serlo $\mathbb{R} \setminus \{1\}$.
Para el conjunto de llegada el análisis puede ser más sencillo, y consideraremos $\mathrm{Rec}(f) = \mathbb{R}$ también (como ejercicio para el lector, puede mostrar que también se puede considerar $\mathrm{Rec}(f) = \mathbb{R} \setminus \{3\}$).

Hemos concluido que $\mathrm{Dom}(f) \neq \mathrm{Dom}(g)$, así que ambas funciones ya no pueden ser iguales. Si nos empeñamos en querer compararlas, podemos hacer lo siguiente: ver a g como si fuera una función solamente definida de $\mathbb{R} \setminus \{1\}$ en $\mathbb{R}$.
Es decir, nos olvidamos que g también puede ser evaluada en $x = 1$. En tal caso, $\mathrm{Dom}(f) = \mathbb{R} \setminus \{1\} = \mathrm{Dom}(g)$, y además $\mathrm{Rec}(f) = \mathbb{R} = \mathrm{Rec}(g)$. 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, en este contexto, las funciones f y g son iguales.

3.4. Funciones y resolución de ecuaciones

Consideremos el siguiente problema: Dada una función $f : A \to B$, y un elemento $y \in B$, queremos encontrar un $x \in A$ tal que $y = f(x)$.
Tomemos el ejemplo de 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 en caso de tenerla, puede tener más de una.

En lo siguiente revisaremos propiedades que nos ayudarán a conocer cuándo este problema que nos planteamos, para una función $f : A \to B$ dada, posee soluciones para cualquier $y \in B$, y si estas soluciones son únicas.

3.5. Inyectividad

Una primera definición importante:

Definición 3.3 (Inyectividad). *Sea $f : A \to B$ una función. Diremos que f es* **inyectiva** *si se cumple que*

$$(\forall x_1, x_2 \in A) \quad [x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)]$$

O, equivalentemente, si se cumple que

$$(\forall x_1, x_2 \in A) \quad [f(x_1) = f(x_2) \Rightarrow x_1 = x_2]$$

Ejemplos:

- Observemos que, entonces, la función $q(x) = x^2$, definida de $\mathbb{R}$ en $\mathbb{R}$, **no** es inyectiva pues, tomando $x_1 = -1$ y $x_2 = 1$, se tiene que

$$x_1 \neq x_2 \wedge f(x_1) = f(x_2)$$

- Un ejemplo de función que sí es inyectiva es el de la función $l : \mathbb{R} \to \mathbb{R}$ dada por $l(x) = ax + b$ con $a \neq 0$:

Supongamos que existen un par de elementos $x_1, x_2 \in \mathbb{R}$ tales que

$$l(x_1) = l(x_2)$$

Podemos, entonces, despejar del modo siguiente:

$$\begin{aligned} ax_1 + b &= ax_2 + b \\ ax_1 &= ax_2 \\ x_1 &= x_2 \end{aligned}$$

El último paso lo obtenemos dividiendo por a, lo cual es válido pues sabemos que $a \neq 0$. O sea, probamos que

$$(\forall x_1, x_2 \in \mathbb{R}) \quad l(x_1) = l(x_2) \Rightarrow x_1 = x_2$$

es decir, que l es inyectiva.

3.6. Sobreyectividad

Definición 3.4 (Sobreyectividad). *Sea $f : A \to B$ una función. Diremos que f es* **sobreyectiva** *si se cumple que*

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

Algunos ejemplos:

Ejemplos:

- La función $q(x) = x^2$, definida de $\mathbb{R}$ en $\mathbb{R}$, *no* es sobreyectiva 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 sí es sobreyectiva.

Sea $y \in \mathbb{R}$ arbitrario. Buscamos 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 $l(x) = y$.

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

3.7. Biyectividad

Definición 3.5 (Biyectividad). *Sea $f : A \to B$ una función. Diremos que f es* **biyectiva** *si es inyectiva y sobreyectiva a la vez.*

Concluimos, entonces, que la función $q(x) = x^2$, definida de $\mathbb{R}$ en $\mathbb{R}$, no es biyectiva. Por el contrario, la función $l(x) = ax + b$, definida de $\mathbb{R}$ en $\mathbb{R}$, sí es biyectiva.

Proposición 3.1. *Una función $f : A \to B$ es biyectiva si y sólo si*

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

Demostración. Observemos que la sobreyectividad 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.

3.8. 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 (3.8), si f no fuera biyectiva, habría elementos de B a los cuáles no sabríamos asociarle un elemento de A.
Recordando que una función de A en B es en realidad un subconjunto de $A \times B$, podemos construir un 'candidatoá función g del siguiente modo:

> Los elementos de $g \subseteq B \times A$ serán todos los pares ordenados $(b, a) \in B \times A$ tales que $(a, b) \in f$, 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 la siguiente propiedad:

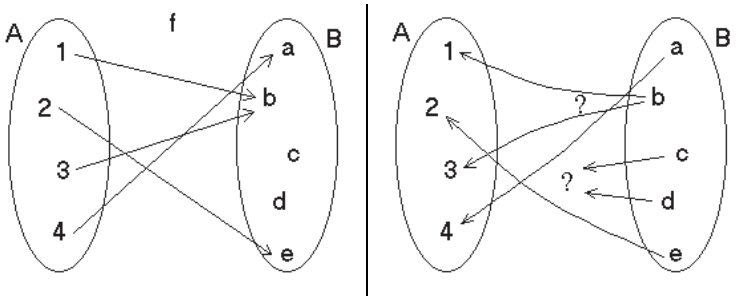

Figura 9: Dificultades para definir la inversa de una función no biyectiva.

Proposición 3.2.

$$f \text{ es biyectiva} \iff g \text{ es función}$$

Demostración.

$$\begin{aligned} f \text{ es biyectiva} &\iff (\forall y \in B)(\exists! x \in A)\ f(x) = y \\ &\iff (\forall y \in B)(\exists! x \in A)\ (y, x) \in g \\ &\iff g \text{ es función} \end{aligned}$$

A la función g que construimos de esta manera le llamaremos...

Definición 3.6 (Función inversa). *Dada f biyectiva, se define la función inversa de f, denotada f^{-1} por:*

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

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

Proposición 3.3.

1. $(\forall x \in A)\ f^{-1}(f(x)) = x$.
2. $(\forall y \in B)\ f(f^{-1}(y)) = y$.
3. f^{-1} *es biyectiva, y* $(f^{-1})^{-1} = f$.

Demostración. Demostraremos (2) y (3).
Para (2), consideremos $y \in B$ cualquiera. Si denotamos $x = f^{-1}(y)$, tenemos entonces que $f(x) = y$, gracias a la afirmación hecha anteriormente. Entonces

$$f(f^{-1}(y)) = f(x) = y$$

Para (2), llamemos $h = f^{-1}$, con lo que h es una función de B en A.
h es inyectiva: Sean $y_1, y_2 \in B$ tales que $h(y_1) = h(y_2)$. Como ambos elementos pertenecen a A, entonces podemos concluir que $f(h(y_1)) = f(h(y_2))$. Recordando que $h = f^{-1}$ y usando la propiedad (1.2) obtenemos que $y_1 = y_2$.
h es sobreyectiva: Sea $x \in A$ cualquiera. Buscamos $y \in B$ tal que $h(y) = x$. Basta tomar, entonces, $y = f(x)$, y así $h(y) = h(f(x))$. Recordando que $h = f^{-1}$ y utilizando la propiedad (1.1) obtenemos que $h(y) = x$.
Por lo tanto h es biyectiva, y tiene una función inversa h^{-1}. Ésta cumple que

$$(\forall x \in A)(\forall y \in B) \quad h(y) = x \iff h^{-1}(x) = y$$

Sean $x \in A, y \in B$ tales que $h(y) = x$. Como $h = f^{-1}$, tenemos que

$$h(y) = x \iff f(x) = y$$

Así, para $x \in A$:

$$h^{-1}(x) = y \iff f(x) = y$$

Con esto se concluye que para cualquier $x \in A$, $h^{-1}(x) = f(x)$. Entonces

$$h^{-1} = f$$

o equivalentemente,

$$(f^{-1})^{-1} = f$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ $f \subseteq A \times B$ es función si la proposición $(\forall a \in A)(\exists b \in B)(a,b) \in f$ es verdadera.

2. ☐ $f \subseteq A \times B$ es función si la proposición $(\forall a \in A)(\exists! b \in B)(a,b) \in f$ es verdadera.

3. ☐ $f \subseteq A \times B$ es función si la proposición $(\forall a \in A)(\forall b \in B)(a,b) \in f$ es verdadera.

4. ☐ Según la notación de función, se tiene que para $a \in A$ $(a, f(a)) \in f$.

5. ☐ Según la notación de función, $b = f(a)$ equivale a $(f(a), b) \in f$.

6. ☐ Según la notación de función $b = f(a)$ equivale a $(f(a), f(b)) \in f$.

7. ☐ El conjunto $A = \{(x,y) \in \mathbb{R} \times \mathbb{R} \ : \ x^2 + y^2 = 1\}$ corresponde a una función de $\mathbb{R}$ en $\mathbb{R}$.

8. ☐ El conjunto $A = \{(x,y) \in [0,1) \times \mathbb{R}_+^* \ : \ x^2 + y^2 = 1\}$ corresponde a una función de $[0,1)$ en $\mathbb{R}$.

9. ☐ El conjunto $A = \{(x,y) \in \mathbb{R} \times \mathbb{R} \ : \ y \in \{-1,1\}\}$ corresponde a una función de $\mathbb{R}$ en $\mathbb{R}$

10. ☐ El conjunto $A = \{(x,y) \in \mathbb{R} \times \mathbb{N} \ : \ y \in \{-1,1\}\}$ corresponde a una función de $\mathbb{R}$ en $\mathbb{N}$

11. ☐ Para que dos funciones f y g sean iguales basta que $(\forall a(f(a) = g(a))$.

12. ☐ Para que dos funciones $f, g : A \to B$ sean iguales basta que $(\forall a \in A)(f(a) = g(a))$.

13. ☐ Para que dos funciones $f : A \to B$ y $f : C \to D$ sean iguales basta que $(\forall a \in A \cap C)(f(a) = g(a))$.

14. ☐ Para que dos funciones $f : A \to B$ y $f : C \to D$ sean iguales se debe cumplir que $\text{Dom}(f) = \text{Dom}(g)$ y que $(\forall a \in A)(f(a) = g(a))$.

15. ☐ Para que dos funciones $f : A \to B$ y $f : C \to D$ sean iguales se debe cumplir que $\text{Dom}(f) = \text{Dom}(g)$, que $\text{Rec}(f) = \text{Rec}(g)$ y que $(\forall a \in A)(f(a) = g(a))$.

16. ☐ El problema de dada un función $f : A \to B$ y $a \in A$, encontrar $x \in B$ tal que $f(a) = x$ siempre tiene una única solución.

17. ☐ El problema de dada un función $f : A \to B$ y $a \in A$, encontrar $x \in B$ tal que $f(a) = x$ no siempre tiene una solución.

18. ☐ El problema de dada un 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.

19. ☐ El problema de dada un función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$ siempre tiene una única solución.

20. ☐ El problema de dada un función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$ no siempre tiene solución.

21. ☐ El problema de dada un función $f : A \to B$ y $b \in B$, encontrar $x \in A$ tal que $f(x) = b$, si tiene solución esta no es siempre única.

22. ☐ Una función $f : A \to B$ es inyectiva si satisface que $(\forall x_1, x_2 \in A)(x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$.

23. ☐ Una función $f : A \to B$ es inyectiva si satisface que $(\forall x_1, x_2 \in A)(x_1 = x_2 \Rightarrow f(x_1) = f(x_2))$.

24. ☐ Una función $f : A \to B$ es inyectiva si satisface que $(\forall x_1, x_2 \in A)(f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

25. ☐ Una función $f : A \to B$ es inyectiva si satisface que $(\forall x_1, x_2 \in A)(f(x_1) \neq f(x_2) \Rightarrow x_1 \neq x_2)$.

26. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}$, definida por $f(x) = x^2$, es inyectiva.

27. ☐ La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, es inyectiva.

28. ☐ La función $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}_+^*$, definida por $f(x) = x^2$, es inyectiva.

29. ☐ La función $f : \mathbb{R} \to \mathbb{R}_+^*$, definida por $f(x) = |x - 1|$, es inyectiva.

30. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}$, definida por $f(x) = |x - 1|$, es inyectiva.

31. ☐ La función $f : (1, +\infty) \to \mathbb{R}$, definida por $f(x) = |x - 1|$, es inyectiva.

32. ☐ Una función $f : A \to B$ es sobreyectiva si satisface que $(\forall a \in A)(\exists b \in B)(f(a) = b)$.

33. ☐ Una función $f : A \to B$ es sobreyectiva si satisface que $(\forall a \in A)(\exists! b \in B)(f(a) = b)$.

34. ☐ Una función $f : A \to B$ es sobreyectiva si satisface que $(\forall b \in B)(\exists a \in A)(f(a) = b)$.

35. ☐ Una función $f : A \to B$ que satisface $(\forall b \in B)(\exists! a \in A)(f(a) = b)$, no necesariamente es sobreyectiva.

36. ☐ Una función $f : A \to B$ que satisface $(\forall b \in B)(\exists! a \in A)(f(a) = b)$, es inyectiva.

37. ☐ Una función $f : A \to B$ que satisface $(\forall b \in B)(\exists! a \in A)(f(a) = b)$, es sobreyectiva, pero no necesariamente inyectiva.

38. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}$, definida por $f(x) = x^2$, es sobreyectiva.

39. ☐ La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = x^2$, no es sobreyectiva.

40. ☐ La función $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}_+^*$, definida por $f(x) = x^2$, es sobreyectiva.

41. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$, definida por $f(x) = x^2$, es sobreyectiva.

42. ☐ Una función es biyectiva si es inyectiva o sobreyectiva.

43. ☐ Una función es biyectiva si es inyectiva y sobreyectiva.

44. ☐ Una función $f : A \to B$ es biyectiva si satisface $(\forall b \in B)(\exists! a \in A)(f(a) = b)$.

45. ☐ La función $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}_+^*$, definida por $f(x) = x^2$, es biyectiva.

46. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$, definida por $f(x) = x^2$, es biyectiva.

47. ☐ La función $f : \mathbb{R}_+^* \to \mathbb{R}$, definida por $f(x) = x^2$, es biyectiva.

48. ☐ La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, siempre es biyectiva.

49. ☐ La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, es biyectiva si $b \neq 0$.

50. ☐ La función $f : \mathbb{R} \to \mathbb{R}$, definida por $f(x) = ax + b$ con $a, b \in \mathbb{R}$, es biyectiva si $a \neq 0$.

51. ☐ Dada una función $f : A \to B$ cualquiera, su inversa existe y se denota f^{-1}.

52. ☐ Existen funciones que no son inyectivas y que tienen una inversa.

53. ☐ La inversa de una función biyectiva, es biyectiva.

54. ☐ Existe una función $f : A \to A$ biyectiva, tal que para algún $a \in A$ se tiene que $f(f^{-1}(a)) \neq f^{-1}(f(a))$.

Guía de Ejercicios

1. Indique cuál de los siguientes conjuntos establece una función:

(a) $R = \{(a,b) \in \mathbb{N}^2 / b = a^p \text{ para algún } p \in N\}$

(b) Sean $a,b,c \in \mathbb{R}\backslash\{0\}$ fijos, $R = \{(x,y) \in \mathbb{R}^2 / y = ax^3 + bx + c\}$

(c) $R = \{(x,y) \in \mathbb{R}^2 / y = ax^3 + bx + c \text{ con } a,b,c \in \mathbb{R}\}$

(d) $R = \{(x,y) \in \mathbb{R}^2 / x = y^2 + 2y + 1\}$

(e) $R = \{(y,x) \in \mathbb{R}^2 / x = (y+1)^2\}$

(f) $R = \{(x,y) \in \mathbb{R}^2 / x = y^3\}$

Indicación: Dado un conjunto A, se usa la notación $A^2 = A \times A$.

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

(b) $f,g : \mathbb{R} \setminus \{-1,0,1\} \to \mathbb{R}$ con$f(x) = \frac{1}{x}, g(x) = \frac{(x+1)(x-1)}{x^3-x}$

(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$f(x) = \frac{sen(x)}{x+1}, g(x) = \frac{sen(x-1)}{x}$

(e) $f,g : \mathbb{R}^+ \to \mathbb{R}$ con $f(x) = \frac{x}{\sqrt{x}}, g(x) = \sqrt{x}$

Indicación: Se usa la notación $\mathbb{R}^+ = (0,\infty)$.

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

(a) $f : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $(\forall X \subseteq A)\ f(X) = X^c$.

(b) $g : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $(\forall X \subseteq A)\ g(X) = X \setminus (X^c)$.

(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 $(\forall X \subseteq A)\ h_3(X) = X \triangle B$.

4. Dados dos conjuntos A y B, determine si las siguientes son funciones y si son inyectivas, sobreyectivas 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 $(\forall a \in A)\ f(a) = (a, b_0)$.

5. Comente sobre la inyectividad, sobreyectividad 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) $f(x) = sen(x)$

(d) $f(x) = \frac{x^2+3x-1}{2x^2-5x+4}$

Indicación: >Se puede *redefinir* el dominio o el conjunto de llegada de f de modo que la función logre ser inyectiva o sobreyectiva?.

6. 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) $f : [0, 2\pi] \to \mathbb{R}, \quad f(x) = sen(x^2)$

(d) $f : \mathbb{R}^+ \to \mathbb{R}, \quad f(x) = \frac{x}{\sqrt{x}}$

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. (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.

P2. 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 $\{f(x) : \ x \in \mathbb{R}\setminus\{2\}\} = \mathbb{R}\setminus\{2\}$.

(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.

P3. (30 min.) Para $a, b \in \mathbb{R}$ considere la recta $L_{a,b} = \{(x, y) \in \mathbb{R}^2 / y = ax + b\}$ y la colección de rectas $\mathcal{L} = \{L_{a,b} \subset \mathbb{R}^2 / a, b \in \mathbb{R}\}$. Se define el conjunto de pares de rectas no paralelas

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

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

P4. Sea U el conjunto universo y $A, B \subset U$. Se define

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

(a) (15 min.) Pruebe que $f(f(X)) = f(X) \quad \forall X \in \mathcal{P}(\mathcal{U})$.

(b) (15 min.) Si $A \neq U \vee B \neq \phi$, pruebe que f no es inyectiva.

(c) (10 min.) Si $A \neq U$ pruebe que f no es sobreyectiva.

P5. Sea $E \neq \phi$ un conjunto fijo. Para todo subconjunto A de E se define la función característica de A como:

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

(a) (10 min.) Describa $\delta_E(x)$ y $\delta_\phi(x)$ 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 $C \subseteq D \Leftrightarrow (\forall x \in E) \quad \delta_C(x) \leq \delta_D(x)$

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

3.9. 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 siguiente diagrama:

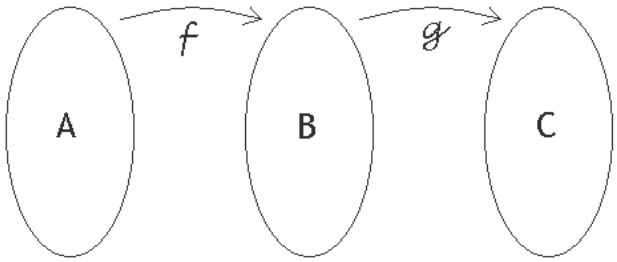

Figura 10: Esquema necesario para poder componer dos funciones f y g.

Definiremos la función **composición de f y g**, la cual denotaremos por $g \circ f$, como una función de A en C, dada por

Definición 3.7 (Función composición).

$$(\forall a \in A) \quad (g \circ f)(a) = g(f(a)).$$

Notemos que para definir $g \circ f$ basta que se cumpla que $\text{Rec}(f) \subseteq \text{Dom}(g)$, para poder evaluar la función g sobre el elemento $f(a)$. Es decir, la definición puede hacerse de manera más general.

Ejemplos:

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

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

es decir

$$g \circ f = h$$

Algunas propiedades de la composición:

Propiedades 1. *Si $f : A \to B$, $g : B \to C$, $h : C \to D$ son funciones, entonces*

1. $h \circ (g \circ f) = (h \circ g) \circ f$ *(esta propiedad se llama asociatividad)*
2. *En general, no hay conmutatividad*
3. $id_B \circ f = f \circ id_A = f$ *(es decir, la función identidad es neutro para la composición)*

4. *Si f es biyectiva, entonces $f \circ f^{-1} = id_B$ y $f^{-1} \circ f = id_A$*

Demostración. Demostremos (4). Para la primera afirmación:

$$f \circ f^{-1} = id_B$$

notamos que $f : A \to B$, por lo que $f^{-1} : B \to A$, y entonces $f \circ f^{-1} : B \to B$, por la definición de composición. Como $\mathrm{Dom}(id_B) = \mathrm{Rec}(id_B) = B$, concluimos que

$$\mathrm{Dom}(id_B) = \mathrm{Dom}(f \circ f^{-1}) \quad \wedge \quad \mathrm{Rec}(id_B) = \mathrm{Rec}(f \circ f^{-1})$$

Falta solamente mostrar que $(\forall w \in B)\ id_B(w) = (f \circ f^{-1})(w)$, lo cual hacemos del modo siguiente:
Sea $w \in B$, y llamemos $x = f^{-1}(w) \in A$. Como f es la función inversa de f^{-1}, tenemos también que $w = f(x)$. Entonces

$$\begin{aligned} (f \circ f^{-1})(w) &= f(f^{-1}(w)) \\ &= f(x) \\ &= w \\ &= id_B(w) \end{aligned}$$

y listo. Para demostrar que $f^{-1} \circ f = id_A$ se sigue el mismo procedimiento.

Algunas propiedades con respecto a la inyectividad y sobreyectividad:

Propiedades 2. *Si $f : A \to B$, $g : B \to C$ son funciones, entonces*

1. *Si f y g son inyectivas, entonces $(g \circ f)$ es inyectiva.*
2. *Si f y g son sobreyectivas, entonces $(g \circ f)$ es sobreyectiva.*
3. *Si f y g son biyectivas, entonces $(g \circ f)$ es biyectiva.*
4. *Si $(g \circ f)$ es inyectiva, entonces f es inyectiva (g no necesariamente lo es).*
5. *Si $(g \circ f)$ es sobreyectiva, entonces g es sobreyectiva (f no necesariamente lo es).*

Demostración. Demostraremos (2) y (4).
Para (2): Queremos ver que la función $g \circ f : A \to C$ es sobreyectiva. Sea $c \in C$. Buscamos un $a \in A$ tal que $(g \circ f)(a) = c$, es decir que $g(f(a)) = c$.
Como $g : B \to C$ es sobreyectiva, sabemos que existe un $b \in B$ tal que $g(b) = c$. Del mismo modo, como $f : A \to B$ es sobreyectiva, sabemos que existe $a \in A$ tal que $f(a) = b$. Así

$$(g \circ f)(a) = g(f(a)) = g(b) = c$$

que es lo que queríamos demostrar.
Probaremos (4):

> Si $(g \circ f)$ es inyectiva, entonces f es inyectiva (g no necesariamente lo es).

Sabemos que $(g \circ f)$ es inyectiva.
Para demostrar que f también lo es, consideremos $a_1, a_2 \in A$ tales que $f(a_1) = f(a_2)$. Notemos que $f(a_1), f(a_2) \in B$ pues $\text{Rec}(f) = B$. Así, evaluando la función g obtenemos

$$g(f(a_1)) = g(f(a_2))$$

es decir

$$(g \circ f)(a_1) = (g \circ f)(a_2)$$

Como sabemos que $(g \circ f)$ es inyectiva, obtenemos que $a_1 = a_2$, por lo que f es también inyectiva.

Método para cálculo de inversas

Una propiedad útil para el cálculo de funciones inversas:

Propiedad 1. *Sea $f : A \to B$ biyectiva, y sea $g : B \to A$*

- *Si $g \circ f = id_A$, entonces $g = f^{-1}$.*
- *Si $f \circ g = id_B$, entonces $g = f^{-1}$.*

Esta propiedad nos dice que para calcular la inversa de una función biyectiva f, basta encontrar una función g que compuesta con f nos dé la identidad. Ya sea que las hayamos compuesto en el orden $g \circ f$ o en el orden $f \circ g$, podemos concluir que $f^{-1} = g$.

Demostración. Demostraremos la primera de ellas, es decir

$$g \circ f = id_A \Rightarrow g = f^{-1}$$

Como f es biyectiva, para que $g = f^{-1}$ basta demostrar que

$$(\forall x \in A)(\forall y \in B) \quad f(x) = y \iff g(y) = x$$

Sean $x \in A, y \in B$. Demostraremos las dos implicancias:
$\Rightarrow$) Supongamos que $f(x) = y$. Como ambos lados de esta igualdad son elementos de B, podemos aplicar g, y obtener

$$\begin{aligned} g(f(x)) &= g(y) \\ (g \circ f)(x) &= g(y) \end{aligned}$$

Como por hipótesis $g \circ f = id_A$, entonces concluimos que

$$g(y) = id_A(x) = x$$

$\Leftarrow$) Supongamos ahora que $g(y) = x$. Como f es sobreyectiva, tenemos que existe $w \in A$ tal que $f(w) = y$. Entonces

$$x = g(y) = g(f(w)) = (g \circ f)(w) = id_A(w) = w$$

Por lo tanto, $f(x) = f(w) = y$.

La siguiente propiedad, es también útil y no es necesario saber de antemano si la función es biyectiva.

Propiedad 2. *Sean $f : A \to B$ y $g : B \to A$, funciones.*

$$\text{Si } g \circ f = id_A \text{ y } f \circ g = id_B, \text{ entonces } g = f^{-1}.$$

Notar que implícitamente, la propiedad implica que f es biyectiva.

DEMOSTRACIÓN. Nos basta probar que f es biyectiva, ya que usando la propiedad anterior tendremos que $g = f^{-1}$.

Pero, gracias a la propiedad (4) respecto de inyectividad y sobreyectividad vista antes, como $g \circ f = id_A$ es inyectiva (ya que id_A siempre lo es), luego f es inyectiva.

Además, usando la propiedad (5), como $f \circ g = id_B$ es sobreyectiva, luego f es sobreyaectiva.

Así, f es biyectiva y se concluye el resultado.

Inversa de una composición

Como consecuencia, podemos obtener la siguiente conclusión:

Proposición 3.4 (Inversa de una composición). *Si $f : A \to B$ y $g : B \to C$ son biyectivas, entonces*

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

DEMOSTRACIÓN. Denotemos $F = g \circ f$ y $G = f^{-1} \circ g^{-1}$.
Tenemos que $F : A \to C$, y que $G : C \to A$. Además, como g y f son biyectivas, entonces gracias a una propiedad anterior sabemos que F también es biyectiva. Así, la afirmación que queremos demostrar puede escribirse como

$$F^{-1} = G$$

Gracias a las propiedades mencionadas, para esto basta mostrar que $G \circ F = id_A$. En efecto,

$$\begin{aligned} G \circ F &= (f^{-1} \circ g^{-1}) \circ (g \circ f) \\ &= f^{-1} \circ (g^{-1} \circ g) \circ f \\ &= f^{-1} \circ id_B \circ f \\ &= f^{-1} \circ f \\ &= id_A \end{aligned}$$

3.10. 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

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

lo que 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

$$\{4, 16\} \text{ es el conjunto de preimágenes de } 36$$

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 el conjunto obtenido al reunir las preimágenes 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 hemos obtenido el conjunto formado por todas las preimágenes de ciertos elementos, podemos formar el conjunto de todas las imágenes de ciertos elementos. Como sabemos que 9,4,1,0,1 y 4 son respectivamente las imágenes de 7,8,9,10,11 y 12, escribimos que

> $\{0, 1, 4, 9\}$ 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)

Conjunto imagen

En esta sección definiremos precisamente los conceptos de conjunto imagen y conjunto preimagen para una función f dada, y estudiaremos varias propiedades.

Definición 3.8 (Conjunto imagen). *Sea $f : A \to B$ una función, y sea $A' \subseteq A$. Definimos el* **conjunto imagen de A' por** *f como*

$$f(A') = \{b \in B : (\exists a \in A')\ f(a) = b\}$$

o equivalentemente

$$b \in f(A') \iff (\exists a \in A')\ f(a) = b$$

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

Propiedades 3. *Sea $f : A \to B$ función. Sean $A_1, A_2 \subseteq A$.*

1. *f es sobreyectiva $\iff$ $f(A) = B$*
2. *$A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$*
3. *$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$*
4. *$f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$*

Demostración. Demostraremos (2).
Supongamos que $A_1 \subseteq A_2$, y sea $y \in f(A_1)$.
Por definición de conjunto imagen, tenemos que $\exists x \in A_1$ tal que $y = f(x)$. Como A_1 está contenido en A_2, entonces $x \in A_2$.
Así, existe un $x \in A_2$ tal que $y = f(x)$, con lo que obtenemos que $y \in f(A_2)$.

Conjunto preimagen

Definimos ahora, el conjunto preimagen:

Definición 3.9 (Conjunto preimagen). *Dado $B' \subseteq B$, el* **conjunto preimagen de B' por** *f como*

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

o, en términos lógicos

$$a \in f^{-1}(B') \iff f(a) \in B'$$

$f^{-1}(B')$ es siempre un subconjunto de A. Es el obtenido al reunir todas las preimágenes de los elementos de B'.

Propiedades 4. *Sea $f : A \to B$ función. Sean $B_1, B_2 \subseteq B$.*

1. $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$
2. $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
3. $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$

Demostración. Demostraremos (2).
Consideremos un elemento x arbitrario. Se tiene que

$$\begin{array}{lcll} x \in f^{-1}(B_1 \cap B_2) & \iff & f(x) \in B_1 \cap B_2 & \text{(def. de conjunto preimagen)} \\ & \iff & f(x) \in B_1 \wedge f(x) \in B_2 & \text{(intersección de conjuntos)} \\ & \iff & x \in f^{-1}(B_1) \wedge x \in f^{-1}(B_2) & \text{(def. de conjunto preimagen)} \\ & \iff & x \in f^{-1}(B_1) \cap f^{-1}(B_2) & \text{(intersección de conjuntos)} \end{array}$$

Enumeramos ahora propiedades que surgen cuando reunimos los conceptos vistos en las secciones anteriores.

Propiedades 5.
1. *Si $A' \subseteq A$, entonces $A' \subseteq f^{-1}(f(A'))$*
2. *Si $B' \subseteq B$, entonces $f(f^{-1}(B')) \subseteq B'$*
3. *f es inyectiva $\iff (\forall A' \subseteq A)\ A' = f^{-1}(f(A'))$*
4. *f es sobreyectiva $\iff (\forall B' \subseteq B)\ f(f^{-1}(B')) = B'$*

Demostración. Demostraremos (3).
$\Rightarrow$) Supongamos que f es inyectiva, y tomemos $A' \subseteq A$. Gracias a (1), sabemos que

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

y por lo tanto sólo nos falta demostrar la otra inclusión.
Sea $x \in f^{-1}(f(A'))$, queremos demostrar que $x \in A'$.
Por definición de conjunto preimagen, tenemos que $f(x) \in f(A')$. Llamando $y = f(x)$, y por definición de conjunto imagen, tenemos que existe un $w \in A'$ tal que $f(w) = y$.
Así, $f(x) = f(w)$, y como f es inyectiva, concluimos que $x = w$. Pero sabíamos que $w \in A'$, por lo tanto $x \in A'$.

$\Leftarrow$) Supongamos, por contradicción, que f no es inyectiva. Entonces existen elementos $x_1, x_2 \in A$ tales que $x_1 \neq x_2$ y $f(x_1) = f(x_2)$. Llamemos y a este valor común (es decir, $y = f(x_1) = f(x_2)$). Definiendo $A' = \{x_1\} \subseteq A$, tenemos que

$$f(A') = f(\{x_1\}) = \{f(x_1)\} = \{y\}$$

por lo que

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

Como $f(x_2) = y$, entonces

$$x_2 \in f^{-1}(f(A'))$$

Utilizando la propiedad, tenemos que $f^{-1}(f(A')) = A'$, con lo que $x_2 \in A'$, es decir $x_2 \in \{x_1\}$, de donde concluimos que $x_1 = x_2$, lo que es una contradicción.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ Si $f : A \to B, g : C \to D$. Basta con que $B \subseteq C$ para que $g \circ f$ exista.

2. ☐ Si $f : A \to B, g : C \to D$. Basta con que $C \subseteq B$ para que $g \circ f$ exista.

3. ☐ Si $f : A \to B, g : C \to D$. Necesariamente se debe tener $B = C$ para que $g \circ f$ exista.

4. ☐ Si $f : A \to B, g : B \to A$ entonces $f \circ g = g \circ f$.

5. ☐ Si $f : A \to A, g : A \to A$ entonces $f \circ g = g \circ f$.

6. ☐ Si $f : A \to B, g : B \to A$ y f es la función identidad, entonces $f \circ g = g \circ f$.

7. ☐ Si $f : A \to B, g : B \to C$ y f es inyectiva, entonces $g \circ f$ también lo es.

8. ☐ Si $f : A \to B, g : B \to C$ y g es inyectiva, $g \circ f$ también lo es.

9. ☐ Si $f : A \to B, g : B \to C$ son tales que f y g son inyectivas, $g \circ f$ también lo es.

10. ☐ Si $f : A \to B, g : B \to C$ y f es sobreyectiva, $g \circ f$ también lo es.

11. ☐ Si $f : A \to B, g : B \to C$ y g es sobreyectiva, $g \circ f$ también lo es.

12. ☐ Si $f : A \to B, g : B \to C$ son tales que f y g son sobreyectivas, $g \circ f$ también lo es.

13. ☐ Si $f : A \to B, g : B \to C$ y f es biyectiva, $g \circ f$ también lo es.

14. ☐ Si $f : A \to B, g : B \to C$ y f es biyectiva, $g \circ f$ es inyectiva.

15. ☐ Si $f : A \to B, g : B \to C$ y f es biyectiva, $g \circ f$ es epiyectiva.

16. ☐ Si $f : A \to B, g : B \to C$ y g es biyectiva, $g \circ f$ también lo es.

17. ☐ Si $f : A \to B, g : B \to C$ y g es biyectiva, $g \circ f$ es inyectiva.

18. ☐ Si $f : A \to B, g : B \to C$ y g es biyectiva, $g \circ f$ es sobreyectiva.

19. ☐ Si $f : A \to B, g : B \to C$ son tales que f y g son biyectivas, $g \circ f$ también lo es.

20. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es inyectiva, g también lo es.

21. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es inyectiva, f también lo es.

22. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es sobreyectiva, g también lo es.

23. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es sobreyectiva, f también lo es.

24. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, g también lo es.

25. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, g es inyectiva.

26. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, g es sobreyectiva.

27. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, f también lo es.

28. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, f es inyectiva.

29. ☐ Si $f : A \to B, g : B \to C$ y $g \circ f$ es biyectiva, f es sobreyectiva.

30. ☐ Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $g \circ f = id_A$.

31. ☐ Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $g \circ f = id_B$.

32. ☐ Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $f \circ g = id_A$.

33. ☐ Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $g = f^{-1}$, luego $f \circ g = id_B$.

34. ☐ Si $f : A \to B, g : B \to A$ son biyectivas, entonces si $f = g^{-1}$, luego $g = f^{-1}$.

35. ☐ Si f es biyectiva, $(f^{-1})^{-1} = f$.

36. ☐ Si f es biyectiva, $(f^{-1})^{-1} = f^{-1}$.

37. ☐ Si $f : A \to B, g : B \to C$ son biyectivas, luego $(f \circ g)^{-1} = f^{-1} \circ g^{-1}$.

38. ☐ Si $f : A \to B, g : B \to C$ son biyectivas, luego $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

39. ☐ Si $f : A \to B, g : B \to C$ son biyectivas, luego $((f \circ g)^{-1})^{-1} = f^{-1} \circ g^{-1}$.

40. ☐ Si $f : A \to B, g : B \to C$ son biyectivas, luego $((f \circ g)^{-1})^{-1} = f \circ g$.

41. ☐ Sea $f : A \to B$, se tiene que f es inyectiva $\Leftrightarrow f(A) = B$.

42. ☐ Sea $f : A \to B$, se tiene que f es inyectiva $\Rightarrow f(A) = B$.

43. ☐ Sea $f : A \to B$, se tiene que f es sobreyectiva $\Leftrightarrow f(A) = B$.

44. ☐ Sea $f : A \to B$, se tiene que f es sobreyectiva $\Rightarrow f(A) = B$.

45. ☐ Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, si $f(A_1) \subseteq f(A_2) \Rightarrow A_1 \subseteq A_2$.

46. ☐ Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, si $A_1 \subseteq A_2 \Rightarrow f(A_1) \subseteq f(A_2)$.

47. ☐ Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

48. ☐ Sea $f : A \to B$ inyectiva y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

49. ☐ Sea $f : A \to B$ y $A_1, A_2 \subseteq A$, entonces $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

50. ☐ Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, si $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$.

51. ☐ Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

52. ☐ Sea $f : A \to B$ y $B_1, B_2 \subseteq B$, $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.

53. ☐ Sea $f : A \to B$, entonces si $A' \subseteq A \Rightarrow A' \subseteq f^{-1}(f(A'))$.

54. ☐ Sea $f : A \to B$, entonces si $B' \subseteq B \Rightarrow f(f^{-1}(B')) \subseteq B'$.

55. ☐ Sea $f : A \to B$, entonces si $B' \subseteq B \Rightarrow B' \subseteq f(f^{-1}(B'))$.

56. ☐ Sea $f : A \to B$ inyectiva, entonces si $A' \subseteq A \Rightarrow A' = f^{-1}(f(A'))$.

57. ☐ Sea $f : A \to B$ sobreyectiva, entonces si $A' \subseteq A \Rightarrow A' = f^{-1}(f(A'))$.

58. ☐ Sea $f : A \to B$ inyectiva, $B' \subseteq B \Rightarrow f(f^{-1}(B')) = B'$.

59. ☐ Sea $f : A \to B$ sobreyectiva, $B' \subseteq B \Rightarrow f(f^{-1}(B')) = B'$.

Guía de Ejercicios

1. Dadas $f : A \to B$, $g : B \to C$ funciones, demuestre las siguientes propiedades enunciadas en las tutorías:

- **(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 sobreyectiva, entonces g es sobreyectiva (f no necesariamente lo es).

2. 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 ej.: $f \circ (h \circ g)$, $f \circ g$, $(h \circ h) \circ g$, etc.), resulta ser una función invertible.
- **(b)** Pruebe que $h \circ g \circ f = g \circ f \circ h = id_{\mathbb{Z}}$, en donde $id_{\mathbb{Z}}$ es la función identidad.
- **(c)** Deducir de lo anterior que $f^{-1} \circ g^{-1} = h$.

3. 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 $(\forall a \in A)\ f(a) = (a, b_0)$.

4. 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)** $d_A \circ f \circ \pi_A$.

5. 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 $(\forall X \subseteq A)\ f(X) = X^c$.

(b) $g : \mathcal{P}(A) \to \mathcal{P}(A)$, dada por $(\forall X \subseteq A)\ g(X) = X \setminus (X^c)$.

(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 $(\forall X \subseteq A)\ h_3(X) = X \triangle B$.

6. Dadas $f : A \to B$, función y $A_1, A_2 \subseteq A$, demuestre las siguientes propiedades enunciadas en las tutorías:

(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) $A_1 \subseteq f^{-1}(f(A_1))$

7. Dadas $f : A \to B$, función y $B_1, B_2 \subseteq B$, demuestre las siguientes propiedades:

(a) $B_1 \subseteq B_2 \Rightarrow f^{-1}(B_1) \subseteq f^{-1}(B_2)$.

(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) $f^{-1}(B_1 \triangle B_2) = f^{-1}(B_1) \triangle f^{-1}(B_2)$.

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. (20 min.) Sean $f, g : \mathbb{R} \to \mathbb{R}$ funciones. Determine explícitamente f y g sabiendo que

$$g \circ f = \frac{3x+2}{9x^2+12x+5} \qquad f^{-1}(x) = \frac{x-2}{3}$$

P2. Sean $f, g : A \to A$ funciones. Probar que si g es biyectiva entonces se tiene que

(a) (15 min.) f es inyectiva $\Leftrightarrow$ $f \circ g$ es inyectiva

(b) (15 min.) f es sobreyectiva $\Leftrightarrow$ $g \circ f$ es sobreyectiva

P3. Sea $A = \{0, 1, 2, 3\}$ y $T : A \to A$ la función definida por $T(0) = 1, T(1) = 2, T(2) = 3, T(3) = 0$. Sea $I = \{h : A \to \mathbb{R} / h$ es función y $h(0) + h(1) + h(2) + h(3) = 0\}$. Dada una función $f : A \to \mathbb{R}$ definimos la función $\bar{f} : A \to \mathbb{R}$ en cada $n \in A$ por $\bar{f}(n) = f \circ T(n) - f(n)$.

(a) (20 min.) Probar que si $f : A \to \mathbb{R}$ es una función de dominio A y recorrido $\mathbb{R}$ entonces $\bar{f} \in I$

(b) (40 min.) Sea $D = \{h : A \to \mathbb{R} / h$ es función y $h(0) = 0\}$. Definimos $\Delta : D \to I$ en cada $f \in D$ por $\Delta(f) = \bar{f}$. Probar que Δ es biyectiva y calcular Δ^{-1}.

P4. Sea $\mathcal{F} = \{h : E \to E / h$ es biyectiva $\}$ y $f \in (F)$

(a) (5 min.) Pruebe que para todo $h \in \mathcal{F}, h \circ f \in \mathcal{F}$

(b) (25 min.) Sea $\varphi_f : (F) \to (F)$ tal que $\varphi_f(h) = h \circ f$. Pruebe que φ_f es biyección.

P5. (15 min.) Sea $E = \{f : \mathbb{R} \to \mathbb{R} / f$ es biyectiva$\}$. Es decir, E contiene a todas las funciones biyectivas de $\mathbb{R}$ en $\mathbb{R}$. Se define la funcion $\xi : E \to E$ tal que para cada $f \in E$, $\xi(f) = f^{-1}$, es decir ξ le asocia a cada función en E su inversa. Sean $f, g \in E$. Probar que $\xi(f \circ g) = \xi(g) \circ \xi(f)$.

P6. (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 $(g \circ f)^{-1}(\mathbb{Z})$

P7. (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

$$f(A) \triangle f(B) = f(A \triangle B)$$

P8. (20 min.) Sea $f : E \to F$ una función y $A, B \subseteq E$. Pruebe que

$$f(B) \setminus f(A) = \phi \Rightarrow f(A \cup B) = f(A)$$

Importante: Visita regularmente `http://www.dim.uchile.cl/~docencia/algebra` para mantenerte al tanto de las novedades del curso.

SEMANA 5: RELACIONES

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones. ▼

4. Relaciones

4.1. Introducción

Definición 4.1 (Relación). *Dados un par de conjuntos no vacíos A y B, llamaremos* ***relación binaria*** *entre A y B, o simplemente* ***relación*** *entre A y B, a un conjunto $\mathcal{R} \subseteq A \times B$.*
Denotaremos $a \mathcal{R} b$ cuando $(a,b) \in \mathcal{R}$, y $a \not\mathcal{R} b$ cuando $(a,b) \notin \mathcal{R}$.

Observemos que, para A y B conjuntos no vacíos, ya conocemos una buena cantidad de relaciones.
Por ejemplo, toda función $f : A \to B$ puede interpretarse como una relación $\mathcal{R} \subseteq A \times B$, donde $a \mathcal{R} b \iff b = f(a)$.

Ejemplos:

1. Tomemos el conjunto $\mathcal{R} = \{(p,n) \in \mathbb{Z} \times \mathbb{N} : |p-n| \leq 5\}$. Éste es una relación entre $\mathbb{Z}$ y $\mathbb{N}$. Diremos que

   "$\mathcal{R}$ es una relación entre $\mathbb{Z}$ y $\mathbb{N}$ dada por ($p \mathcal{R} n \iff |p-n| \leq 5$)"

2. $\leq$ es una relación de $\mathbb{R}$ consigo mismo, interpretando $\leq$ como el conjunto $\{(x,y) \in \mathbb{R} \times \mathbb{R} : x \leq y\}$.

3. En $\mathbb{N} \times \mathbb{N}$, decimos que $a \mid b \iff (\exists k \in \mathbb{N})\ b = k \cdot a$. La relación que estamos simbolizando con la barra vertical $\mid$ se conoce como *divisibilidad*, y decimos que "a divide a b" cuando $a \mid b$. A modo de ejemplo, tenemos que $2 \mid 8$, $7 \mid 21$, $4 \nmid 5$ y $9 \nmid 28$.

4. Para $p, q \in \mathbb{Z}$, definimos la relación *igualdad módulo 3*, que simbolizaremos por $\equiv_3$, por $p \equiv_3 q \iff (\exists k \in \mathbb{Z})\ (p-q) = 3k$. Así, por ejemplo, $8 \equiv_3 11$ y $11 \equiv_3 -1$.

5. Sea P el conjunto de todos los seres humanos, y definimos para $p_1, p_2 \in P$ la relación $p_1 \mathcal{H} p_2 \iff p_1$ es hermano o hermana de p_2.

4.2. Relaciones de un conjunto en si mismo

A continuación nos preocuparemos de las relaciones de un conjunto no vacío A consigo mismo, es decir las relaciones $\mathcal{R} \subseteq A \times A$.
Dada una relación $\mathcal{R}$ en el conjunto A, definimos las siguientes propiedades (al igual que con la inyectividad, sobreyectividad y biyectividad de funciones, estas propiedades pueden ser o no cumplidas por cada relación):

Definición 4.2 (Tipos de relaciones).

- *Diremos que* $\mathcal{R}$ *es* ***refleja*** *si y sólo si*

$$(\forall x \in A)\ x\ \mathcal{R}\ x$$

- *Diremos que* $\mathcal{R}$ *es* ***simétrica*** *si y sólo si*

$$(\forall x, y \in A)\ x\ \mathcal{R}\ y \Rightarrow y\ \mathcal{R}\ x$$

- *Diremos que* $\mathcal{R}$ *es* ***antisimétrica*** *si y sólo si*

$$(\forall x, y \in A)\ (x\ \mathcal{R}\ y \wedge y\ \mathcal{R}\ x) \Rightarrow x = y$$

- *Diremos que* $\mathcal{R}$ *es* ***transitiva*** *si y sólo si*

$$(\forall x, y, z \in A)\ (x\ \mathcal{R}\ y \wedge y\ \mathcal{R}\ z) \Rightarrow x\ \mathcal{R}\ z$$

Observación (Importante): Debemos observar que la simetría y la antisimetría no son propiedades contrapuestas:

Por un lado puede ocurrir que una relación no sea ni simétrica ni antisimétrica, pero también hay relaciones que cumplen ambas propiedades simultáneamente. Estas últimas, sin embargo, no pueden ser muy complejas, pues si $\mathcal{R} \subseteq A \times A$:

$$\mathcal{R} \text{ es simétrica y antisimétrica} \iff (\forall x, y \in A)\ [x\ \mathcal{R}\ y \Rightarrow x = y]$$

Demostración. $\Leftarrow$) Queda como ejercicio para el lector.

$\Rightarrow$) Sean $x, y \in A$ tales que $x\ \mathcal{R}\ y$.
Como $\mathcal{R}$ es simétrica, entonces también $y\ \mathcal{R}\ x$. Así,

$$x\ \mathcal{R}\ y \wedge y\ \mathcal{R}\ x$$

y como $\mathcal{R}$ es antisimétrica, concluimos que $x = y$.

Observemos que si tenemos una relación $\mathcal{R} \subseteq A \times A$ tal que existen elementos $x_0 \neq y_0$ en A tales que $x_0\ \mathcal{R}\ y_0$, entonces $\mathcal{R}$ es o bien simétrica, o bien antisimétrica.

Relaciones de orden

Definición 4.3 (Relación de orden). *Sea* $\mathcal{R}$ *una relación en el conjunto* A*. Diremos que* $\mathcal{R}$ *es una* ***relación de orden*** *en* A*, o simplemente que es un* ***orden en*** A*, si es una relación refleja, antisimétrica y transitiva.*

- Si $\mathcal{R}$ es un orden en A, diremos que a **precede** a b cada vez que $a\ \mathcal{R}\ b$.

- Además, diremos que dos elementos $a, b \in A$ son **comparables** si se cumple que $(a\ \mathcal{R}\ b) \vee (b\ \mathcal{R}\ a)$.

- Si $\mathcal{R}$ es un orden que hace que todo par de elementos sea comparable, entonces diremos que $\mathcal{R}$ es un **orden total**. En caso contrario, diremos que es un **orden parcial**.

Es fácil verificar, entonces, que $\leq$ es un orden total en $\mathbb{R}$.

Ejemplo: Divisibilidad

Recordando la relación de divisibilidad $|$ que ya definimos, tenemos que ésta es un orden parcial en $\mathbb{N}$, pero no es un orden total.

Demostración. Veamos que $|$ cumple las tres propiedades requeridas:

- $|$ es refleja pues para cada $n \in \mathbb{N}$ se tiene que $n = 1 \cdot n$.
- Si $a \mid b$ y $b \mid a$, entonces existen $k, j \in \mathbb{N}$ tal que $b = ka$ y $a = jb$.

  Con esto, $b = kjb$, o equivalentemente $b(1 - kj) = 0$. De modo análogo, obtenemos que $a = jka$, y con ello $a(1 - jk) = 0$. Entonces

  $$a(1 - kj) = b(1 - kj)$$

  Si $kj \neq 1$, entonces podemos dividir por $(1 - kj)$ y concluir que $a = b$.

  Si $kj = 1$, como ambos son elementos de $\mathbb{N}$, tenemos que forzosamente $k = j = 1$ (se puede demostrar por contradicción, queda como ejercicio para el lector). Así, $a = jb = 1 \cdot b = b$.

  En cualquier caso $a = b$, con lo que $|$ resulta ser antisimétrica.

- Supongamos que $a \mid b$ y que $b \mid c$. Entonces, existen $k, j \in \mathbb{N}$ tales que $b = ka$ y $c = jb$. Así, $c = (j \cdot k)a$, por lo que $a \mid c$, y $|$ resulta ser transitiva también.

Concluimos que $|$ es un orden parcial. Finalmente, vemos que $|$ no es orden total pues, por ejemplo, 2 y 3 no son comparables: $2 \nmid 3$ y $3 \nmid 2$.

Relaciones de equivalencia

Definición 4.4 (Relación de equivalencia). *Una relación $\mathcal{R}$ en el conjunto A se llamará* **relación de equivalencia** *si es*

- *Refleja.*
- *Simétrica.*
- *Transitiva.*

Una relación de equivalencia en el fondo define un criterio de semejanza entre los elementos de A.
Por esto, consideraremos a continuación los subconjuntos formados por elementos "equivalentes" para la relación.

Definición 4.5 (Clase de equivalencia). *Dado un elemento $a \in A$, definimos la* clase de equivalencia de a asociada a $\mathcal{R}$ *como el conjunto*

$$\{x \in A : a \ \mathcal{R} \ x\}$$

el cual denotaremos por $[a]_{\mathcal{R}}$.

Ejemplos:

- Un ejemplo sencillo de relación de equivalencia es la igualdad entre números reales.

- Otro ejemplo lo podemos tomar del diccionario español: sea Σ el conjunto de todas las palabras del diccionario español.

  Para $v, w \in \Sigma$ definimos la relación $\approx$ como

  $$v \approx w \iff v \text{ y } w \text{ comienzan con la misma letra.}$$

  Es fácil ver que $\approx$ es una relación de equivalencia en Σ.

  Calculemos en este caso la clase de equivalencia de algunas palabras: la clase $[\text{hola}]_\approx$ es el conjunto de todas las palabras en Σ que comienzan con h, mientras que $[\text{casa}]_\approx$ es el conjunto de todas las palabras que comienzan con c.

  En este ejemplo, notemos que podemos escribir

  $$\Sigma = [\text{ahora}]_\approx \cup [\text{bote}]_\approx \cup [\text{casa}]_\approx \cup \ldots \cup [\text{zorro}]_\approx$$

  Además, se tiene que $[\text{tapa}]_\approx \cap [\text{velero}]_\approx = \emptyset$, y que $[\text{manzana}]_\approx = [\text{menos}]_\approx$.

Veremos que estas últimas propiedades se generalizan a cualquier relación de equivalencia.

Propiedades 6. *Sean $x, y \in A$ y $\mathcal{R}$ una relación de equivalencia definida en A.*

1. $[x]_\mathcal{R} \neq \emptyset$
2. $x \mathcal{R} y \iff [x]_\mathcal{R} = [y]_\mathcal{R}$
3. $x \not\mathcal{R} y \iff [x]_\mathcal{R} \cap [y]_\mathcal{R} = \emptyset$
4. *Como consecuencia de las anteriores,*
   $[x]_\mathcal{R} \neq [y]_\mathcal{R} \iff [x]_\mathcal{R} \cap [y]_\mathcal{R} = \emptyset$

Demostración. Demostraremos (2) y (3).
Para (2):
$\Rightarrow$) Sea a un elemento.

$$\begin{aligned} & a \in [x]_\mathcal{R} \\ \iff \quad & a \mathcal{R} x \quad \text{(def. de clase de equivalencia)} \\ \iff \quad & a \mathcal{R} y \quad \text{(pues } x \mathcal{R} y\text{)} \\ \iff \quad & a \in [y]_\mathcal{R} \quad \text{(def. de clase de equivalencia)} \end{aligned}$$

$\Leftarrow$) Notemos que $x \in [x]_\mathcal{R}$. Como $[x]_\mathcal{R} = [y]_\mathcal{R}$, concluimos que $x \in [y]_\mathcal{R}$. Por definición de clase de equivalencia, obtenemos que $x \mathcal{R} y$.
Para (3):
$\Rightarrow$) Por contrarrecíproca. Como $[x]_\mathcal{R} \cap [y]_\mathcal{R} \neq \emptyset$, tenemos que existe $a \in [x]_\mathcal{R} \cap [y]_\mathcal{R}$. Como $a \in [x]_\mathcal{R}$, tenemos que $a \mathcal{R} x$. Análogamente, tenemos que $a \mathcal{R} y$. Como $\mathcal{R}$ es una relación de equivalencia, en particular es transitiva, y entonces $x \mathcal{R} y$.

$\Leftarrow$) Por contrarrecíproca también. Si $x \mathcal{R} y$, tenemos que $x \in [y]_{\mathcal{R}}$. Como trivialmente $x \in [x]_{\mathcal{R}}$, entonces

$$x \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}}$$

por lo que $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \neq \emptyset$.

Definición 4.6 (Conjunto cuociente). *Al conjunto de todas las clases de equivalencia inducidas sobre A por una relación de equivalencia $\mathcal{R}$ se le llama* conjunto cuociente*, y se denota $A/\mathcal{R}$.*
Éste es un conjunto cuyos elementos son clases de equivalencia, es decir:

$$C \in A/\mathcal{R} \iff (\exists x \in A)\ C = [x]_{\mathcal{R}}$$

Vimos que el conjunto de palabras Σ antes definido podía escribirse como unión de ciertas clases de equivalencia. Éstas eran conjuntos disjuntos entre sí, pues cada uno de ellos contenía a todas las palabras que comenzaban con una letra específica. Esta noción que dice que un conjunto puede ser escrito como unión de otros conjuntos, todos ellos disjuntos, es la de partición.

Definición 4.7 (Partición). *Sea A un conjunto no vacío. Una colección de conjuntos $\{P_1, \ldots, P_n\} \subseteq \mathcal{P}(A)$ se llamará* **partición** *de A si cumple:*

- $(\forall i \in \{1, \ldots, n\})\ P_i \neq \emptyset$
- $(\forall i, j \in \{1, \ldots, n\})\ i \neq j \Rightarrow P_i \cap P_j = \emptyset$
- $A = P_1 \cup P_2 \cup P_3 \cup \ldots \cup P_n$

Consideremos un conjunto no vacío A. Entonces toda relación de equivalencia $\mathcal{R}$ definida sobre A induce en él una partición, la cual está formada por todas las clases de equivalencia de los elementos de A.

También, toda partición $\{P_1, \ldots, P_n\}$ de A induce en él una relación de equivalencia $\mathcal{R}$, la cual está dada por

$$a \mathcal{R} b \iff (\exists i \in \{1, \ldots, n\})\ a \in P_i \wedge b \in P_i.$$

Ejemplo importante: Congruencia módulo
Un tipo de relaciones de equivalencia de particular importancia lo conforman las llamadas relaciones **igualdad módulo** p, de las cuales ya conocemos la igualdad módulo 3.
Sea $p \in \mathbb{N}$, $p \geq 2$. Se define en $\mathbb{Z}$ la relación $\equiv_p$ por

$$x \equiv_p y \iff (\exists k \in \mathbb{Z})\ (x - y) = kp$$

Si $x \equiv_p y$, diremos que x e y son **iguales módulo** p, o que son **congruentes módulo** p. Como ejemplo, tenemos que $13 \equiv_3 7$ pues $13 - 7 = 6 = 2 \cdot 3$, y que $12 \equiv_5 27$, pues $12 - 27 = -15 = -3 \cdot 5$.
Dado un $p \in \mathbb{N}$, $p \geq 2$, $\equiv_p$ resulta ser una relación de equivalencia sobre $\mathbb{Z}$. Así, $\equiv_p$ induce en $\mathbb{Z}$ clases de equivalencia, y al conjunto cuociente $\mathbb{Z}/\equiv_p$ le llamaremos $\mathbb{Z}_p$.
Para trabajar con ella, se necesita el siguiente teorema, llamado teorema de la división euclidiana, que viene de la Teoría de Números:

Teorema 4.1. *Sean $a, b \in \mathbb{Z}$. Existe un único par $q, r \in \mathbb{Z}$ tal que*

$$a = q \cdot b + r \quad \wedge \quad 0 \leq r < |b|$$

Se llama teorema de la división porque su aplicación a un par $a, b \in \mathbb{Z}$ equivale a calcular la división entera $a \div b$. Ésta debe tener un cuociente $q \in \mathbb{Z}$ y un resto $r \in \mathbb{Z}$, el cual debe ser menor que $|b|$.

Propiedad 3. *Se tiene que*

$$\mathbb{Z}_p = \{[0]_p, [1]_p, \ldots, [p-1]_p\}$$

En particular, concluimos que $\mathbb{Z}_p$ tiene exactamente p elementos.

Demostración. Demostraremos esta igualdad mediante dos inclusiones.
$\supseteq$) Recordemos que $\mathbb{Z}_p = \mathbb{Z}/\equiv_p$, es decir que $\mathbb{Z}_p$ es el conjunto de todas las clases de equivalencia $[\cdot]_p$ inducidas por $\equiv_p$ en $\mathbb{Z}$. Como

$$0, 1, \ldots, p-1 \in \mathbb{Z}$$

entonces por definición de conjunto cuociente

$$[0]_p, [1]_p, \ldots, [p-1]_p \in \mathbb{Z}_p$$

$\subseteq$) Sea $C \in \mathbb{Z}_p$. C es una clase de equivalencia, luego existe $x \in \mathbb{Z}$ tal que $C = [x]_p$.

Aplicando el teorema de la división, obtenemos que existen un cuociente $q \in \mathbb{Z}$ y un resto $r \in \mathbb{Z}$ $(0 \leq r \leq p-1)$ tales que

$$x = p \cdot q + r$$

de donde se concluye

$$x - r = p \cdot q$$

lo que significa que

$$x \equiv_p r$$

Gracias a una propiedad que demostramos anteriormente, esto nos dice

$$[x]_p = [r]_p$$

Por lo tanto $C = [r]_p$, y como $0 \leq r \leq p-1$, entonces

$$C \in \{[0]_p, [1]_p, \ldots, [p-1]_p\}$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ Una relación $R \subseteq A \times A, R \neq \phi$ siempre cumple alguna de las siguientes propiedades: R es refleja, R es simétrica, R es antisimétrica, R es transitiva.

2. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x = 2y\}$ es una relación refleja.

3. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x = 2y\}$ es una relación simétrica.

4. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x = 2y\}$ es una relación antisimétrica.

5. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x = 2y\}$ es una relación transitiva.

6. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{N})\}$ es una relación refleja.

7. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{R})\}$ es una relación refleja.

8. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{N})\}$ es una relación simétrica.

9. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{Q})\}$ es una relación simétrica.

10. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{N})\}$ es una relación antisimétrica.

11. ☐ $R = \{(x,y) \in \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} / (\exists k)(\frac{x}{y} = 2k \wedge k \in \mathbb{N})\}$ es una relación transitiva.

12. ☐ $R = \{(x,y) \in \mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} / (\exists k)(\frac{x}{y} \leq 3k \wedge k \in \mathbb{N})\}$ es una relación refleja.

13. ☐ $R = \{(x,y) \in \mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} / (\exists k)(\frac{x}{y} \leq 3k \wedge k \in \mathbb{N})\}$ es una relación simétrica.

14. ☐ $R = \{(x,y) \in \mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} / (\exists k)(\frac{x}{y} \leq 3k \wedge k \in \mathbb{N})\}$ es una relación antisimétrica.

15. ☐ $R = \{(x,y) \in \mathbb{N} \setminus \{0\} \times \mathbb{N} \setminus \{0\} / (\exists k)(\frac{x}{y} \leq 3k \wedge k \in \mathbb{N})\}$ es una relación transitiva.

16. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2\}$ es una relación refleja.

17. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2\}$ es una relación simétrica.

18. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2\}$ es una relación antisimétrica.

19. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2\}$ es una relación transitiva.

20. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in [-r,r] \times [-r,r] / x^2 + y^2 = r^2\}$ es una relación refleja.

21. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in [-r,r] \times [-r,r] / x^2 + y^2 = r^2\}$ es una relación simétrica.

22. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in [-r,r] \times [-r,r] / x^2 + y^2 = r^2\}$ es una relación antisimétrica.

23. ☐ Sea $r \in \mathbb{R}$, $R = \{(x,y) \in [-r,r] \times [-r,r] / x^2 + y^2 = r^2\}$ es una relación transitiva.

24. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2, \quad r \in \mathbb{R}\}$ es una relación refleja.

25. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2, \quad r \in \mathbb{R}\}$ es una relación simétrica.

26. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2, \quad r \in \mathbb{R}\}$ es una relación antisimétrica.

27. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x^2 + y^2 = r^2, \quad r \in \mathbb{R}\}$ es una relación transitiva.

28. ☐ Una relación simétrica nunca es antisimétrica.

29. ☐ Una relación antisimétrica nunca es simétrica.

30. ☐ La $=$ es una relación que es simétrica y antisimétrica a la vez.

31. ☐ La única relación simétrica y antisimétrica a la vez es la igualdad.

32. ☐ No existen relaciones que sean de equivalencia y de orden a la vez.

33. ☐ 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.

34. ☐ 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.

35. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy \geq 0\}$ es una relación refleja.

36. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy \leq 0\}$ es una relación refleja.

37. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy \leq 0\}$ es una relación simétrica.

38. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy \leq 0\}$ es una relación antisimétrica.

39. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy > 0\}$ es una relación transitiva.

40. ☐ $R = \{(x,y) \in \mathbb{Z} \setminus \{0\} \times \mathbb{Z} \setminus \{0\} / xy < 0\}$ es una relación transitiva.

41. ☐ $R = \{(x,y) \in [0,\infty) \times [0,\infty) / x \geq 0\}$ es una relación refleja.

42. ☐ $R = \{(x,y) \in [0,\infty) \times [0,\infty) / x \geq 0\}$ es una relación simétrica.

43. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x \leq 0\}$ es una relación antisimétrica.

44. ☐ $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x \leq 0\}$ es una relación transitiva.

45. ☐ $(-\infty, 0)$ y $[0,\infty)$ son las clases de equivalencia de $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / xy \geq 0\}$

46. ☐ $(-\infty, 0)$ y $(0,\infty)$ son las clases de equivalencia de $R = \{(x,y) \in (\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\}) / xy > 0\}$

47. ☐ $(-\infty, 0)$ y $[0,\infty)$ son las clases de equivalencia de $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / x + y \geq 0\}$

48. ☐ Sea A el conjunto de alumnos de primer a no. La relación en A, dada por $a_1 \mathcal{R} a_2 \Leftrightarrow a_1$ tiene mejor nota que a_2, es una relación de orden.

49. ☐ Sea A el conjunto de alumnos de primer a no. La relación en A, dada por $a_1 \mathcal{R} a_2 \Leftrightarrow a_1$ tiene mejor o igual nota que a_2, es una relación de orden total.

50. ☐ Sea A el conjunto de alumnos de primer a no. La relación en A, dada por $a_1 \mathcal{R} a_2 \Leftrightarrow a_1$ tiene mejor o igual nota que a_2, es una relación de orden parcial.

51. ☐ $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x < y\}$ es una relación de orden total.

52. ☐ $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x < y\}$ es una relación de orden parcial.

53. ☐ Dos clases de equivalencia siempre tienen al menos un elemento en común.

54. ☐ $\{x \in \mathbb{N} / x = 2n, \quad n \in \mathbb{N}\}$ y $\{x \in \mathbb{N} / x = 2n + 1, \quad n \in \mathbb{N}\}$, son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x = 2y\}$

55. ☐ $\{x \in \mathbb{N} / x = 2n, \quad n \in \mathbb{N}\}$ y $\{x \in \mathbb{N} / x = 2n + 1, \quad n \in \mathbb{N}\}$, son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / \frac{x}{y} = 2\}$

56. ☐ $\{x \in \mathbb{N} / x = 2n, \quad n \in \mathbb{N}\}$ y $\{x \in \mathbb{N} / x = 2n + 1, \quad n \in \mathbb{N}\}$, son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / \frac{x}{y} = 2n, \quad n \in \mathbb{N}\}$

57. ☐ $\{x \in \mathbb{N} / x = 2n, \quad n \in \mathbb{N}\}$ y $\{x \in \mathbb{N} / x = 2n + 1, \quad n \in \mathbb{N}\}$, son las clases de equivalencia de $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x - y = 2n, \quad n \in \mathbb{N}\}$

Guía de Ejercicios

1. Estudie si las siguientes relaciones son o no reflejas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

(a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y = ax + b\}$, con $a \neq 0$.

(b) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y = ax + b \wedge y = ax + d\}$, con $a \neq 0, b \neq d$.

(c) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y = ax + b \wedge y = cx + d\}$, con $ac = -1$.

(d) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y \leq ax + b \wedge y \leq cx + d\}$, con $b, d > 0$.

(e) $R = \{(x,y) \in [-r,r] \times [-r,r] / y^2 + x^2 \leq r^2 \wedge |y| \leq \frac{r}{2}\}$, con $r > 0$.

(f) $R = \{(x,y) \in [-\frac{r}{2},\frac{r}{2}] \times [-r,r] / y^2 + x^2 \leq r^2 \wedge |y| \leq \frac{r}{2}\}$, con $r > 0$.

(g) $R = \{(x,y) \in [-\frac{r}{2},\frac{r}{2}] \times [-r,r] / y^2 + x^2 \leq r^2\}$, con $r > 0$.

2. Estudie si las siguientes relaciones son o no simétricas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

(a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y \neq x\}$

(b) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y = x\}$

(c) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y^2 = x^2\}$

(d) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / |y| = x\}$

(e) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / xy = 2k, k \in \mathbb{Z}\}$

(f) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / xy < 0\}$

3. Estudie si las siguientes relaciones son o no antisimétricas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

(a) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y \neq x\}$

(b) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y < x\}$

(c) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / y \geq x\}$

(d) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / |y| = x\}$

(e) $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} / xy = 2k, \text{ para algún } k \in \mathbb{N}\}$

4. Estudie si las siguientes relaciones son o no transitivas. En caso que no lo sean, para demostrarlo, enuncie un contraejemplo.

(a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / y \neq x\}$.

(b) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / |y| \geq x\}$

(c) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / y^2 < x^3\}$

(d) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / xy = 1\}$

(e) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x^y \in \mathbb{Q}\}$

(f) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} / x - y = pk, \text{ para algún } k \in \mathbb{Q}\}$

5. 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) Sea H el conjunto de todos los hombres y M el conjunto de todas las mujeres. Se define $E \subseteq H \times M$ por

$$E = \{(h, m) \in H \times M / h \text{ esta casado con m}\}$$

Es decir, E es el conjunto de todos los matrimonios.
Indicación: En esta parte haga los supuestos de estime convenientes y vea qué pasa si los cambia (por ej., 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.

(1) Sea R_1 la relación definida en E por:
$(h_1, m_1)R_1(h_2, m_2) \Leftrightarrow$ Algún miembro del matrimonio 1 es hermano(a) de algún miembro del matrimonio 2

(2) Sea R_2 la relación definida en E por:
$(h_1, m_1)R_2(h_2, m_2) \Leftrightarrow$ h_1 es hermano(a) de h_2

(3) Sea R_3 la relación definida en E por:
$(h_1, m_1)R_3(h_2, m_2) \Leftrightarrow$ Algún miembro del matrimonio 1 es de mayor o igual estatura que algún miembro del matrimonio 2

(4) Sea R_4 la relación definida en E por:
$(h_1, m_1)R_4(h_2, m_2) \Leftrightarrow$ m_1 es de menor estatura que m_2

(5) Sea R_5 la relación definida en E por:
$(h_1, m_1)R_5(h_2, m_2) \Leftrightarrow$ Las edades del matrimonio 1 suman mas que las edades del matrimonio 2

(6) Sea R_6 la relación definida en E por:
$(h_1, m_1)R_6(h_2, m_2) \Leftrightarrow$ Las edades del matrimonio 1 suman a lo menos la suma de las edades del matrimonio 2

(7) Sea R_7 la relación definida en E por:
$(h_1, m_1)R_7(h_2, m_2) \Leftrightarrow$ Las edades del matrimonio 1 suman lo mismo que las edades del matrimonio 2

(b) $x\mathcal{R}y \Leftrightarrow x^2 + y = y^2 + x$

(c) $(x, y)\mathcal{R}(z, w) \Leftrightarrow x < z \wedge y + w = 2k, k \in \mathbb{N}$

(d) $(x, y)\mathcal{R}(z, w) \Leftrightarrow x + z = y + w$

(e) $(x, y)\mathcal{R}(z, w) \Leftrightarrow x \leq z \wedge y \geq w$

(f) $(x, y)\mathcal{R}(z, w) \Leftrightarrow xw \leq zy$

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. Sobre un conjunto de proposiciones $\mathcal{P}$ lógicas se define la relación $\mathcal{R}$ por

$$p\mathcal{R}q \Leftrightarrow ((p \wedge q) \Leftrightarrow q)$$

Además, para $p, q \in \mathcal{P}$ se dice que $p = q$ si y solo si $p \Leftrightarrow q$.

(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.

P2. Considere el conjunto $A = \mathbb{Z} \times \mathbb{Z}$.Se define la relación $\mathcal{R}$ en A por:

$$(a_1, a_2)\ \mathcal{R}\ (b_1, b_2) \ \Leftrightarrow\ a_1 + a_2 - b_1 - b_2 = 2k \text{ para un cierto } k \in \mathbb{Z}.$$

(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 $f : [(1,0)]_{\mathcal{R}} \to [(0,0)]_{\mathcal{R}}$.

P3. (30 min.) Sea A el conjunto de todas las relaciones binarias en $\mathbb{R}$. Sobre A definamos la relación binaria Ω siguiente:
Sean $R_1, R_2 \in A$, entonces

$$R_1 \Omega R_2 \Leftrightarrow [(\forall x, y \in \mathbb{R})(xR_1y \Rightarrow xR_2y)]$$

Pruebe que Ω es una relación de orden. Muestre además que Ω es de orden parcial en A.

P4. Sea $p \in \mathbb{Z}, p \geq 2$. Se define en $\mathbb{Q}^+ = \{q \in \mathbb{Q} / q > 0\}$ la relación Ω_p por:

$$x\Omega_p y \Leftrightarrow \exists \alpha \in \mathbb{Z}, \frac{x}{y} = p^{\alpha}$$

(a) (20 min.) Demostrar que Ω_p es relación de equivalencia en $\mathbb{Q}^+$.

(b) (10 min.) Describa por extensión $[1]_{\Omega_2}$.

P5. Sea A un conjunto no vacío y $f : A \to A$ una función que satisface la condicion siguiente:

$$\exists n \in \mathbb{N} \setminus \{0\} \text{ tal que } f^{(n)} = id_A.$$

Se define en A la relación R por:

$$xRy \Leftrightarrow \exists k \in \{1, 2, ..., n\} \text{ tal que } f(k)(x) = y.$$

(a) (30 min.) Demuestre que R es relación de equivalencia.

(b) Considere $A = \{0,1\}^3 y f : A \to A$ definida por $f(x_1, x_2, x_3) = (x_2, x_3, x_1)$

(b.1) (10 min.) Pruebe que f satisface la propiedad enunciada.

(b.2) (20 min.) Determine y escriba todas las clases de equivalencia inducidas por R en A.

P6. Sea E un conjunto y $A \neq \phi$ un subconjunto fijo de E. Se define en $\mathcal{P}(E)$ la relación $\mathcal{R}$ por:

$$X\mathcal{R}Y \Leftrightarrow A \cap X = A \cap Y$$

(a) (10 min.) Demuestre que $\mathcal{R}$ es relación de equivalencia.

(b) (15 min.) Demuestre que el conjunto cuociente $\mathcal{P}(E)/\mathcal{R} = \{[X]/X \in \mathcal{P}(A)\}$.

(c) (15 min.) Demuestre que para $X, Y \in \mathcal{P}(A)$ se tiene que $X \neq Y \Rightarrow [X] \neq [Y]$.

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

SEMANA 6: PRINCIPIO DE INDUCCIÓN Y SUMATORIAS

5. Principio de inducción

5.1. Principio de inducción: Primera forma

Una categoría importante de proposiciones y teoremas es la de las propiedades de los números naturales. Aquí tenemos, por ejemplo

$$(\forall n \in \mathbb{N})\ n < 2^n$$

$$(\forall n \in \mathbb{N})\ (n \text{ es primo} \wedge n \neq 2) \Rightarrow n \text{ es impar}$$

$$(\forall n \geq 1)\ 3^{2n+1} + 2^{n+2} \text{ es divisible por } 7$$

En general, si $p(n)$ es una proposición cuya variable libre n pertenece a $\mathbb{N}$, las distintas formas del **principio de inducción** nos proporcionan proposiciones equivalentes a la proposición

$$(\forall n \geq n_0)\ p(n)$$

Estas formas alternativas nos facilitarán en muchos casos obtener una demostración de la propiedad buscada.

Definición 5.1 (Principio de inducción, primera forma). *Consideremos la proposición*

$$(\forall n \geq n_0)\ p(n)$$

donde $n_0 \in \mathbb{N}$ es un número natural fijo.
La primera forma del principio de inducción nos dice que esta proposición es equivalente a

$$p(n_0) \wedge [(\forall n \geq n_0)\ p(n) \Rightarrow p(n+1)]$$

Observemos los siguientes ejemplos:

Proposición 5.1. *Demostrar que*

$$(\forall n \in \mathbb{N}) \quad 3^{2n+1} + 2^{n+2} \text{ es divisible por } 7$$

Demostración. El caso base es $n = 0$. Aquí, tenemos que demostrar que

$$3^{2\cdot 0+1} + 2^{0+2} \text{ es divisible por } 7$$

Pero esto es verdadero, pues $3^{2\cdot 0+1} + 2^{0+2} = 3 + 4 = 7$.
Supongamos ahora que tenemos un $n \in \mathbb{N}$ tal que se cumple la propiedad, es decir que $3^{2n+1} + 2^{n+2}$ es divisible por 7. Con esta información, a la cual llamamos **hipótesis inductiva**, tenemos que demostrar que $3^{2(n+1)+1} + 2^{(n+1)+2}$ es también divisible por 7.
Gracias a la hipótesis inductiva, tenemos que existe un $k \in \mathbb{N}$ tal que $3^{2n+1}+2^{n+2} = 7k$. Entonces:

$$\begin{aligned} 3^{2(n+1)+1} + 2^{(n+1)+2} &= 3^{2n+3} + 2^{n+3} \\ &= 9 \cdot 3^{2n+1} + 2 \cdot 2^{n+2} \\ &= (7 \cdot 3^{2n+1} + 2 \cdot 3^{2n+1}) + 2 \cdot 2^{n+2} \end{aligned}$$

donde esta descomposición la hacemos de modo de poder factorizar el término $3^{2n+1} + 2^{n+2}$.
Así, continuamos desarrollando

$$\begin{aligned} 3^{2(n+1)+1} + 2^{(n+1)+2} &= 7 \cdot 3^{2n+1} + 2 \cdot (3^{2n+1} + 2^{n+2}) \\ &= 7 \cdot 3^{2n+1} + 2 \cdot 7k \\ &= 7 \cdot \underbrace{(3^{2n+1} + 2k)}_{\in \mathbb{N}} \end{aligned}$$

por lo que concluimos que $3^{2(n+1)+1}+2^{(n+1)+2}$ es divisible por 7. Gracias al principio de inducción, la propiedad en cuestión es cierta.

Proposición 5.2. *Demostrar que*

$$(\forall n \geq 1)\ 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

Demostración. El caso base a demostrar en esta ocasión es $n = 1$. Aquí, tenemos que demostrar que

$$1 = \frac{1 \cdot (1+1)}{2}$$

lo que es cierto.
Supongamos ahora que la propiedad vale para algún $n \geq 1$ (hipótesis inductiva). Debemos demostrar que la propiedad también es cierta para $n + 1$. Es decir, que

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

En efecto:

$$\begin{aligned} 1 + 2 + \ldots + (n+1) &= 1 + 2 + \ldots + n + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

y se concluye la veracidad de la propiedad gracias al principio de inducción.

5.2. Principio de inducción: Segunda forma

La segunda forma del principio de inducción nos dice:

Definición 5.2 (Principio de inducción, segunda forma). *La proposición*

$$(\forall n \geq n_0)\ p(n)$$

es equivalente a

$$p(n_0) \wedge \Big[(\forall n > n_0)\ [p(n_0) \wedge \ldots \wedge p(n-1) \Rightarrow p(n)]\Big]$$

Como ejemplo de la aplicación de esta forma del principio de inducción, recordemos que los números compuestos son los números naturales mayores que 1 que poseen un divisor distinto de 1 y de sí mismos, es decir, si $n \geq 2$:

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

Recordemos también que los números primos son los que no son compuestos.

Ejemplo:

Proposición 5.3. *Todo número natural $n \geq 2$ posee al menos un divisor que es un número primo. Es decir,*

$$(\forall n \geq 2)(\exists p \text{ número primo})\ p \mid n$$

Demostración. Utilizaremos segunda forma de inducción. El caso base es $n = 2$, para el cual observamos que $p = 2$ es un número primo tal que $p \mid n$.

Hagamos ahora el paso inductivo: Sea $n > 2$, y supongamos que para todo valor $k = 2, 3, \ldots, n-1$ se tiene que k posee un divisor primo. Separamos por casos:

- Si n es primo, entonces $p = n$ es un número primo tal que $p \mid n$.
- Si n no es primo, entonces existe un natural $d \in \{2, \ldots, n-1\}$ tal que $d \mid n$. Por hipótesis inductiva y notando que $d < n$, entonces existe un número primo p tal que $p \mid d$.

  Tenemos entonces que $p \mid d$ y $d \mid n$, y gracias a que $\mid$ es una relación transitiva, obtenemos que $p \mid n$.

Definición 5.3 (Fórmulas de recurrencia). *Consideremos el siguiente set de igualdades, al cual llamaremos* **recurrencia***:*

$$\begin{aligned} x_0 &= a \\ x_{n+1} &= f(x_0, \ldots, x_n) \quad (\forall n \geq 0) \end{aligned}$$

Las recurrencias nos permitirán una forma alternativa de definir secuencias de números, como por ejemplo

$$\begin{aligned} x_0 &= 2 \\ x_{n+1} &= 2 + x_n \quad (\forall n \geq 0) \end{aligned}$$

define la secuencia $2, 4, 6, 8, 10, \ldots$ de números pares positivos.
Una cualidad importante de las fórmulas de recurrencia es que son altamente compatibles con las demostraciones que utilizan principio de inducción. Por ejemplo, consideremos la fórmula de recurrencia

$$\begin{aligned} x_0 &= 1 \\ x_{n+1} &= 1 + \left(\frac{x_n}{2}\right)^2 \quad (\forall n \geq 0) \end{aligned}$$

Demostraremos que $(\forall n \in \mathbb{N})\ x_n \leq 2$.

DEMOSTRACIÓN. Lo haremos utilizando primera forma de inducción. El caso base resulta ser cierto pues corresponde a demostrar que $x_0 \leq 2$ (recordemos que $x_0 = 1$). Supongamos ahora que para algún $n \in \mathbb{N}$ se tiene que $x_n \leq 2$. Se tiene, entonces, que

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

con lo que $x_{n+1} \leq 2$, y se concluye la demostración.

Consideremos la secuencia de números definida por la recurrencia

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_{n+2} &= f_{n+1} + f_n \quad (\forall n \in \mathbb{N}) \end{aligned}$$

la cual se llama secuencia de **números de Fibonacci**. Sus primeros términos son

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_3 = f_2 + f_1 = 1 + 1 &= 2 \\ f_4 = f_3 + f_2 = 2 + 1 &= 3 \\ f_5 = f_4 + f_3 = 3 + 2 &= 5 \\ f_6 = f_5 + f_4 = 5 + 3 &= 8 \\ &\vdots \end{aligned}$$

Observación: Los números de Fibonacci están relacionados con muchos elementos de la naturaleza. Visita `http://es.wikipedia.org/wiki/Sucesi%C3%B3n_de_Fibonacci`, para más detalles.

Ejemplo: Números de Fibonacci

Entre muchas propiedades que cumplen, demostraremos la siguiente:

Proposición 5.4.

$$(\forall n \geq 1)\ f_{4n} \textit{ es divisible por } 3$$

DEMOSTRACIÓN. La demostraremos usando primera forma de inducción. El caso base es $n = 1$, en el cual tenemos que probar que f_4 es divisible por 3. Esto es directo, pues como ya vimos, $f_4 = 3$.
Para el paso inductivo, supongamos que f_{4n} es divisible por 3 para algún $n \geq 1$. Existe, entonces, un $k \in \mathbb{N}$ tal que $f_{4n} = 3k$. Debemos demostrar que

$$f_{4(n+1)} \text{ es divisible por } 3$$

Desarrollemos este término, utilizando la fórmula de recurrencia que cumplen

los números de Fibonacci:

$$\begin{aligned} f_{4(n+1)} &= f_{4n+4} \\ &= f_{4n+3} + f_{4n+2} \\ &= (f_{4n+2} + f_{4n+1}) + (f_{4n+1} + f_{4n}) \\ &= f_{4n+2} + 2f_{4n+1} + f_{4n} \\ &= (f_{4n+1} + f_{4n}) + 2f_{4n+1} + f_{4n} \\ &= 3f_{4n+1} + 2f_{4n} \\ &= 3f_{4n+1} + 2 \cdot 3k \\ &= 3(f_{4n+1} + 2k) \end{aligned}$$

con lo que $f_{4(n+1}$ también es divisible por 3, que era lo que deseábamos.

6. Sumatorias

6.1. Introducción

Sea $a_0, a_1, a_2, \ldots, a_n$ una secuencia de números reales. En esta sección estudiaremos propiedades y métodos de cálculo para su suma

$$a_0 + a_1 + a_2 + \ldots + a_n$$

Introduciremos para este efecto una notación especial:

$$a_0 + a_1 + a_2 + \ldots + a_n = \sum_{k=0}^{n} a_k$$

Al símbolo $\sum$ le llamaremos **sumatoria**.
Más generalmente:

Definición 6.1 (Sumatoria). *Si $a_M, a_{M+1}, \ldots, a_N$ es una secuencia de números reales, definimos su sumatoria por recurrencia:*

$$\begin{aligned} \sum_{k=M}^{M} a_k &= a_M \\ \sum_{k=M}^{n} a_k &= a_n + \sum_{k=M}^{n-1} a_k \quad (\forall n = M+1, \ldots, N) \end{aligned}$$

En este capítulo estudiaremos propiedades y métodos de cálculo para sumatorias de diversos tipos.
La sumatoria cumple la siguiente lista de propiedades:

Proposición 6.1. *1. Suma de la secuencia constante igual a 1.*

$$\sum_{k=I}^{J} 1 = (J - I + 1)$$

2. Sea $\lambda \in \mathbb{R}$, y sean $(a_k)_{k=1}^n$, $(b_k)_{k=1}^n$ dos secuencias.

2.1 *Factorización de constantes.*

$$\sum_{k=I}^{J} \lambda \cdot a_k = \lambda \cdot \sum_{k=I}^{J} a_k$$

2.2 *Separación de una suma.*

$$\sum_{k=I}^{J} (a_k + b_k) = \sum_{k=I}^{J} a_k + \sum_{k=I}^{J} b_k$$

3. Traslación del índice, si $s \in \mathbb{N}$.

$$\sum_{k=I}^{J} a_k = \sum_{k=I+s}^{J+s} a_{k-s}$$

4. Separación en dos sumas, si $I \leq L < J$.

$$\sum_{k=I}^{J} a_k = \sum_{k=I}^{L} a_k + \sum_{k=L+1}^{J} a_k$$

5. Propiedad telescópica.

$$\sum_{k=I}^{J} (a_k - a_{k+1}) = a_I - a_{J+1}$$

Demostración. Demostraremos (1) y (6).
Para (1): Lo haremos por inducción sobre $J \geq I$.
Caso base $J = I$: debemos demostrar que

$$\sum_{k=I}^{I} 1 = (I - I + 1)$$

lo cual es directo, pues ambos lados valen 1.
Supongamos ahora que $\sum_{k=I}^{J} 1 = (J - I + 1)$. Entonces

$$\sum_{k=I}^{J+1} 1 = 1 + \sum_{k=I}^{J} 1 = 1 + (J - I + 1) = (J + 1) - I + 1$$

Para (6): Nuevamente por inducción sobre $J \geq I$.
Si $J = I$, el resultado se reduce a demostrar que

$$\sum_{k=I}^{I} (a_k - a_{k+1}) = a_I - a_{I+1}$$

lo cual es directo gracias a la definición de sumatoria.
Supongamos ahora que $\sum_{k=I}^{J} (a_k - a_{k+1}) = a_I - a_{J+1}$. Entonces

$$\sum_{k=I}^{J+1} (a_k - a_{k+1}) = (a_{J+1} - a_{J+2}) + \sum_{k=I}^{J} (a_k - a_{k+1}) = (a_{J+1} - a_{J+2}) + (a_I - a_{J+1}) = a_I - a_{J+2}$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \in \mathbb{N})[p(n) \Rightarrow p(n+1)]$ son verdaderas.

2. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0) \wedge (\forall n \in \mathbb{N})[p(n) \Rightarrow p(n+1)]$ es verdadera.

3. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0) \vee (\forall n \in \mathbb{N})[p(n) \Rightarrow p(n+1)]$ es verdadera.

4. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \in \mathbb{N})[p(n+1) \Rightarrow p(n)]$ son verdaderas.

5. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \in \mathbb{N})[p(n) \Rightarrow p(2n)]$ son verdaderas.

6. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \in \mathbb{N})[p(2n) \Rightarrow p(2n+1)]$ son verdaderas.

7. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0), (\forall n \in \mathbb{N})[p(2n) \Rightarrow p(2n+1)]$ y $(\forall n \geq 1)[p(2n-1) \Rightarrow p(2n)]$ son verdaderas.

8. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0), \{(\forall n \in \mathbb{N})[p(2n) \Rightarrow p(2n+1)] \vee (\forall n \geq 1)[p(2n-1) \Rightarrow p(2n)]\}$ son verdaderas.

9. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \geq 1)[p(n-1) \Rightarrow p(n)]$ son verdaderas.

10. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \geq 1)[p(n-1) \Rightarrow p(n+1)]$ son verdaderas.

11. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0), p(1) \wedge ... \wedge p(n)$ son verdaderas para algún $n \in \mathbb{N}$.

12. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \geq 1)[(p(0) \wedge ... \wedge p(n-1) \wedge p(n)) \Rightarrow p(n+1)]$ son verdaderas.

13. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \geq 1)[(p(0) \wedge ... \wedge p(n-1)) \Rightarrow p(n+1)]$ son verdaderas.

14. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \geq 1)[(p(0) \wedge ... \wedge p(n-1)) \Rightarrow p(n)]$ son verdaderas.

15. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n > k)[p(k) \wedge ... \wedge p(n-1) \Rightarrow p(n)]$ son verdaderas para algún $k \in \mathbb{N}$.

16. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $(\forall n > k)[p(k) \wedge ... \wedge p(n-1) \Rightarrow p(n)]$ es verdadera para algún $k \in \mathbb{N}$.

17. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(k) \wedge ... \wedge p(n)$ es verdadera para algunos $k, n \in \mathbb{N}$.

18. ☐ Una proposición lógica $(\forall n \in \mathbb{N})p(n)$ es verdadera ssi $p(0)$ y $(\forall n \in \mathbb{N})[p(n) \Leftrightarrow p(n+1)]$ son verdaderas.

19. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda a_i = \lambda \sum_{i=0}^{N} a_i$.

20. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = \lambda + \sum_{i=0}^{N} a_i$.

21. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = (N+1)\lambda + \sum_{i=0}^{N} a_i$.

22. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales y $\lambda \in \mathbb{R}$, se tiene que $\sum_{i=0}^{N} \lambda + a_i = N\lambda + 1 + \sum_{i=0}^{N} a_i$.

23. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=1}^{N+1} a_{i-1}$.

24. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=2}^{N+3} a_{i-2}$.

25. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales y $N \geq 1$ par, se tiene que $\sum_{i=0}^{N} a_i = \sum_{i=0}^{N/2} a_{2i} + \sum_{i=0}^{\frac{N}{2}-1} a_{2i+1}$.

26. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N}(a_i + b_i) = \sum_{i=1}^{N} a_i + \sum_{j=1}^{N} b_j$.

27. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N}(a_i + b_i) = \sum_{i=1}^{N} \left(a_i + \sum_{j=1}^{N} b_j\right)$.

28. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N}(a_i + b_i) = \sum_{i=1}^{N} \left(-N + a_i + \sum_{j=1}^{N} b_i\right)$.

29. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=j}^{N} a_i = \sum_{j=i}^{N} a_j$.

30. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N} a_j$.

31. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N-1}(a_j - a_N)$.

32. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \sum_{j=0}^{N-1}(a_j + a_N)$.

33. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \left(\sum_{j=0}^{N-1} a_j\right) + a_N$.

34. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=0}^{N} a_i = \left(\sum_{j=0}^{N-1} a_j\right) - a_N$.

35. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N} a_i - a_{i-1} = a_N - a_0$.

36. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N} a_i - a_{i-1} = a_0 - a_N$.

37. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N} a_i - (a_i - 1) = a_N - a_0$.

38. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N}(a_i+1)-a_i = a_{N+1}-a_1$.

39. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N} a_{i-1}-a_i = a_N-a_0$.

40. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=1}^{N} a_{i-1}-a_i = a_0-a_N$.

41. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=5}^{N} a_{i-1}-a_i = a_5-a_N$.

42. ☐ Sea $(a_n)_{n\geq 0}$ una secuencia de términos reales, se tiene que $\sum_{i=5}^{N} a_{i-1}-a_i = a_4-a_N$.

Guía de Ejercicios

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

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

(b) $\forall n \geq 1, \quad 3^{2n+1} + 2^{n+2}$ es divisible por 7.

(c) $\forall n \geq 1, \quad n^3 + 5n$ es divisible por 6.

(d) $\forall n \geq 1, \quad 5^{2m+1} + 7^{2m+1}$ es divisible por 6.

(e) $\forall n \geq 1, \quad (x-y)$ divide a $x^n - y^n$.

2. Demuestre las siguientes propiedades usando inducción.

(a) $\forall n \in \mathbb{N}, \quad \sum_{k=1}^{2n} (-1)^k (2k+1) = \alpha n$, y determine el valor de la constante α.

(b) $\forall n \in \mathbb{N}, \quad 1 + \frac{1}{4} + \frac{1}{9} + ... + \frac{1}{n^2} \leq 2 - \frac{1}{n}$.

(c) $\forall n \geq 1, \quad \sum_{i=1}^{n} i^2 = \frac{n(2n+1)(n+1)}{6}$.

(d) $\forall n \geq 1, \quad \sum_{i=1}^{n} i = \frac{n^2+n}{2}$.

3. Resuelva los siguiente problemas

(a) $\forall n \in \mathbb{N}$, demuestre que el producto de n números naturales mayores estrictos que uno y no necesariamente consecutivos es mayor estricto que n.

(b) $\forall n \in \mathbb{N}$, demuestre que si tiene n rectas en el plano, de modo tal que no existen rectas paralelas y además la intersección entre ellas es dos a dos (es decir, no existen tres rectas que se corten en el mismo punto), entonces el total de regiones formadas es $(\sum_{j=0}^{n} j) + 1$.

(c) $\forall n \in \mathbb{N}$, demuestre que n puntos sobre una recta generan $n+1$ segmentos.

4. Encuentre el valor de las siguientes sumatorias. (Sin usar inducción).

(a) $\displaystyle\sum_{i=0}^{n} i + i^2$.

(b) $\displaystyle\sum_{i=0}^{n} (i-1)^2 - i^2$.

(c) $\displaystyle\sum_{i=1}^{n} \text{sen}(i) - \text{sen}(i+1)$.

(d) $\displaystyle\sum_{i=1}^{n} \cos(i+2) + \cos(i) - \cos(i+1) - \cos(i-1)$.

(e) $\displaystyle\sum_{i=1}^{n} \frac{i}{i^2+2i+1} - \frac{i-1}{i^2}$.

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. (30 min.) Probar que para todo natural mayor o igual que 1 se tiene $\sum_{k=1}^{n+1} \frac{1}{n+k} \leq \frac{5}{6}$.

P2. (20 min.) Probar por inducción que para $n \geq 1$, $2 \cdot 7^n + 3 \cdot 5^n - 5$ es divisible por 24.

P3. (20 min.) Demuestre que $(\forall n \geq 10) n^3 < 2^n$.

P4. Consideremos la siguiente sucesión $\{a(n)\}_{n\geq 1}$ definida por recurrencia.

$$a(2) = a(1) = 1$$

y sea

$$a(n) = 3[a(n-1) + a(n-2)] + 1$$

Queremos probar que $a(3n) + a(3n+1)$ es divisible por 32.

(a) (20 min.) Pruebe usando inducción que $a(3n+2) - 1$ es divisible por 2.

(b) (20 min.) Pruebe usando inducción que $3a(3n+1) + 5$ es divisible por 8.

(c) (20 min.) Pruebe usando inducción que $a(3n) + a(3n+1)$ es divisible por 32.

P5. Se define $H_n = \sum_{i=1}^{n} \frac{1}{i}, \quad \forall n \geq 1$

a) (10 min.) Demuestre usando inducción que

$$H_{2^k} \leq 1 + k \quad \forall k \in \mathbb{N}$$

b) (20 min.) Demuestre usando inducción que

$$\sum_{i=1}^{n} H_i = (n+1)H_n - n \quad \forall n \geq 1$$

P6. (20 min.) Demuestre usando inducción que:

$$(1+x)(1+x^2)(1+x^{2^2})(1+x^{2^3})...(1+x^{2^{n-1}}) = \frac{x^{2^n}-1}{x-1} \qquad \forall n \geq 1, x \neq 1$$

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

6.2. Progresiones aritméticas

Definición 6.2 (Progresión aritmética). *Es una sumatoria del tipo*

$$\sum_{k=0}^{n}(A+kd)$$

es decir, donde $a_k = A + kd$*, para valores* $A, d \in \mathbb{R}$*.*

Utilizando las propiedades de sumatoria, obtenemos que esta suma es igual a

$$A \cdot \sum_{k=0}^{n} 1 + d \cdot \sum_{k=0}^{n} k$$

Nos basta, entonces, calcular la sumatoria

$$\sum_{k=0}^{n} k$$

Para ello utilizaremos el método de Gauss: como la suma en $\mathbb{R}$ es conmutativa, entonces

$$S = \sum_{k=0}^{n} k$$

puede ser calculado de las dos formas siguientes

$$\begin{aligned} \mathrm{S} &= 0 + 1 + 2 + \ldots + (\mathrm{n}\text{-}1) + \mathrm{n} \\ \mathrm{S} &= \mathrm{n} + (\mathrm{n}\text{-}1) + (\mathrm{n}\text{-}2) + \ldots + 1 + 0 \end{aligned}$$

Si sumamos estas dos igualdades, obtenemos

$$\begin{aligned} \mathrm{S} &= 0 + 1 + 2 + \ldots + (n-1) + n \\ \mathrm{S} &= n + (n-1) + (n-2) + \ldots + 1 + 0 \\ \hline 2S &= n + n + n + \ldots + n + n \end{aligned}$$

Como cada suma posee $(n+1)$ sumandos, obtenemos que

$$S = \frac{n(n+1)}{2}$$

Proposición 6.2. *Si* $n \geq 0$*,*

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

DEMOSTRACIÓN. Por inducción sobre $n \geq 0$.
Caso $n = 0$: Hay que demostrar que

$$\sum_{k=0}^{0} k = \frac{0 \cdot 1}{2}$$

lo cual es directo pues ambos lados valen 0.
Supongamos que la fórmula vale para algún $n \geq 0$. Entonces

$$\begin{aligned}
\sum_{k=0}^{n+1} k &= (n+1) + \sum_{k=0}^{n} k \\
&= (n+1) + \frac{n(n+1)}{2} \quad \text{(Aquí aplicamos la hipótesis inductiva.)} \\
&= \frac{(n^2+n) + 2(n+1)}{2} \\
&= \frac{n^2+3n+2}{2} = \frac{(n+1)(n+2)}{2}
\end{aligned}$$

con lo que completamos la demostración.

Es importante notar que

$$\sum_{k=0}^{n} k = 0 + \sum_{k=1}^{n} k = \sum_{k=1}^{n} k$$

por lo que es irrelevante si la suma se considera desde $k = 0$ o desde $k = 1$.

También, notemos que si $1 \leq n_1 \leq n_2$ son números naturales, entonces

$$\sum_{k=n_1}^{n_2} k = \sum_{k=0}^{n_2} k - \sum_{k=0}^{n_1-1} k = \frac{n_2(n_2+1)}{2} - \frac{(n_1-1)n_1}{2} = \frac{(n_1+n_2)(n_2-n_1+1)}{2}$$

por lo que sabemos calcular esta suma entre cualquier par de números.

Finalmente, volviendo a la progresión aritmética, podemos ahora dar su fórmula explícita:

Proposición 6.3 (Fórmula progesión aritmética).

$$\sum_{k=0}^{n} (A + kd) = A(n+1) + d\frac{n(n+1)}{2}$$

6.3. Progresiones geométricas

Definición 6.3 (Progresión geométrica). *Es una sumatoria del tipo*

$$\sum_{k=0}^{n} Ar^k$$

es decir, donde $a_k = Ar^k$, para valores $A, r \in \mathbb{R}$.

Supongamos que $r \neq 1$. El caso $r = 1$ es muy sencillo, y queda como ejercicio para el lector.
Similarmente a como procedimos antes, podemos decir que esta suma equivale a

$$A \cdot \sum_{k=0}^{n} r^k$$

por lo que basta calcular esta última sumatoria.

Denotemos

$$S = \sum_{k=0}^{n} r^k$$

Se tiene entonces que

$$r \cdot S = \sum_{k=0}^{n} r^{k+1}$$

por lo que

$$S - r \cdot S = \sum_{k=0}^{n} (r^k - r^{k+1})$$

$$S - r \cdot S = \sum_{k=0}^{n} (r^k - r^{k+1})$$

Reconocemos en esta última igualdad una suma telescópica, la cual vale $r^0 - r^{n+1}$.
Por lo tanto

$$S(1 - r) = 1 - r^{n+1}$$

y gracias a que $r \neq 1$ se obtiene la fórmula

Propiedad 4. *Si $n \geq 0$ y $r \neq 1$,*

$$\sum_{k=0}^{n} r^k = \frac{1 - r^{n+1}}{1 - r}$$

Queda propuesto al lector demostrar por inducción esta propiedad.
Nuevamente es posible calcular esta suma entre cualquier par de números. Si $1 \leq n_1 \leq n_2$, entonces

$$\sum_{k=n_1}^{n_2} r^k = \sum_{k=0}^{n_2} r^k - \sum_{k=0}^{n_1-1} r^k = \frac{1 - r^{n_2+1}}{1 - r} - \frac{1 - r^{n_1}}{1 - r} = \frac{r^{n_1} - r^{n_2+1}}{1 - r}$$

Así, volviendo al caso de la progresión geométrica, obtenemos que ésta cumple la fórmula

Proposición 6.4. *Fórmula progresión geométrica Si $r \neq 1$,*

$$\sum_{k=0}^{n} Ar^k = \frac{A(1 - r^{n+1})}{1 - r}$$

6.4. Algunas sumas importantes

Veamos a continuación algunas sumas importantes que podemos calcular usando lo conocido.

Propiedad 5. *Si $n \geq 0$,*

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Demostración. Queda propuesto como ejercicio, demostrar esta propiedad usando inducción.
Aquí lo haremos directamente, notando que para cualquier $k \in \{0, \ldots, n\}$ se tiene que

$$(k+1)^3 = k^3 + 3k^2 + 3k + 1.$$

Por ende, tendremos la siguiente igualdad

$$\sum_{k=0}^{n} (k+1)^3 = \sum_{k=0}^{n} k^3 + 3k^2 + 3k + 1.$$

Y aplicando propiedades de las sumas, obtenemos:

$$\begin{aligned}\sum_{k=0}^{n} (k+1)^3 &= \sum_{k=0}^{n} k^3 + \sum_{k=0}^{n} 3k^2 + \sum_{k=0}^{n} 3k + \sum_{k=0}^{n} 1 \\ &= \sum_{k=0}^{n} k^3 + 3\sum_{k=0}^{n} k^2 + 3\sum_{k=0}^{n} k + \sum_{k=0}^{n} 1\end{aligned}$$

Despejamos entonces el valor de la suma buscada, obteniendo:

$$\begin{aligned}\sum_{k=0}^{n} k^2 &= \frac{1}{3}\left(\sum_{k=0}^{n} (k+1)^3 - \sum_{k=0}^{n} k^3 - 3\sum_{k=0}^{n} k - \sum_{k=0}^{n} 1\right) \\ &= \frac{1}{3}\Big(\underbrace{\sum_{k=0}^{n} ((k+1)^3 - k^3)}_{(1)} - 3\underbrace{\sum_{k=0}^{n} k}_{(2)} - \underbrace{\sum_{k=0}^{n} 1}_{(3)}\Big).\end{aligned}$$

Y todos los términos en el lado derecho se pueden calcular:

- La suma (1), por propiedad telescópica,

$$\sum_{k=0}^{n} ((k+1)^3 - k^3) = (n+1)^3 - 0 = (n+1)^3.$$

- La suma (2), por la propiedad vista para progresiones aritméticas,

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}.$$

- La suma (3) por propiedad vista en la tutoría pasada,

$$\sum_{k=0}^{n} 1 = n + 1.$$

En resumen, tenemos que:

$$\begin{aligned}\sum_{k=0}^{n} k^2 &= \frac{1}{3}\left((n+1)^3 - \frac{3n(n+1)}{2} - (n+1)\right)\\ &= \frac{(n+1)}{3}\left(2n^2+2n+1-\frac{3n}{2}-1\right)\\ &= \frac{(n+1)}{3}\left(n^2+\frac{n}{2}\right)\\ &= \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

Concluyendo el resultado.

Otra suma importante, del mismo tipo que la anterior es

Propiedad 6. *Si $n \geq 0$,*

$$\sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Demostración. La demostración queda propuesta como ejercicio, tanto usando inducción como de forma directa.
Para probarlo directamente, se usa la misma técnica anterior, o sea se calcula $(k+1)^4$.

7. Teorema del binomio de Newton

7.1. Coeficientes binomiales

Consideremos la siguiente fórmula de recurrencia:

$$\begin{aligned} f_0 &= 1\\ f_n &= n \cdot f_{n-1} \quad \text{si } n \geq 1\end{aligned}$$

Definición 7.1 (Factorial). *Llamaremos* **factorial** *de n (denotado $n!$) al valor f_n.*

Por ejemplo, el factorial de 4 es

$$4! = 4 \cdot 3! = 4 \cdot 3 \cdot 2! = 4 \cdot 3 \cdot 2 \cdot 1! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 24$$

Los números factoriales poseen la siguiente interpretación en el contexto de armar combinaciones: sea $k \leq n$. Entonces

$$\frac{n!}{(n-k)!}$$

corresponde a la cantidad de k-tuplas que se puede formar a partir de un conjunto de n elementos, SIN repetirlos.
Por ejemplo, si $A = \{a, b, c, d\}$, ¿cuántos pares ordenados (2-tuplas) distintos podemos formar con sus elementos, sin repetirlos?

$$\begin{array}{cccc} (a,b) & (b,a) & (c,a) & (d,a) \\ (a,c) & (b,c) & (c,b) & (d,b) \\ (a,d) & (b,d) & (c,d) & (d,c) \end{array} \quad \longrightarrow 12 \text{ combinaciones, y } 12 = \tfrac{4!}{(4-2)!}$$

Continuando con la interpretación combinatorial, sea $k \leq n$. Definimos

Definición 7.2 (Coeficiente binomial). *Se define*

$$\binom{n}{k}$$

(se lee "n sobre k") como el número de subconjuntos de tamaño k que posee un conjunto de tamaño n.

¿Cuánto vale $\binom{n}{k}$?
Observemos que por cada subconjunto de tamaño k de un conjunto de n elementos, podemos formar varias k-tuplas: pensando en el ejemplo de $A = \{a, b, c, d\}$, a partir del subconjunto $\{a, c\}$ podemos formar los pares ordenados (a, c) y (c, a).

El número de k-tuplas que se pueden formar a partir de un conjunto de tamaño n será, entonces, el número de subconjuntos de tamaño k que éste posea, pero para considerar los posibles reordenamientos que hacen diferentes a las tuplas, necesitamos multiplicar por la cantidad de formas en que es posible ordenar un conjunto de k elementos: este último valor es $k!$. Por lo tanto, el número de k-tuplas que se puede formar es

$$\binom{n}{k} \cdot k!$$

por lo que

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

Propiedades 7. *Si $0 \leq k \leq n$,*

1. $\binom{n}{0} = 1, \binom{n}{1} = n$
2. $\binom{n}{k} = \binom{n}{n-k}$
3. *Si $k < n$,* $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$

Demostración. Demostraremos (3).

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!} \\
&= \frac{n!}{k!(n-k)(n-k-1)!} + \frac{n!}{(k+1)k!(n-k-1)!} \\
&= \frac{n!}{k!(n-k-1)!}\left(\frac{1}{n-k} + \frac{1}{k+1}\right) \\
&= \frac{n!}{k!(n-k-1)!} \cdot \frac{(n-k)+(k+1)}{(n-k)(k+1)} \\
&= \frac{n!}{k!(n-k-1)!} \cdot \frac{n+1}{(n-k)(k+1)} \\
&= \frac{(n+1)n!}{(k+1)k!\ (n-k)(n-k-1)!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

La propiedad (3) 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. Rellenamos 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**.

7.2. Binomio de Newton

Teorema 7.1 (Binomio de Newton). *Sean $x, y \in \mathbb{R}, n \in \mathbb{N}$. Entonces*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Ejemplo:

$$\begin{aligned}(x+2)^3 &= \binom{3}{0}x^0 2^3 + \binom{3}{1}x^1 2^2 + \binom{3}{2}x^2 2^1 + \binom{3}{3}x^3 2^0 \\ &= 1 \cdot x^0 2^3 + 3 \cdot x^1 2^2 + 3 \cdot x^2 2^1 + 1 \cdot x^3 2^0 \\ &= 8 + 12x + 6x^2 + x^3\end{aligned}$$

Veamos, antes de probar el teorema, una forma intuitiva de comprender por qué aparecen los coeficientes $\binom{n}{k}$. Pensemos en $n = 3$.

$$\begin{aligned}(x+y)^3 &= (x+y)(x+y)(x+y) \\ &= x^3 + x^2y + xyx + xy^2 + yx^2 + yxy + y^2x + y^3\end{aligned}$$

El término x^2y viene de haber elegido x en los primeros dos paréntesis, y haber elegido y en el tercero. $\binom{3}{2}$ representa la cantidad de combinaciones donde se eligió x exactamente dos veces, las cuales son: x^2y, xyx, yx^2. Si reordenamos los factores, obtenemos

$$x^2y + xyx + yx^2 = \binom{3}{2}x^2y$$

Finalmente se concluye que

$$(x+y)^3 = \binom{3}{0}x^0y^3 + \binom{3}{1}x^1y^2 + \binom{3}{2}x^2y^1 + \binom{3}{3}x^3y^0$$

Demostración. Probémoslo por inducción en $n \in \mathbb{N}$.
Primero analicemos el caso base, $n = 0$. Por un lado $(x+y)^0 = 1$ y por otro $\sum_{k=0}^{0}\binom{0}{k}x^ky^{0-k} = \binom{0}{0}x^0y^0 = 1$ (Aquí suponemos que $\forall x \in \mathbb{R}, x^0 = 1$). Es decir, la propiedad se cumple para $n = 0$.

Sea entonces $n \geq 0$ tal que se tiene que $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}$ (H.I.). Probemos que se tiene el teorema para $n+1$:

$$\begin{aligned}(x+y)^{n+1} &= (x+y)(x+y)^n \\ &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k} \quad \text{Aplicamos H.I.} \\ &= \sum_{k=0}^{n}x^{k+1}y^{n-k} + \sum_{k=0}^{n}x^ky^{n+1-k}.\end{aligned}$$

Ahora, si $1 \leq k \leq n$, sabemos por propiedad de los coeficientes binomiales que

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Luego,

$$\begin{aligned}(x+y)^{n+1} &= x^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=1}^{n}\binom{n}{k}x^ky^{n-k+1} + y^{n+1} \\ &= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^ky^{n-k+1} + \sum_{k=1}^{n}\binom{n}{k}x^ky^{n-k+1} + y^{n+1} \quad \text{Cambio de variable.} \\ &= x^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]x^ky^{n-k+1} + y^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^ky^{n+1-k}.\end{aligned}$$

De donde se concluye el teorema.

Calculemos las siguientes sumatorias:

1. $\sum_{k=1}^{n}\frac{1}{k(k+1)}$
2. $\sum_{k=0}^{n}k \cdot k!$
3. $\sum_{k=0}^{n}\binom{n}{k}$
4. $\sum_{k=0}^{n}\binom{n}{k}\frac{1}{k+1}$

1. Para ésta, utilizamos la descomposición

$$\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$$

con lo que la suma a calcular se convierte en

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right) = \frac{1}{1} - \frac{1}{n+1} = 1 - \frac{1}{n+1}$$

usando la propiedad telescópica.

2. Consideremos la igualdad $(k+1)! = (k+1)k! = k \cdot k! + k!$, con la que obtenemos que

$$k \cdot k! = (k+1)! - k!$$

Sumando a ambos lados, llegamos a

$$\sum_{k=0}^{n} k \cdot k! = \sum_{k=0}^{n} ((k+1)! - k!) = (n+1)! - 0! = (n+1)! - 1$$

pues es una suma telescópica.

3. Esta suma resulta ser una aplicación directa 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, utilizando la fórmula de Newton se tiene que

$$\sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n$$

4. Para este tipo de sumatorias, debemos llevarlas a la forma del Binomio de Newton, típicamente ingresando los factores que "sobran" al coeficiente binomial. Reescribamos el término de la suma:

$$\begin{aligned} \binom{n}{k} \frac{1}{k+1} &= \frac{n!}{k!(n-k)!} \cdot \frac{1}{k+1} \\ &= \frac{n!}{(k+1)!(n-k)!} \end{aligned}$$

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

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} = \frac{1}{n+1} \sum_{k=0}^{n} \binom{n+1}{k+1}$$

Hacemos una traslación de índice en la suma de la derecha, para obtener

$$\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} = \frac{1}{n+1} \sum_{k=1}^{n+1} \binom{n+1}{k}$$

Esto de la derecha se parece bastante a un Binomio de Newton: bastaría rellenar con $1^k 1^{n+1-k}$, sin embargo primero debemos procurar que el índice k sume sobre todos los valores $0, 1, \ldots, n+1$. Sumamos y restamos el término asociado a $k = 0$, y seguimos desarrollando:

$$\begin{aligned}
\sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} &= \frac{1}{n+1} \left(\sum_{k=0}^{n+1} \binom{n+1}{k} - \binom{n+1}{0} \right) \\
&= \frac{1}{n+1} \left(\sum_{k=0}^{n+1} \binom{n+1}{k} 1^k 1^{n+1-k} - 1 \right) \\
&= \frac{1}{n+1} ((1+1)^{n+1} - 1) \\
&= \frac{1}{n+1} (2^{n+1} - 1)
\end{aligned}$$

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ Sea $n \geq 1$ y $q \neq 1$. $\sum_{i=0}^{n-1} q^i = \frac{1-q^n}{1-q}$.

2. ☐ Sea $n \geq 1$ y $q \neq 1$. $\sum_{i=0}^{n-1} q^i = \frac{1-q^{n+1}}{1-q}$.

3. ☐ Sea $n \geq 1$ y $q \neq 1$. $\sum_{i=0}^{n-1} q^i = \frac{1}{1-q}$.

4. ☐ Sea $n \geq 1$ y $q \neq 1$. $\sum_{i=k}^{n-1} q^i = q^k \frac{1-q^{n-k}}{1-q}$.

5. ☐ Sea $n \geq 1$ y $q \neq 1$. $\sum_{i=k}^{n-1} q^i = q^k \frac{1-q^n}{1-q}$.

6. ☐ Sea $n \geq 1$. $\sum_{i=0}^{n-1} i = \frac{n(n+1)}{2}$.

7. ☐ Sea $n \geq 1$. $\sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}$.

8. ☐ Sea $n \geq 0$. $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

9. ☐ Sea $n \geq 0$. $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$.

10. ☐ Sea $n \geq 0$. $\sum_{i=0}^{n-1} i^2 = \frac{n(n-1)(2n-1)}{6}$.

11. ☐ Sea $n \geq 0$. $\sum_{i=0}^{n-1} i^2 = \frac{n(n-1)(2n+1)}{6}$.

12. ☐ Sea $n \geq 1$. $\sum_{i=0}^{n-1} sen(i) \leq n$.

13. ☐ $\sum_{i=0}^{n} a_i + b_i = \sum_{i=0}^{n}(a_i + \sum_{j=0}^{n} b_j)$.

14. ☐ $\sum_{i=0}^{n} a_i + b_i = \sum_{i=0}^{n}(a_i + \sum_{j=i}^{n} b_i)$.

15. ☐ $\sum_{i=0}^{n} a_i + b_i = \sum_{i=0}^{n} a_i + \sum_{i=0}^{n} b_i$.

16. ☐ Sean $k \leq n$. $\binom{n}{k} + \binom{n+1}{k+1} = \binom{n+1}{k+1}$.

17. ☐ Sean $1 \leq k \leq n$. $\binom{n-1}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

18. ☐ Sean $k \leq n$. $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

19. ☐ Sean $1 \leq k \leq n$. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k+1}$.

20. ☐ Sean $1 \leq k \leq n$. $\binom{n-1}{k-1} + \binom{n}{k} = \binom{n+1}{k+1}$.

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 $\binom{n}{k} y$.

Guía de Ejercicios

1. Encuentre el valor de las siguientes sumas, usando sumas conocidas:

a) $\sum_{k=1}^{n-1} k(k+1)$.
b) $\sum_{k=3}^{n-1}(k-2)(k+1)$.
c) $\sum_{k=4}^{n-2} 2k^3 - \frac{1}{3}k + 2$.
d) $\sum_{k=1}^{n} \frac{1}{k(k-1)}$.
e) $\sum_{k=1}^{n} \frac{(k+1)!(1-k)}{k^2+k}$.
f) $\sum_{k=1}^{n} \binom{n}{k} - \sum_{k=0}^{n-1} \binom{n+1}{k}$.
g) $\sum_{i=0}^{n-1} x^{n-1-i}y^i$. $\quad (= \frac{x^n-y^n}{x-y})$

2. 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) $\sum_{k=2}^{n+1} \binom{k}{2}$ $\quad (= \binom{n+2}{3})$.
i) $\sum_{i=1}^{n} \binom{i+j-1}{j}$ $\quad (= \binom{n+j}{j+1})$.
j) $\sum_{k=2}^{n+1} \binom{k}{2}$.
k) $\sum_{k=0}^{n} \frac{\binom{n}{k}}{k+1}$.
l) $\sum_{k=0}^{n} \binom{n}{k}^2$.

3. 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 $(1+2x+3x^2)^5$.

4. 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) $\binom{n}{0}\binom{n}{p} + \binom{n}{1}\binom{n-1}{p-1} + \ldots + \binom{n}{p}\binom{n-p}{0} = 2^p\binom{n}{p}$.
c) $\binom{n}{k} = \binom{n+1}{k+1} - \binom{n}{k+1}$

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 :

$$\frac{1}{\sqrt{a}_0 + \sqrt{a}_1} + \frac{1}{\sqrt{a}_1 + \sqrt{a}_2} + ... + \frac{1}{\sqrt{a}_{n-1} + \sqrt{a}_n} = \frac{n}{\sqrt{a}_0 + \sqrt{a}_n}.$$

Guía de Problemas

La presente guía le permitirá tener una idea bastante precisa del tipo de problemas que debe ser capaz de resolver en una evaluación y el tiempo promedio que debería demorar en resolverlos. En total debería poder resolverla en 3 horas. Le recomendamos que trabaje en ella una hora antes de la clase de trabajo dirigido, que resuelva sus dudas en la clase de trabajo dirigido y que luego dedique una hora a escribir con detalles las soluciones.

P1. (20 min.) Calcular las siguientes sumatorias

a. $\sum_{k=n}^{m} \log(1+\frac{1}{k})$, donde $n \leq m$.

b. $\sum_{k=1}^{n-1} \frac{1}{k!\ (n-k)!}$, donde $n \geq 1$.

P2. (15 min.) Calcular para $m \geq 1$,

$$\sum_{i=\frac{m(m-1)}{2}+1}^{\frac{m(m+1)}{2}} (2i-1)$$

P3. (15 min.) Calcular

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k(k+1)}(\sqrt{k+1}+\sqrt{k})}$$

P4. (20 min.) Sean $x, y \in \mathbb{R}\setminus\{0\}$, $x \neq y$. Pruebe sin usar inducción que para todo $n \geq 1$,

$$\sum_{i=0}^{n-1} x^{n-1-i}y^i = \frac{x^n - y^n}{x-y}$$

P5. Dadas $f, g : \mathbb{N} \to \mathbb{R}$, se define $(f*g) : \mathbb{N} \to \mathbb{R}$ por:

$$\forall n \in \mathbb{N} \qquad (f*g)(n) = \sum_{k=0}^{n} f(k)g(n-k)$$

(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

$$n!(f*g)(n)$$

P6. (20 min.) Demuestre que $\forall n \in \mathbb{N}$

$$\sum_{k=0}^{n}(1-x)^k = \sum_{k=0}^{n}(-1)^k \binom{n+1}{k+1} x^k$$

P7. (20 min.) Calcule la suma $\sum_{k=0}^{n} k7^k \binom{n}{k}$.

P8. *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:

$$\sum_{i=k}^{n} \binom{n}{i}\binom{i}{k} = \binom{n}{k}2^{n-k}$$

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

SEMANA 8: PRINCIPIO DE INDUCCIÓN Y SUMATORIAS

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

7.3. Sumas dobles

Veremos a continuación un caso particular de suma, en el que la que el término general a_k es a su vez una suma, para cada k.
Es decir, veremos cómo sumar sobre más de un índice.

Definición 7.3 (Suma doble). *Es una sumatoria del tipo*

$$\sum_{k=0}^{n} b_k$$

en donde b_k es a su vez una sumatoria, o sea $b_k = \sum_{j=0}^{m} a_{k,j}$.
Reescribiendo:

$$\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj}.$$

Notar que:

- El término general a_{kj}, se denota así pues puede depender de ambos índices.
- Los límites inferior y superior de $\sum_{j=0}^{m} a_{k,j}$ puede depender del índice k.

Intercambio de sumas

En el caso en que los límites inferior y superior de b_k **no dependen de** k, podremos intercambiar el orden de las sumatorias.
Para ver esto, notemos que los términos que estamos sumando son:

$$\begin{array}{ccccc} a_{00} & a_{01} & a_{02} & \cdots & a_{0m} \\ a_{10} & a_{11} & a_{12} & \cdots & a_{1m} \\ \vdots & & \ddots & & \vdots \\ a_{n0} & a_{n1} & a_{n2} & \cdots & a_{nm} \end{array}$$

y que por ende, la suma doble representa el sumar 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:

Propiedad 7 (Intercambio de sumas). *Si tenemos una suma doble $\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj}$, cuyos límites inferiores y superiores no dependen de los índices. Entonces:*

$$\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} = \sum_{j=0}^{m}\sum_{k=0}^{n} a_{kj}.$$

Queda propuesto como ejercicio probar esta propiedad, usando inducción en $n \in \mathbb{N}$.
Un ejemplo importante es aquel en que:

$$a_{kj} = c_k d_j.$$

O sea, cuando el término general es la multiplicación de dos términos dependiendo independientemente cada índice. En este caso:

$$\begin{aligned}\sum_{k=0}^{n}\sum_{j=0}^{m} a_{kj} &= \sum_{k=0}^{n}\sum_{j=0}^{m} c_k d_j \\ &= \sum_{k=0}^{n} c_k \left(\sum_{j=0}^{m} d_j\right) \quad c_k \text{ es una constante para la segunda suma.} \\ &= \sum_{k=0}^{n} c_k \underbrace{\left(\sum_{j=0}^{m} d_j\right)}_{S}.\end{aligned}$$

Y como la cantidad S es una constante para la suma sobre k, resulta:

$$\sum_{k=0}^{n}\sum_{j=0}^{m} c_k d_j = \left(\sum_{k=0}^{n} c_k\right)\left(\sum_{j=0}^{m} d_j\right)$$

Ejemplo:

Calcular $\sum_{i=0}^{n}\sum_{j=0}^{m} ij$.

Tenemos que, gracias a lo anterior:

$$\sum_{i=0}^{n}\sum_{j=0}^{m} ij = (\sum_{i=0}^{n} i)(\sum_{j=0}^{m} j) = \frac{n(n+1)}{2}\frac{m(m+1)}{2}.$$

Ejemplo:

Calcular $\sum_{i=0}^{n}\sum_{j=0}^{i}(i-j)^2$.

Acá tenemos la tentación de desarrollar $(i-j)^2 = i^2 + 2ij + j^2$ y ocupar sumas conocidas, además del resultado anterior.

Sin embargo, el límite superior de la segunda suma, depende de i por lo que no se puede recurrir a lo anterior.

Acá nos bastará notar qué valores posibles puede tomar $i-j$, para i fijo y j móvil.

Para $j = i$, $i - j = 0$ y crece a medida que decrece j, hasta $j = 0$ en donde vale $i - j = i$.

Por ende hacemos el cambio de índice en la primera sumatoria

$$k = i - j \quad \text{con} \quad k \in \{0, \ldots, i\}.$$

Esto resulta en:

$$\sum_{i=0}^{n}\sum_{k=0}^{i} k^2 = \sum_{i=0}^{n} \frac{i(i+1)(2i+1)}{6}.$$

En donde esta última suma es perfectamente calculable y dicho cálculo queda de ejercicio.

Una última definición, que generaliza la noción anterior es la de:

Definición 7.4 (Suma múltiple). *Se trata de una suma:*

$$\sum_{k_0=0}^{n_0}\sum_{k_1=0}^{n_1}\sum_{k_2=0}^{n_2}\cdots\sum_{k_l=0}^{n_l} a_{k_0k_1\ldots k_l}.$$

Esta generalización también satisface:

Propiedad 8 (Intercambio de sumas). *Si los límites inferiores y superiores no dependen de los índices:*

$$\sum_{k_0=0}^{n_0}\sum_{k_1=0}^{n_1}\sum_{k_2=0}^{n_2}\cdots\sum_{k_l=0}^{n_l} a_{k_0k_1\ldots k_l} = \sum_{k_l=0}^{n_l}\sum_{k_{l-1}=0}^{n_{l-1}}\sum_{k_{l-2}=0}^{n_{l-2}}\cdots\sum_{k_0=0}^{n_0} a_{k_0k_1\ldots k_l}.$$

Y en general para cualquier reordenamiento de las sumas.

8. Cardinalidad

Habitualmente nos topamos con la necesidad de contar los elementos de un determinado conjunto. Tratamos así de establecer una correspondencia entre conjuntos y números naturales diciendo, por ejemplo, que $\{a, b, c\}$ tiene 3 elementos y que $\{2, 3, 5, 7, 11, 13, 17\}$ tiene 7 elementos.
El problema de este enfoque típico es que no nos sirve para ciertos conjuntos, como $\mathbb{N}$, $\mathbb{Z}$ o $\mathbb{R}$. De éstos sólo decimos que tienen una cantidad "infinita" de elementos.

La teoría de cardinalidad viene a establecer conceptos más precisos, que nos permitirán obtener resultados más poderosos que los sugeridos por la sola intuición. Esta teoría reemplaza la noción de "número de elementos" por la de "cardinal", así como la noción de "contar" por "establecer funciones biyectivas".

Ejemplo:

Consideremos $A = \{a, z, x, p, q, r, s\}$, el cual es un conjunto de 7 elementos, y el conjunto $\mathbb{N}_7 = \{x \in \mathbb{N} : 1 \leq x \leq 7\}$. Es fácil construir una biyección entre A y $\mathbb{N}_7$, como por ejemplo la dada por el siguiente esquema.

$$\begin{aligned} \text{a} &\longrightarrow 1 \\ \text{p} &\longrightarrow 2 \\ \text{q} &\longrightarrow 3 \\ \text{r} &\longrightarrow 4 \\ \text{s} &\longrightarrow 5 \\ \text{x} &\longrightarrow 6 \\ \text{z} &\longrightarrow 7 \end{aligned}$$

Así, reemplazaremos nuestra idea de "tener 7 elementos" por la idea equivalente que es "poder construir una biyección hacia $\mathbb{N}_7$". Lo importante de este nuevo enfoque es que nos permite eventualmente trabajar con conjuntos que tengan infinitos elementos.
Definamos esta nueva noción:

Definición 8.1 (Cardinalidad). *Dados A, B conjuntos no vacíos. Diremos que A y B* **tienen el mismo cardinal** *si existe una función $f : A \to B$ que sea biyectiva. En tal caso denotaremos $|A| = |B|$.*

También, denotaremos $|A| \leq |B|$ cuando exista una función $f : A \to B$ que sea inyectiva.

Se tiene las siguientes propiedades básicas acerca de $|\cdot|$:

Propiedades 8. *1.* $|A| \leq |A|$

2. Si $A \subseteq B$, entonces $|A| \leq |B|$

3. Si $|A| \leq |B|$ y $|B| \leq |C|$, entonces $|A| \leq |C|$

4. $|A| \leq |B| \wedge |B| \leq |A| \iff |A| = |B|$

Vale la pena hacer notar que la última propiedad es difícil de demostrar, escapándose del alcance de este curso.

8.1. Conjuntos finitos

Sea $n \in \mathbb{N}$ un natural cualquiera. Definimos el conjunto

$$\mathbb{N}_n = \{x \in \mathbb{N} : 1 \leq x \leq n\}$$

(por ejemplo, tenemos así que $\mathbb{N}_0 = \emptyset$, $\mathbb{N}_2 = \{1, 2\}$, y $\mathbb{N}_7 = \{1, 2, 3, 4, 5, 6, 7\}$)

Dado un conjunto cualquiera E, diremos que es **finito** si y sólo si existe $k \in \mathbb{N}$ tal que $|\mathbb{N}_k| = |E|$.
Así, podemos establecer las siguientes propiedades, las cuales se demuestran utilizando principio de inducción:

Propiedades 9. *1.* $|\mathbb{N}_{k+1}| \not\leq |\mathbb{N}_k|$ *(esto se nota $|\mathbb{N}_k| < |\mathbb{N}_{k+1}|$)*

2. $m \leq n \iff |\mathbb{N}_m| \leq |\mathbb{N}_n|$

Gracias a ellas, denotaremos $|\mathbb{N}_k| = k$.
Cualquier conjunto que no sea finito, diremos que es **infinito**.

Propiedad 9. $\mathbb{N}$ *es infinito.*

Demostración. Supongamos que $\mathbb{N}$ fuese finito. Entonces, existiría un $k \in \mathbb{N}$ tal que

$$|\mathbb{N}| = |\mathbb{N}_k|$$

Además, sabemos que $\mathbb{N}_{k+1} \subseteq \mathbb{N}$, y por lo tanto

$$|\mathbb{N}_{k+1}| \leq |\mathbb{N}|$$

con lo que concluimos que

$$|\mathbb{N}_{k+1}| \leq |\mathbb{N}_k|$$

lo cual es una contradicción.

8.2. Conjuntos numerables

Llamaremos conjunto **numerable** a cualquier conjunto que tenga la misma cardinalidad de $\mathbb{N}$.

Propiedad 10. *$\mathbb{Z}$ es numerable.*

Demostración. Listemos ordenadamente los elementos de $\mathbb{Z}$:

$\mathbb{Z}$	...	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	...

y 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:

$$f(n) = \begin{cases} \frac{n}{2} & \text{si } n \text{ es par} \\ \frac{-(n+1)}{2} & \text{si } n \text{ es impar} \end{cases}$$

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.

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 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.

Propiedad 11. *$\mathbb{N} \times \mathbb{N}$ es numerable.*

Demostración. 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						...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

De esta manera hemos establecido un proceso que enumera $\mathbb{N} \times \mathbb{N}$, por lo que sabemos que hay una función biyectiva entre $\mathbb{N}$ y $\mathbb{N} \times \mathbb{N}$, y así concluimos lo que deseábamos demostrar.

Propiedades 10. *Sea A un conjunto infinito cualquiera. Entonces*

1. *Sea A un conjunto infinito. Entonces $|\mathbb{N}| \leq |A|$.*
2. *Sea A un conjunto infinito tal que $|A| \leq |\mathbb{N}|$. Entonces $|A| = |\mathbb{N}|$.*

Demostración. Demostraremos (1).
Construiremos inductivamente una secuencia de elementos distintos $a_0, a_1, a_2, \ldots$ contenida en A.
Como A es infinito, en particular es no vacío. Sea, entonces, $a_0 \in A$.
El conjunto $A \setminus \{a_0\}$ debe ser también infinito, y en particular es no vacío también. Sea, entonces, $a_1 \in A \setminus \{a_0\}$.

Si hemos extraído de A los elementos $a_0, a_1, \ldots, a_n$, tenemos que $A \setminus \{a_0, a_1, \ldots, a_n\}$ es no vacío. Así, escogemos $a_{n+1} \in A \setminus \{a_0, a_1, \ldots, a_n\}$.

Entonces $\{a_0, a_1, a_2, \ldots\} \subseteq A$, y luego $|\{a_0, a_1, a_2, \ldots\}| \leq |A|$.
Si consideramos $f : \mathbb{N} \to \{a_0, a_1, a_2, \ldots\}$ dada por $f(n) = a_n$, como todos los a_k son distintos, tenemos que f es inyectiva. Así $|\mathbb{N}| \leq |\{a_0, a_1, a_2, \ldots\}|$, con lo que concluimos el resultado.

8.3. Uniones de cantidades infinitas de conjuntos

Dados dos conjuntos A y B, ya habíamos definido su unión $A \cup B$ diciendo que

$$x \in A \cup B \iff x \in A \vee x \in B$$

Esta definición puede ser extendida para una cantidad finita de conjuntos $A_0, \ldots, A_n$ del modo siguiente

$$\begin{aligned} x \in A_0 \cup A_1 \cup \ldots \cup A_n &\iff x \in A_0 \vee x \in A_1 \vee \ldots \vee x \in A_n \\ &\iff (\exists k \in \{0, 1, \ldots, n\})\ x \in A_k \end{aligned}$$

Pensemos ahora en una cantidad infinita de conjuntos. Más precisamente, pensemos que tenemos una colección numerable de conjuntos $A_0, A_1, \ldots, A_n, \ldots$ que deseamos unir (notemos que al hablar de "colección numerable" nos referimos a que hay un conjunto A_k por cada número natural k, sin embargo cada conjunto A_k no necesariamente es numerable).

Para simplificarnos la escritura, denotaremos al conjunto unión ($A_0 \cup A_1 \cup \ldots \cup A_n \cup \ldots$) como

$$\bigcup_{k\in\mathbb{N}} A_k$$

¿Cómo definir este conjunto unión? Extenderemos de forma muy sencilla la definición de una cantidad finita de conjuntos, así:

$$x \in \bigcup_{k\in\mathbb{N}} A_k \iff (\exists k \in \mathbb{N})\ x \in A_k$$

8.4. Propiedades de conjuntos numerables

Propiedad 12. *Sean A, B conjuntos numerables. Entonces $A \times B$ es numerable.*

Demostración. Como A y B son numerables, sabemos que existen funciones biyectivas

$$f : \mathbb{N} \to A \qquad g : \mathbb{N} \to B$$

Con éstas, construimos la función $\phi : \mathbb{N} \times \mathbb{N} \to A \times B$ dada por

$$\phi(i, j) = (f(i), g(j))$$

Queda propuesto al lector verificar que ϕ es también biyectiva. Concluimos entonces que $|\mathbb{N} \times \mathbb{N}| = |A \times B|$, y como $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$ se concluye que $A \times B$ es numerable.

Corolario 8.1. *$\mathbb{Q}$ es numerable.*

Demostración. 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 un elemento $x \in \mathbb{Q}$. Sabemos que se puede escribir de la forma $x = \frac{p}{q}$ con $p \in \mathbb{Z}$, $q \in \mathbb{N} \setminus \{0\}$, y donde p y q son primos relativos. Podemos entonces construir una función $\Phi : \mathbb{Q} \to \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$, de modo que $\Phi(x) = (p, q)$. Es decir:

$$\begin{gathered}\text{Para } x \in \mathbb{Q}, \text{ definimos } \Phi(x) = (p, q) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\}),\\ \text{donde } p, q \text{ son primos relativos y } x = \tfrac{p}{q}.\end{gathered}$$

Es fácil demostrar que esta Φ es inyectiva, en efecto: sean $x_1, x_2 \in \mathbb{Q}$ tales que $\Phi(x_1) = \Phi(x_2)$. Consideramos $p_1, p_2 \in \mathbb{Z}$ y $q_1, q_2 \in \mathbb{N} \setminus \{0\}$ tales que

$$\Phi(x_1) = (p_1, q_1) \quad \wedge \quad \Phi(x_2) = (p_2, q_2)$$

Como $\Phi(x_1) = \Phi(x_2)$, se tiene que $p_1 = p_2$ y $q_1 = q_2$. Por definición de Φ, concluimos entonces que

$$x_1 = \frac{p_1}{q_1} = \frac{p_2}{q_2} = x_2$$

Gracias a la inyectividad de Φ, obtenemos que $|\mathbb{Q}| \leq |\mathbb{Z} \times (\mathbb{N} \setminus \{0\})|$. Como tanto $\mathbb{Z}$ como $\mathbb{N} \setminus \{0\}$ son numerables, gracias a la propiedad para el producto cartesiano tenemos que $|\mathbb{Z} \times (\mathbb{N} \setminus \{0\})| = |\mathbb{N}|$. Así,

$$|\mathbb{N}| \leq |\mathbb{Q}| \quad \wedge \quad |\mathbb{Q}| \leq |\mathbb{N}|$$

y entonces $\mathbb{Q}$ es numerable.

Propiedad 13. *Sean $A_0, \ldots, A_n$ conjuntos numerables. Entonces $A_0 \times \ldots \times A_n$ es numerable.*

Propiedad 14. *Sea $A_0, A_1, \ldots, A_n, \ldots$ una colección numerable de conjuntos, donde cada A_k es un conjunto numerable. Entonces su unión*

$$\bigcup_{k\in\mathbb{N}} A_k \text{ también es numerable}$$

Proposición 8.1. *Sea A un conjunto infinito, y sea $x \in A$. Se tiene que $|A| = |A \setminus \{x\}|$.*

Demostración. Tal como hicimos en una demostración anterior, contruyamos un conjunto numerable

$$A' = \{a_0, a_1, a_2, a_3, \ldots\} \subseteq A$$

Sin pérdida de generalidad, podemos suponer que $x \notin A'$.
para definir la función $f : A \to A \setminus \{x\}$ dada por

$$(\forall a \in A) \quad f(a) = \begin{cases} a_0 & \text{si } a = x \\ a_{k+1} & \text{si } a \in A' \wedge a = a_k \\ a & \text{si } a \notin A' \wedge a \neq x \end{cases}$$

Esta f deja invariantes a todos los elementos que no pertenecen a $A' \cup \{x\}$, y a los elementos de este conjunto los traslada todos en una posición ($x \to a_0$, $a_k \to a_{k+1}$). Notemos que, gracias a la definición de f: para $a \in A$,

- Si $f(a) = a_0$, entonces $a = x$.
- Si $f(a) \in A' \setminus \{a_0\}$, entonces $a \in A'$.
- Si $f(a) \notin A'$, entonces $a \notin A' \cup \{x\}$.

Con estas herramientas, queda propuesto al lector demostrar que f es biyectiva, con lo que se concluye la demostración.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

Nota: En todas las preguntas se asume que los índices y términos son independientes unos de otros, a menos que se nale claramente. Por ejemplo, si m depende de k, será denotado $m(k)$ ó m_k.

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. ☐ $\sum_{i=0}^{n}\sum_{j=0}^{m} ij = \frac{n(n+1)m(m+1)}{4}$.

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. ☐ $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{n(n+1)(m+1)}{2}$.

11. ☐ $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{n(n+1)}{2}$.

12. ☐ $\sum_{i=0}^{n}\sum_{j=0}^{m} i = \frac{m(m+1)(n+1)}{2}$.

13. ☐ $\sum_{i=0}^{N}\sum_{j=i}^{M}\sum_{k=j}^{L} a_k = \sum_{k=0}^{N}\sum_{j=k}^{M}\sum_{i=j}^{L} a_i$

14. ☐ $\sum_{i=0}^{N}\sum_{j=0}^{M}\sum_{k=0}^{L} a_k = \sum_{j=0}^{N}\sum_{k=0}^{M}\sum_{i=0}^{L} a_i$.

15. ☐ $\sum_{i=0}^{N}\sum_{j=0}^{i} a_i = \sum_{j=0}^{N}\sum_{i=0}^{j} a_j$.

16. ☐ $\sum_{i=0}^{N}\sum_{j=0}^{i} a_j = \sum_{j=0}^{N}\sum_{i=0}^{j} a_i$.

17. ☐ Para todo conjunto A, $|A| < |A|$.

18. ☐ Para todo conjunto A, $|A| \leq |A|$.

19. ☐ Dados A y B conjuntos, $A \subseteq B \Rightarrow |A| \leq |B|$.

20. ☐ Dados A y B conjuntos, $A \subseteq B \Rightarrow |B| \leq |A|$.

21. ☐ Dados A y B conjuntos, $A \subseteq B \Rightarrow |A| < |B|$.

22. ☐ Dados A, B y C conjuntos, $|A| \leq |B| \wedge |B| \leq |C| \Rightarrow |A| \leq |C|$.

23. ☐ Dados A y B conjuntos, $|A| \leq |B| \wedge |B| \leq |A| \Leftrightarrow |A| = |B|$.

24. ☐ $|\mathbb{N}| < |\mathbb{Z}|$.

25. ☐ $|\mathbb{N}| < |\mathbb{Z} \times \mathbb{Z}|$.

26. ☐ $|\mathbb{N}| = |\mathbb{Z} \times \mathbb{Z}|$.

27. ☐ $|\mathbb{N}| = |\mathbb{Q} \times \mathbb{Z}|$.

28. ☐ No todo conjunto infinito A cumple que $|\mathbb{N}| \leq |A|$.

29. ☐ Union finita de conjuntos numerables es numerable.

30. ☐ Union numerable de conjuntos numerables es numerable.

31. ☐ Producto cartesiano finito de conjuntos numerables es numerable.

32. ☐ Producto cartesiano finito de conjuntos finitos es finito.

33. ☐ El producto cartesiano de un conjunto finito no vacío con uno numerable es finito.

34. ☐ El producto cartesiano de un conjunto finito no vacío con uno numerable es numerable.

35. ☐ Todo subconjunto no vacío de un conjunto numerable es numerable.

36. ☐ Todo subconjunto de un conjunto numerable es numerable.

37. ☐ Todo subconjunto infinito de un conjunto numerable es numerable.

38. ☐ Todo subconjunto de un conjunto finito es numerable.

39. ☐ Todo subconjunto de un conjunto finito es finito.

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) $\sum_{i=0}^{N}\sum_{j=i}^{N} q^j$

(f) $\sum_{i=0}^{N}\sum_{k=0}^{N} \binom{N}{k}$

(g) $\sum_{i=0}^{N}\sum_{k=i}^{N} \binom{N}{k}$

(h) $\sum_{i=0}^{N}\sum_{k=0}^{i} \binom{i}{k} a^k b^{i-k}$

(i) $\sum_{i=0}^{N}\sum_{k=0}^{i} \binom{i}{k} a^k b^{N-k}$

3. Pruebe que los siguientes conjuntos son numerables. Se nale 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) $A = \{C_r \subseteq \mathbb{R}^2 | C_r$ es una circunferencia centrada en $(0,0)$ y de radio $r \in \mathbb{N}\}$.

4. 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) $A \cup B$.

Guía de Problemas

P1. (20 min.) Demuestre, sin usar inducción, que:

$$\sum_{k=1}^{n}(1+4+4^2+\cdots+4^{k-1})\binom{n}{k}=\frac{5^n-2^n}{3}.$$

P2. (20 min.) Calcule, sin usar inducción:

$$\sum_{j=1}^{n}\sum_{i=1}^{j}\sum_{k=0}^{i}\binom{i}{k}\frac{8^{k+1}}{3^i}.$$

P3. (20 min.) Sea $A=\{x\in\mathbb{R}\ /\exists\ k\in\mathbb{Z},\exists i\in\mathbb{N}, x=\frac{k}{3^i}\}$. Pruebe que A es numerable.

P4. (30 min.) Pruebe que el siguiente conjunto es numerable:

$$C=\{x\in[0,+\infty)/\exists n\in\mathbb{N}\setminus\{0\},\ x^n\in\mathbb{N}\}$$

P5. (a) (20 min.) Pruebe que el conjunto de todas las rectas no verticales que pasan por el punto $(0,1)$ y cortan al eje OX en una coordenada racional es numerable.

(b) (20 min.) Pruebe que 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 es numerable.

P6. (30 min.) Sea $A=\{\frac{p}{q}\ /(\exists n\in\mathbb{N}, q=2^n)\wedge(p\in\mathbb{N}, p<q)\}$. Probar que A es numerable.
Indicación: Puede usar que la unión numerable de conjuntos finitos no vacíos es numerable.

P7. (30 min) Sea $A=\{0,1,2,...,n\}$ y considere la secuencia de elementos en A, $(x_0,x_1,x_2,x_3,...)$ (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 $x_\ell=x_j$.

P8. Sea $E=\{(a_1,...,a_n)\in\{-1,1\}^n/n\in\mathbb{N}, n\geq 2, \sum_{i=1}^{n}a_i=0\}$. Demuestre que

(a) (15 min.) E es infinito

(b) (15 min.) E tiene la misma cardinalidad de $\mathbb{N}$

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

SEMANA 9: CARDINALIDAD Y ESTRUCTURAS ALGEBRAICAS

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

9. Cardinalidad

9.1. Conjuntos no numerables

Vimos cuáles son los conjuntos numerables, una serie de propiedades acerca de ellos, y conocimos varios conjuntos numerables, como $\mathbb{Z}$, $\mathbb{N}\times\mathbb{N}$ y $\mathbb{Q}$. Queda, así, la pregunta:

¿hay conjuntos no numerables? ¿cuáles son?

En esta sección veremos que:

Propiedad 15. $\mathbb{R}$ *no es un conjunto numerable, es decir, que NO existe una función*

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

que sea biyectiva.

El argumento que mostraremos fue presentado por Cantor, y se le conoce comúnmente como argumento de **diagonalización**.

Demostración. Observemos, para empezar, que basta demostrar que $[0,1)$ es no numerable, es decir que

$$|[0,1)|>|\mathbb{N}|$$

puesto que $|[0,1)|\leq|\mathbb{R}|$.
¿Qué particularidad especial poseen los reales de $[0,1)$? Todos ellos se pueden escribir en base decimal como

$$x=0.a_1a_2a_3a_4\ldots$$

donde a_k es el k-ésimo dígito decimal de x.
Supongamos que $[0,1)$ es un conjunto numerable, es decir que existe una función biyectiva de $\mathbb{N}$ en $[0,1)$, a la cual llamaremos f. Al k-ésimo dígito de la expansión decimal del real $f(n)$ le llamaremos a_k^n, con lo que

$$f(n)=0.a_1^na_2^na_3^na_4^n\ldots$$

Podemos entonces ordenar los números de $[0,1)$ en una tabla infinita

$$\begin{array}{rcl} f(0) &=& 0.a_1^0a_2^0a_3^0a_4^0\ldots\\ f(1) &=& 0.a_1^1a_2^1a_3^1a_4^1\ldots\\ f(2) &=& 0.a_1^2a_2^2a_3^2a_4^2\ldots\\ f(3) &=& 0.a_1^3a_2^3a_3^3a_4^3\ldots\\ \vdots & \vdots & \vdots \end{array}$$

El punto importante es que, ya que hemos supuesto que f es biyectiva, entonces TODOS los reales de $[0,1)$ aparecen alguna vez en esta lista infinita. Mostraremos que esto es una contradicción, es decir que existe un real $\bar{x}\in[0,1)$ que no está en la lista.

Definamos la siguiente secuencia de valores: para $k \geq 1$,

$$b_k = \begin{cases} 0 & \text{si } a_k^k = 1 \\ 1 & \text{si } a_k^k \neq 1 \end{cases}$$

y el valor $\bar{x}$ dado por

$$\bar{x} = 0.b_1 b_2 b_3 b_4 \ldots$$

Éste es un elemento de $[0, 1)$.

Como supusimos que f es biyectiva, entonces existe $N \in \mathbb{N}$ tal que $f(N) = \bar{x}$. Entonces sus dígitos en base decimal deben ser iguales uno a uno:

$$0.a_1^N a_2^N a_3^N a_4^N \ldots = 0.b_1 b_2 b_3 b_4 \ldots$$

Es decir,

$$(\forall k \geq 1)\ a_k^N = b_k$$

Aquí aparece la contradicción, pues tomando $k = N$, $a_N^N = b_N$, sin embargo b_N fue escogido para ser distinto de a_N^N: si $a_N^N = 1$ entonces $b_N = 0$, y si $a_N^N \neq 1$ entonces $b_N = 1$.

Una observación relevante:

Observación:

- $[0, 1)$ tiene en realidad el mismo cardinal que $\mathbb{R}$. En efecto, utilizando el ejemplo final del capítulo anterior tenemos que $|[0, 1)| = |(0, 1)|$. Consideramos ahora $\phi : (0, 1) \to \mathbb{R}$ dada por

$$\phi(x) = \tan\left(\pi x - \frac{\pi}{2}\right)$$

  ϕ es una biyección pues es composición de funciones biyectivas, con lo que $|(0, 1)| = |\mathbb{R}|$ y se concluye que $|[0, 1)| = |\mathbb{R}|$.

10. Estructuras algebraicas

10.1. Ley de composición interna

Definición 10.1 (Ley de composición interna). *Dado A un conjunto no vacío. Una **ley de composición interna** (l.c.i.) es una función*

$$\begin{array}{rccc} * : & A \times A & \to & A \\ & (x, y) & \to & x * y \end{array}$$

Comúnmente tratamos con leyes de composición interna, las cuales seguramente conocemos con el nombre de **operaciones**. Tenemos como ejemplos:

- $+$ en $\mathbb{R}$
- $\cdot$ en $\mathbb{Q}$
- $\cup$ en $\mathcal{P}(A)$, donde A es un conjunto

Observemos que, por ejemplo, la división NO es una ley de composición interna en $\mathbb{R}$, pues $3/0$ no es un número real.
Para estudiar estas operaciones definidas sobre conjuntos, definimos:

Definición 10.2 (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 el conjunto A tenemos definida una segunda operación $\triangle$, entonces denotaremos por $(A, *, \triangle)$ la estructura algebraica que considera ambas leyes de composición interna en A.

Notemos que conocemos ya varias estructuras algebraicas: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$. Otras estructuras algebraicas que no son tan conocidas son

- Si A es un conjunto, entonces $(\mathcal{P}(A), \cup)$ y $(\mathcal{P}(A), \Delta)$ son estructuras algebraicas, y en general cualquier operación de conjuntos en A nos sirve para formar una.

- Sea X conjunto no vacío, y $F = \{f : X \to X \text{ función}\}$. Entonces $(F, \circ)$ es una estructura algebraica, donde $\circ$ es la composición de funciones.

Como vemos, hay una enorme cantidad de estructuras algebraicas posibles, sin embargo 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.

10.2. Propiedades básicas

Definición 10.3. *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 $a \in A$ será un elemento* **absorbente** *si*

$$(\forall x \in A)\ x * a = a * x = a$$

- *Un elemento $a \in A$ será un elemento* **idempotente** *si $a * a = a$.*

- *Si $(A, *, \triangle)$ es un estructura algebraica con dos operaciones, diremos que $\triangle$* **distribuye** *con respecto $a *$ si*

$$(\forall x, y, z \in A)\ x \triangle (y * z) = (x \triangle y) * (x \triangle z)$$
$$(\forall x, y, z \in A)\ (y * z) \triangle x = (y \triangle x) * (z \triangle x)$$

Es importante notar que:

Proposición 10.1 (Unicidad del neutro). *Una estructura $(A, *)$ posee a lo más un elemento neutro.*

Demostración. Supongamos que $(A, *)$ posee dos neutros e, 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 $e = e'$.

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 $A = \{a, b, c, d\}$.

$*$	a	b	c	d
a	a	c	a	c
b	c	b	b	a
c	a	b	c	d
d	c	b	d	a

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

$$a * b = b * a = c$$
$$a * d = d * a = c$$

Sin embargo, podemos afirmar la siguiente propiedad...

Propiedad 16. *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}.

Demostración. 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,

$$\begin{aligned} & y \\ = \quad & y * e \\ = \quad & y * (x * z) \\ = \quad & (y * x) * z \quad \text{(por asociatividad)} \\ = \quad & e * z \\ = \quad & z \end{aligned}$$

Si $(A, *)$ una estructura algebraica asociativa y con neutro $e \in A$, entonces también cumple las siguientes propiedades:

Propiedades 11. *1. Si $x \in A$ posee inverso, entonces x^{-1} también. Más aún, $(x^{-1})^{-1} = x$*

2. *Si $x, y \in A$ poseen inversos, entonces $x*y$ también posee inverso, y $(x*y)^{-1} = y^{-1} * x^{-1}$*

3. *Si $x \in A$ posee inverso, entonces es* **cancelable**. *Es decir, para $y, z \in A$:*

$$x * y = x * z \Rightarrow y = z$$
$$y * x = z * x \Rightarrow y = z$$

Demostración. Demostratemos (2).
Sea $w = y^{-1} * x^{-1}$. Queremos probar que $w = (x * y)^{-1}$. Para ello, calculemos

$$\begin{aligned} w * (x * y) &= (w * x) * y \quad \text{(asociatividad)} \\ &= ((y^{-1} * x^{-1}) * x) * y \quad \text{(def. de } w\text{)} \\ &= (y^{-1} * (x^{-1} * x)) * y \quad \text{(asociatividad)} \\ &= (y^{-1} * e) * y \\ &= y^{-1} * y = e \end{aligned}$$

Queda propuesto al lector mostrar que también $(x*y)*w = e$. Así, concluimos que

$$w = (x * y)^{-1}$$

10.3. La estructura $\mathbb{Z}_n$

Sea $n \geq 2$. Definimos anteriormente la relación $\equiv_n$ (congruencia módulo n) en $\mathbb{Z}$, y definimos $\mathbb{Z}_n = \mathbb{Z}/\equiv_n$ su conjunto de clases de equivalencia. Vimos también que

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

Queremos definir operaciones de suma $+_n$ y producto $\cdot_n$ con los cuales $(\mathbb{Z}_n, +_n, \cdot_n)$ sea una estructura algebraica con buenas propiedades. Lo haremos del modo siguiente: para $[x]_n, [y]_n \in \mathbb{Z}_n$

$$\begin{aligned} [x]_n +_n [y]_n &= [x + y]_n \\ [x]_n \cdot_n [y]_n &= [x \cdot y]_n \end{aligned}$$

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 10.2. *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*

$$(x_1 + y_1) \equiv_n (x_2 + y_2) \quad \wedge \quad (x_1 \cdot y_1) \equiv_n (x_2 \cdot y_2)$$

Es decir, si $[x_1]_n = [x_2]_n$ y $[y_1]_n = [y_2]_n$, entonces

$$[x_1 + y_1]_n = [x_2 + y_2]_n \quad \wedge \quad [x_1 \cdot y_1]_n = [x_2 \cdot y_2]_n$$

Demostración. 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

$$x_1 - x_2 = k_x n \quad \wedge \quad y_1 - y_2 = k_y n$$

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 $\mathbb{Z}_n$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ $|[0,1)| \leq |\mathbb{R}|$

2. ☐ $|\mathbb{R}| < |[0,1)|$

3. ☐ $|[0,1)| < |\mathbb{N}|$

4. ☐ $|[0,1)| = |\mathbb{N}|$

5. ☐ $|\mathbb{N}| < |[0,1)|$

6. ☐ $|\mathbb{Q}| = |[0,1)|$

7. ☐ $|\mathbb{Q}| < |[0,1)|$

8. ☐ $|\mathbb{N}| = |\mathbb{R}|$

9. ☐ $|\mathbb{N}| = |\mathbb{Q}|$

10. ☐ $|\mathbb{N}| = |\mathbb{Z}|$

11. ☐ $|\mathbb{Z}| < |\mathbb{N}|$

12. ☐ $|\mathbb{Q}| < |\mathbb{N}|$

13. ☐ $|\mathbb{N}| < |\mathbb{N} \times \mathbb{N}|$

14. ☐ $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N} \times \mathbb{N}|$

15. ☐ $|\mathbb{N}| < |\mathbb{R}|$

16. ☐ Dado $p \in \mathbb{N} \setminus \{1\}$, $|\mathbb{Z}| = |\mathbb{Z}_p|$

17. ☐ $|\mathbb{N}| = |\mathbb{Q} \times \mathbb{Z}|$

18. ☐ $|\mathbb{N}| < |\mathbb{Q} \times \mathbb{Z}|$

19. ☐ La suma en $\mathbb{R}$ es una ley de composición interna.

20. ☐ La suma en $\mathbb{N}$ es una ley de composición interna.

21. ☐ La suma en $\mathbb{Z}$ es una ley de composición interna.

22. ☐ La suma en $\mathbb{Z} \setminus \{0\}$ es una ley de composición interna.

23. ☐ La suma en $\{n \in \mathbb{N} / n \text{ es par}\}$ es una ley de composición interna.

24. ☐ La suma en $\{n \in \mathbb{N} / n \text{ es impar}\}$ es una ley de composición interna.

25. ☐ La multiplicación en $\mathbb{R}$ es una ley de composición interna.

26. ☐ La multiplicación en $\mathbb{N}$ es una ley de composición interna.

27. ☐ La multiplicación en $\mathbb{Z}$ es una ley de composición interna.

28. ☐ La multiplicación en $\mathbb{Q}$ es una ley de composición interna.

29. ☐ La multiplicación en $\mathbb{Q} \setminus \{1\}$ es una ley de composición interna.

30. ☐ Una operación $*$ sobre un conjunto A, es conmutativa si $\forall x, y \in A,\ x*y = y$.

31. ☐ Una operación $*$ sobre un conjunto A, es conmutativa si $\forall x, y \in A,\ x * y = y * x$.

32. ☐ Una operación $*$ sobre un conjunto A, es asociativa si $\forall x, y \in A,\ x*y = y*x$.

33. ☐ Una operación $*$ sobre un conjunto A, es asociativa si $\forall x, y, z \in A,\ (x*y)*z = (y * z) * (x * z)$.

34. ☐ Sea una operación $*$ sobre un conjunto A, con neutro e. $x \in A$ es invertible si $\exists y \in A,\ x * y = e = y * x$.

35. ☐ Sea una operación $*$ sobre un conjunto A, con neutro e. $x \in A$ es absorvente si $\exists y \in A,\ x * y = x = y * x$.

36. ☐ Sea una operación $*$ sobre un conjunto A, con neutro e. $x \in A$ es absorvente si $\forall y \in A,\ x * y = x = y * x$.

37. ☐ Dada una operación $*$ sobre un conjunto A, $x \in A$ es idempotente si $\forall y \in A,\ x * y = y$.

38. ☐ Dada una operación $*$ sobre un conjunto A, $x \in A$ es idempotente si $x*x = x$.

39. ☐ El neutro en una estructura algebraica es único.

40. ☐ El inverso de un elemento en una estructura algebraica es siempre único.

41. ☐ El inverso de un elemento en una estructura algebraica es único, si la operación es conmutativa.

42. ☐ El inverso de un elemento en una estructura algebraica es único, si la operación es asociativa.

43. ☐ El 0 es un elemento cancelable en $(\mathbb{N}, +)$.

44. ☐ El 0 es un elemento cancelable en $(\mathbb{R}, \cdot)$.

45. ☐ El 0 es un elemento absorbente en $(\mathbb{N}, +)$.

46. ☐ El 0 es un elemento absorbente en $(\mathbb{R}, \cdot)$.

47. ☐ El 1 es un elemento idempotente de $(\mathbb{R}, \cdot)$.

48. ☐ El 1 es un elemento idempotente de $(\mathbb{R}, +)$.

49. ☐ El 0 es un elemento idempotente de $(\mathbb{R}, +)$.

Guía de Ejercicios

Observación: En esta guía la notación A^k, para un A conjunto y $k \in \mathbb{N} \leq 1$, está dada por:

$$A^k = \underbrace{A \times \cdots \times A}_{\text{k veces}} = \{(x_1, x_2 \ldots, x_k) \mid (\forall i \in \{1, \ldots, k\})\ x_i \in A\}.$$

1. 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 $|\mathbb{N}| < |\mathbb{R}|$.

2. Muestre que los siguientes conjuntos son finitos.

(a) $A = \{f : \{1, ..., n\} \to \{1, ..., n\} / f$ es biyectiva $\}$

(b) $B = \{$ *todas las permutaciones de n elementos distintos* $\}$

(c) $C = \{f : \mathbb{R} \to \mathbb{N} /$ f es biyectiva $\}$

(d) $D = \{$ *todas las estaturas de los habitantes del planeta tierra* $\}$

(e) Dados $a < b \in \mathbb{R}$, $E = (-\infty, b] \cap [a, \infty) \cap \mathbb{N}$

3. 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) $A = \{(m, n) \in \mathbb{Z}^2 / m \leq n\}$

(b) $C = \{x \in \mathbb{R} / \exists k \in \mathbb{Z}, \exists i \in \mathbb{N}, x = k/3^i\}$

(c) $D = \{x = (x_1, x_2, x_3) \in \mathbb{Z}^3 / x_1 < x_2 < x_3\}$

(d) $G = \{$ *circunferencias de radio y centro racional* $\}$

4. 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) $B = \{(x, y) \in \mathbb{R}^2 / x + y = 1\}$

(b) Sea $r \in \mathbb{Q} \setminus \{0\}$, $C = \{(x, y) \in \mathbb{R}^2 / x^2 + y^2 = r^2\}$

(c) Sean $a, b \in \mathbb{Q}$ con $a < b$, $E = (-\infty, b] \cap [a, \infty)$

5. Se nale si las siguientes operaciones son o no son 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 $A \neq \emptyset$. $\circ$ (composición de funciones) en el conjunto de las funciones de A en A.

(g) $\cap$ en $\mathcal{P}(A)$, para cierto $A \neq \emptyset$.

6. Considerando las operaciones anteriores, 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.

(e) Determine la existencia de elementos aborbentes.

(f) Determine la existencia de elementos idempotentes.

7. Demuestre las siguientes propiedades dejadas propuestas en la tutoría, 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**. Es decir, para $y, z \in A$:

$$x * y = x * z \Rightarrow y = z$$
$$y * x = z * x \Rightarrow y = z$$

Guía de Problemas

Observación: En esta guía la notación A^k, para un A conjunto y $k \in \mathbb{N} \leq 1$, está dada por:

$$A^k = \underbrace{A \times \cdots \times A}_{\text{k veces}} = \{(x_1, x_2, \ldots, x_k) \mid (\forall i \in \{1, \ldots, k\})\ x_i \in A\}.$$

P1. (15 min.) Pruebe que el conjunto $E = \{x = (x_1, x_2, x_3) \in \mathbb{R} \times \mathbb{N}^2 / \exists n \in \mathbb{N},\ x_1 + x_2 + x_3 = n\}$ es numerable.

P2. Pruebe que los siguientes conjuntos son no numerables:

(a) (15 min.) $A = \{x \in \mathbb{R}^3 / \exists n \in \mathbb{N},\ x_1 + x_2 + x_3 = n\}$.

(b) (15 min.) $\mathcal{T} = \{T \subseteq \mathbb{R}^2 \mid T \text{ es un triángulo}\}$.

P3. (20 min.) Pruebe que el conjunto de todas las rectas no verticales que pasan por el punto $(0, 1)$ es no numerable.

P4. (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.

P5. 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.

(f) (10 min.) Encuentre los elementos idempotentes de $(\mathcal{F}, \star)$

P6. Sea $(E, *)$ una estructura algebraica y $\mathcal{R}$ una relación de equivalencia que satisface la siguiente propiedad:

$$(\forall x_1, x_2, y_1, y_2)\ \ x_1 \mathcal{R} x_2 \wedge y_1 \mathcal{R} y_2 \Rightarrow (x_1 * y_1) \mathcal{R} (x_2 * y_2).$$

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 que la clase de equivalencia de $x * y$ no depende de los representantes de $[x]_\mathcal{R}$ e $[y]_\mathcal{R}$ que se escojan.

(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 $(E/\mathcal{R}, \otimes)$.

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

SEMANA 10: ESTRUCTURAS ALGEBRAICAS Y NÚMEROS COMPLEJOS

10.4. Grupos

Un **grupo** es un caso particular de una 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, las cuales son bastantes.

Definición 10.4 (Grupo). *Sea $(G,*)$ una estructura algebraica. Diremos que es un* **grupo** *si*

- $*$ *es asociativa.*
- $(G,*)$ *posee neutro $e \in G$.*
- *Todo elemento $x \in G$ posee inverso $x^{-1} \in G$.*

Además, si $*$ es conmutativa, llamaremos a $(G,*)$ **grupo abeliano**.

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 las siguientes propiedades (las cuales ya vimos):

1. El inverso de cada elemento es único
2. $(\forall x \in G)\ (x^{-1})^{-1} = x$
3. $(\forall x,y \in G)\ (x*y)^{-1} = y^{-1}*x^{-1}$
4. Todo elemento $x \in G$ es cancelable.

Si $(G,*)$ es un grupo, las siguientes propiedades se agregan a las mencionadas:

Propiedades 12. *Dado $(G,*)$ grupo, entonces:*

1. *Para todo $a,b \in G$, las ecuaciones*
$$a*x_1 = b$$
$$x_2*a = b$$
tienen solución única. Ellas son $x_1 = a^{-1}*b$ y $x_2 = b*a^{-1}$

2. *El único elemento idempotente de G es su neutro.*

Demostración. 1. Consideremos sólo el caso de la primera ecuación. Como G es grupo, a posee neutro a^{-1}. Luego tendremos:

$$\begin{aligned} a^{-1}*(a*x_1) = a^{-1}*b &\Leftrightarrow (a^{-1}*a)*x_1 = a^{-1}*b \quad \text{Por asociativida.}\\ &\Leftrightarrow e*x_1 = a^{-1}*b \quad \text{Por definición de inverso.}\\ &\Leftrightarrow x_1 = a^{-1}*b \quad \text{Por definición de neutro.}\end{aligned}$$

Y esta última expresión es única, pues a^{-1} es único.

2. Si a es un elemento idempotente, satisface: $a*a = a$.
Pero esto es precisamente una ecuación como la anterior (con $b = a$ y a nuestra incógnita). Luego sabemos que la solución es única y es:
$$a = a^{-1}*a = e.$$

Subgrupos

Definición 10.5 (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 a los cuales llamaremos **triviales**:

$$(G, *) \quad \text{y} \quad (\{e\}, *)$$

donde e es el neutro de $(G, *)$.

Propiedades 13. *Sea $(G, *)$ un grupo, y $(H, *)$ un subgrupo de él. Un par de propiedades básicas que salen de ver los elementos de H como elementos de G:*

1. *Si $e \in G$ es el neutro de G y $e_H \in H$ es el neutro de H, entonces $e = e_H$.*

2. *Además, sea $x \in H$. Si $x^{-1} \in G$ es el inverso de x en $(G, *)$ y $\tilde{x} \in H$ es el inverso de x en $(H, *)$, entonces $x^{-1} = \tilde{x}$.*

Estas propiedades quedan propuestas como ejercicios.

Subgrupos: Caracterización

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 10.1. *Sea $H \neq \emptyset$. Entonces*

$$(H, *) \text{ es subgrupo de } (G, *) \iff (\forall x, y \in H)\ x * y^{-1} \in H$$

DEMOSTRACIÓN. 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 que 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 vimos antes, $y^{-1} \in H$. Así que aplicando la hipótesis para x e y^{-1}, tenemos que:

  $$x * (y^{-1})^{-1} \in H \ \Leftrightarrow\ x * y \in H.$$

Concluímos de esta manera que $(H, *)$ es subgrupo de $(G, *)$.

Ejemplo: $\mathbb{Z}_n$ como grupo

Propiedad 17. *Sea $n \geq 2$. Entonces $(\mathbb{Z}_n, +_n)$ es un grupo.*

DEMOSTRACIÓN. Demostraremos que $+_n$ es asociativa, y que posee neutro. Las otras propiedades necesarias quedan de ejercicio para el lector.
Asociatividad: Sean $[x]_n, [y]_n, [z]_n \in \mathbb{Z}_n$. Se tiene que

$$\begin{aligned} ([x]_n +_n [y]_n) +_n [z]_n &= [x + y]_n +_n [z]_n \\ &= [(x + y) + z]_n \end{aligned}$$

Como $+$ es asociativa en $\mathbb{Z}$ y $x, y, z \in \mathbb{Z}$ entonces

$$(x + y) + z = x + (y + z)$$

Entonces

$$\begin{aligned} ([x]_n +_n [y]_n) +_n [z]_n &= [x + (y + z)]_n \\ &= [x]_n +_n [y + z]_n \\ &= [x]_n +_n ([y]_n +_n [z]_n) \end{aligned}$$

Neutro: Demostraremos que $[0]_n \in \mathbb{Z}_n$ es neutro para $+_n$.
En efecto, si $[x]_n \in \mathbb{Z}_n$

$$\begin{aligned} [x]_n +_n [0]_n &= [x + 0]_n = [x]_n \\ [0]_n +_n [x]_n &= [0 + x]_n = [x]_n \end{aligned}$$

Teorema de Lagrange

Sea $(G, *)$ un grupo. Diremos que es un grupo **finito** si G es un conjunto finito. A $|G|$ se le llama **orden** del grupo. Por ejemplo, $\mathbb{Z}_3$ es un grupo finito de orden 3.

Teorema 10.2 (Teorema de Lagrange). *Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo cualquiera de él. Entonces $|H|$ divide a $|G|$.*

Demostración. Definamos primero, dado $g \in G$, la **traslación izquierda** de H como el conjunto $g * H = \{g * h \mid h \in H\}$. Notemos que dado que g es cancelable, $|H| = |g * H|$.

Además, definimos las siguiente relación $\mathcal{R}$ sobre G por:

$$g_1 \mathcal{R} g_2 \;\Leftrightarrow\; (\forall g_1, g_2 \in G)\; g_2 \in g_1 * H.$$

Lo cual equivale a $(\exists h \in H)\; g_2 = g_1 * h$ y también a $g_1^{-1} * g_2 \in H$ (Verifíquelo).
Se tiene que $\mathcal{R}$ es una relación de equivalencia. En efecto:

- **Refleja.** Sea $g \in G$. Como H es subgrupo, $e \in H$ y $g = g * e$, pero esto es exactamente que $g \mathcal{R} g$.
- **Simétrica.** Sean $g_1, g_2 \in G$ tales que $g_1 \mathcal{R} g_2 \;\Leftrightarrow\; g_1^{-1} * g_2 \in H$.

  Pero como H es subgrupo, el inverso de este último término también pertence a H. Es decir:

  $$(g_1^{-1} * g_2)^{-1} = g_2 {-1} * g_1 \in H.$$

  Así, $g_2 \mathcal{R} g_1$.
- **Transitiva.** Supongamos que $g_1 \mathcal{R} g_2$ y $g_2 \mathcal{R} g_3$. Esto se traduce en que

  $$g_1^{-1} * g_2,\; g_2^{-1} * g_3 \in H.$$

  Y como H es cerrado para $*$, se deduce que:

  $$(g_1^{-1} * g_2) * (g_2^{-1} * g_3) = g_1^{-1} * g_3 \in H.$$

  De donde se conlcluye que $g_1 \mathcal{R} g_3$.

Ahora, dado que $\mathcal{R}$ es de equivalencia podemos calcular, para $g \in G$:

$$\begin{aligned}[g]_{\mathcal{R}} &= \{g' \in G \mid g\mathcal{R}g'\} \\ &= \{g' \in G \mid (\exists h \in H)\ g' = g * h\} \\ &= g * H.\end{aligned}$$

Luego, $|[g]_{\mathcal{R}}| = |H|$.
Sean entonces $[g_1]_{\mathcal{R}},\ [g_2]_{\mathcal{R}}, \ldots, [g_s]_{\mathcal{R}}$ las clases de equivalencia de $\mathcal{R}$.
Sabemos que estas clases conforman una partición de G, es decir: $G = [g_1]_{\mathcal{R}} \cup [g_2]_{\mathcal{R}} \cup \cdots \cup [g_s]_{\mathcal{R}}$. Luego:

$$\begin{aligned}|G| &= \sum_{i=1}^{s} |[g_i]_{\mathcal{R}}| \\ &= \sum_{i=1}^{s} |H| = s|H|.\end{aligned}$$

De donde se concluye el resultado.

Ejemplo: Diferencia simétrica

Antes de seguir:

Observación: Como implicancia de este teorema, tenemos por ejemplo que $(\mathbb{Z}_3, +_3)$ sólo puede tener subgrupos de orden 1 ó 3. Si $(H, +_3)$ es un subgrupo de orden 1, entonces debe tenerse que $H = \{[0]_3\}$, y si $(H, +_3)$ es un subgrupo de orden 3, entonces necesariamente $H = \mathbb{Z}_3$ (ejercicio para el lector). Es decir, los únicos subgrupos que tiene $(\mathbb{Z}_3, +_3)$ son los triviales. Este resultado es también válido para $(\mathbb{Z}_p, +_p)$ con p primo.

Sea A un conjunto no vacío. Veamos que $(\mathcal{P}(A), \Delta)$ es un grupo abeliano, donde Δ denota la diferencia simétrica

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X) = (X \cup Y) \setminus (X \cap Y)$$

Demostración. 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, notando que $X \Delta X = (X \setminus X) \cup (X \setminus X) = \emptyset \cup \emptyset = \emptyset$, obtenemos que todo $X \in \mathcal{P}(A)$ es invertible, y que $X^{-1} = X$ (es decir, cada elemento es su propio inverso).

10.5. Morfismos

Sean $(A, *)$ y $(B, \triangle)$ dos estructuras algebraicas, y sea $f : A \to B$ una función. Sabemos que si $x, y \in A$ entonces $f(x), f(y) \in B$. Como sobre A tenemos definida una operación $*$, podemos hacernos la pregunta: ¿cuánto vale $f(x * y)$?

Los morfismos serán las funciones de A en B tales que $f(x*y)$ se construye operando $f(x)$ y $f(y)$, es decir tales que $f(x*y) = f(x)\triangle f(y)$ (recordemos que como $f(x), f(y) \in B$, entonces la operación que podemos aplicarles no es $*$, sino $\triangle$).

Definición 10.6 (Morfismo). *Una función $f : A \to B$ es un* **homomorfismo***, o simplemente un* **morfismo***, si*

$$(\forall x, y \in A)\ f(x*y) = f(x)\triangle f(y)$$

Definición 10.7 (Isomorfismo). *Si $f : A \to B$ es un morfismo, y además es una función biyectiva, entonces le llamaremos* **isomorfismo***.*

Si existe un isomorfismo $f : A \to B$, diremos que $(A, *)$ y $(B, \triangle)$ son **estructuras isomorfas**, lo cual denotaremos $(A, *) \cong (B, \triangle)$. $\cong$ resulta ser una relación de equivalencia entre estructuras algebraicas con una operación.

Propiedad 18.

$$(\mathbb{R}_+, \cdot) \cong (\mathbb{R}, +)$$

Demostración. Consideremos la función

$$\begin{array}{rccc} \log: & \mathbb{R}_+ & \to & \mathbb{R} \\ & x & \to & \log(x) \end{array}$$

log es una función biyectiva, y cumple $\log(x \cdot y) = \log(x) + \log(y)$ para $x, y \in \mathbb{R}_+$.

Morfismos sobreyectivos

Propiedades 14. *Sean $(A, *)$ y $(B, \triangle)$ estructuras algebraicas, y sea $f : A \to B$ un morfismo sobreyectivo. Se tiene que:*

1. *Si $*$ es asociativa, entonces $\triangle$ también.*
2. *Si $*$ es conmutativa, entonces $\triangle$ también.*
3. *Si $(A, *)$ tiene neutro $e \in A$, entonces $(B, \triangle)$ también tiene neutro, el cual es $f(e)$.*
4. *Sea $(A, *)$ es asociativa con neutro e, y sea $a \in A$. Si a posee inverso a^{-1}, entonces $f(a)$ también posee inverso, y más aún, $(f(a))^{-1} = f(a^{-1})$.*

Demostración. Demostraremos lo segundo.
Sean $b_1, b_2 \in B$. Como f es sobreyectiva, entonces existen $a_1, a_2 \in A$ tales que

$$f(a_1) = b_1 \quad \wedge \quad f(a_2) = b_2$$

Entonces

$$\begin{array}{rll} & b_1 \triangle b_2 & \\ = & f(a_1)\triangle f(a_2) & \\ = & f(a_1 * a_2) & (f \text{ es morfismo}) \\ = & f(a_2 * a_1) & (* \text{ es conmutativa}) \\ = & f(a_2)\triangle f(a_1) & (f \text{ es morfismo}) \\ = & b_2 \triangle b_1 & \end{array}$$

Tarea 10.1: Demuestre que:

1. La composición de morfismos es un morfismo.
2. Si f es un isomorfismo de $(A, *)$ en $(B, \triangle)$ entonces f^{-1} es también un isomorfismo pero de $(B, \triangle)$ en $(A, *)$.
3. La relación de isomrofía entre estructuras algebraicas ($\cong$) es una relación de equivalencia.

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 el es 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 al dos inversos.

9. ☐ En un grupo no vacío no existen elementos cancelables.

10. ☐ En un grupo no vacío 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 un grupo $(G, *)$ y $a \in G$ idempotente, el conjunto $\{a, a * a\}$ tiene dos elementos.

21. ☐ Dado un grupo $(G, *)$ y $a \in G$ idempotente, el conjunto $\{a, a * a\}$ tiene un elemento.

22. ☐ Dado un grupo $(G, *)$, de neutro e y $a \in G$ idempotente, el conjunto $\{a, a * a\}$ es igual a $\{e\}$.

23. ☐ Dado un grupo $(G, *)$, un subconjunto no vacío $H \subseteq G$ de dice subgrupo de G si $*$ es cerrada en H.

24. ☐ Dado un grupo $(G, *)$, un subconjunto no vacío $H \subseteq G$ de dice subgrupo de G si $(H, *)$ es también grupo.

25. ☐ Dado un grupo $(G, *)$, un ejemplo de subgrupo de G es $(\emptyset, *)$.

26. ☐ G es siempre subgrupo de sí mismo (para la misma operación).

27. ☐ G es subgrupo de sí mismo sólo cuando $(G, *)$ es abeliano.

28. ☐ Dado un grupo $(G, *)$ y H un subgrupo, el neutro de H es a veces distinto del de G.

29. ☐ Dado un grupo $(G, *)$ y H un subgrupo, el inverso de un elemento $x \in H$ pertenece a $G \setminus H$.

30. ☐ Dado un grupo $(G, *)$ y H un subgrupo, el inverso de un elemento $x \in H$ pertenece a H.

31. ☐ Dado un grupo $(G, *)$, para probar que $H \subseteq G$ es subgrupo basta verificar que $\forall x, y \in H,\ x * y \in H$.

32. ☐ Dado un grupo $(G, *)$, para probar que $H \subseteq G$ es subgrupo basta verificar que $\forall x, y \in H,\ x * y^{-1} \in H$.

33. ☐ Dado $n \geq 2$, $(\mathbb{Z}_n, +_n)$ es un grupo.

34. ☐ Dado $n \geq 2$, $(\mathbb{Z}_n \setminus \{[0]_n\}, +_n)$ es un grupo.

35. ☐ Dado un grupo finito $(G, *)$ y cualquier subgrupo $H \subseteq G$, $|G|$ es múltiplo de $|H|$.

36. ☐ Dado un grupo finito $(G, *)$ y cualquier subgrupo $H \subseteq G$, existe $k \in \mathbb{N}$ tal que $|G| = k|H|$.

37. ☐ Si un grupo G tiene un subgrupo con 16 elementos, entonces $|G|$ es par.

38. ☐ $(\mathbb{Z}_7, +_7)$ tiene subgrupos de tama no 5.

39. ☐ Dado $p > 1$ primo, $(\mathbb{Z}_p, +_p)$ tiene al menos tres subgrupos distintos.

40. ☐ Un morfismo entre estructuras se dice isomorfismo si es inyectivo.

41. ☐ $(\mathbb{R}, \cdot) \cong (\mathbb{R}, +)$.

42. ☐ $(\mathbb{R}_+, \cdot) \cong (\mathbb{R}, +)$.

43. ☐ Un morfismo entre las estructuras $(A, *)$ y $(B, \triangle)$ satisface que $(\forall x, y \in A)\ f(x) \triangle f(y) = f(x * y)$.

44. ☐ Dado un morfismo entre dos grupos $(A, *)$ y $(B, \triangle)$, la preimagen del neutro de B contiene al neutro de A.

45. ☐ Existen morfismos no sobreyectivos entre dos grupos $(A, *)$ y $(B, \triangle)$ tales que la preimagen del neutro de B es vacía.

46. ☐ Dado un morfismo sobreyectivo f, entre los grupos $(A, *)$ y $(B, \triangle)$, se tiene que para $x \in A$, $(f(x^{-1}))^{-1} = f(x)$.

47. ☐ Dado un morfismo sobreyectivo 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.

Guía de Ejercicios

1. Se nale 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. Dado $(G, *)$ grupo y $H \subseteq G$, subgrupo. Pruebe las siguientes propiedades, propuestas en la tutoría:

(a) $(\forall x, y \in H)\ x * y^{-1} \in H$.

(b) Si $e \in G$ es el neutro de G y $e_H \in H$ es el neutro de H, entonces $e = e_H$.

(c) Sea $x \in H$. Si $x^{-1} \in G$ es el inverso de x en $(G, *)$ y $\tilde{x} \in H$ es el inverso de x en $(H, *)$, entonces $x^{-1} = \tilde{x}$.

3. En la demostración de que $(\mathbb{Z}_n, +_n)$, para $n \geq 2$ es grupo, quedó como ejercicio demostrar la existencia de inversos. Es decir, demuestre que para cualquier $x \in \mathbb{Z}_n$, x admite un inverso para $+_n$.

4. 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 $(G, \circ)$.

5. 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 morfismo. 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) $\mathrm{Im}(f)$ es un subgrupo de $(G_2, \triangle)$.

(d) El conjunto $\{x \in G_1 \mid f(x) = e_2\}$ es un subgrupo de $(G_1, *)$.

Guía de Problemas

P1. (30 min.) Sea $(G, *)$ un grupo y $f : G \to G$ la función definida por $f(g) = g^{-1}$ para cada $g \in G$ (recordar que g^{-1} es el inverso de g para la operación $*$). Probar que

$$f \text{ es un isomorfismo } \Leftrightarrow G \text{ es un grupo Abeliano.}$$

P2. Sea $(G, *)$ un grupo con neutro $e \in G$ y

$$A = \{F : G \to G \ / \ F \text{ es un isomorfismo de } (G, *) \text{ en } (G, *)\}.$$

(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 $g, h \in G$.
- $F_e = id_G$ (id_G es la función identidad en 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 $B = \{F_g \ / \ g \in G\}$ es un subgrupo de $(A, \circ)$.

P3. (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. (Ind: calcule $(a * b) * (b * a)$).

P4. (20 min.) Sea $(G, *)$ un grupo tal que $G = \{e, a, b\}$ con e neutro en G. Pruebe que $a^{-1} = b$.

P5. Sean $(G, *)$ y $(H, \circ)$, grupos con neutros e_G y e_H respectivamente. Se define en $G \times H$ la ley de composición interna $\triangle$ por:

$$(a, b) \triangle (c, d) = (a * c, b \circ d)$$

(a) (20 min.) Demuestre que $(G \times H, \triangle)$ es grupo.

(b) (20 min.) Demuestre que las funciones φ y ψ definidas por

$$\varphi: \begin{array}{ccc} G \times H & \longrightarrow & G \\ (g, h) & \longmapsto & \varphi((g, h)) = g \end{array} \quad y, \quad \psi: \begin{array}{ccc} G \times H & \longrightarrow & H \\ (g, h) & \longmapsto & \psi((g, h)) = h \end{array}$$

son homomorfismos sobreyectivos.

(c) (20 min.) Considere $G = H$ y $* = \circ$ y la función $f : G \times G \to G$ definida por

$$f((a, b)) = (a * b)^{-1} \quad \forall (a, b) \in G \times G$$

Pruebe que

f es un homomorfismo de $(G \times G, \triangle)$ en $(G, *) \Leftrightarrow$ El grupo $(G, *)$ es abeliano.

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

SEMANA 11: ESTRUCTURAS ALGEBRAICAS Y NÚMEROS COMPLEJOS

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

10.6. Anillos

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 $(\mathbb{Z}_n, +_n, \cdot_n)$ puede ser un cuerpo si n cumple una condición especial.

Definición 10.8 (Anillo). *Una estructura $(A, +, \cdot)$ se llamará* **anillo** *si:*

- $(A, +)$ *es grupo abeliano.*
- $\cdot$ *es asociativa.*
- $\cdot$ *distribuye con respecto a* $+$.

- Para trabajar con una notación más familiar, al neutro de $(A, +)$ lo denotaremos 0, y para todo $x \in A$, a su inverso (para la operación $+$) se le denotará $-x$.

- Si la operación $\cdot$ posee neutro en A, éste se denotará por 1 y diremos que $(A, +, \cdot)$ es un **anillo con unidad**. Si $x \in A$ posee inverso para la operación $\cdot$, éste se denotará por x^{-1}.

- Si $\cdot$ es conmutativa, $(A, +, \cdot)$ se llamará **anillo conmutativo**.

Así, $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.

Relación entre ambos neutros

Observemos que $(\{a\}, +, \cdot)$ es una estructura algebraica si definimos

$$a + a = a \quad , \quad a \cdot a = a$$

Su principal curiosidad es que a es el neutro para ambas operaciones.
De acuerdo a las notaciones que mencionamos, en esta estructura (que resulta ser un anillo) se cumple que $0 = 1$.
Esta rara propiedad es única en su tipo, ya que

Proposición 10.3. *Si $(A, +, \cdot)$ es un anillo con unidad y A posee al menos dos elementos distintos, entonces $0 \neq 1$, o sea los neutros de ambas operaciones son distintos.*

Demostración. Como A posee dos elementos distintos, existe $a \in A$ con $a \neq 0$.

- Como el anillo posee unidad, tenemos que $1 \cdot a = a$.

- Por otro lado, tenemos que

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a \\ &= 0 \cdot a + 0 \cdot a \end{aligned}$$

por lo que

$$\begin{aligned} 0 \cdot a + (-0 \cdot a) &= (0 \cdot a + 0 \cdot a) + (-0 \cdot a) \\ 0 &= 0 \cdot a + (0 \cdot a + (-0 \cdot a)) \\ 0 &= 0 \cdot a \end{aligned}$$

Si fuera cierto que $0 = 1$, entonces tendríamos que $1 \cdot a = 0 \cdot a$, con lo que $a = 0$, lo que es una contradicción. Por lo tanto, debe tenerse que $0 \neq 1$.

Propiedades 15. *Sea $(A, +, \cdot)$ un anillo. Entonces:*

1. $(\forall x \in A)\ 0 \cdot x = x \cdot 0 = 0$
2. $(\forall x, y \in A)\ -(x \cdot y) = (-x) \cdot y = x \cdot (-y)$
3. $(\forall x, y \in A)\ (-x) \cdot (-y) = x \cdot y$
4. *Si el anillo posee unidad, entonces*

$$(\forall x \in A)\ -x = (-1) \cdot x = x \cdot (-1)$$

Demostración. Probaremos (1) y (4).
Para (1), veamos primero que:

$$\begin{aligned} 0 \cdot x &= (0+0) \cdot x \\ &= 0 \cdot x + 0 \cdot x \quad \text{Gracias a la distributividad.} \end{aligned}$$

Ahora, como A es grupo, $0 \cdot x$ es cancelable. Por lo que de lo anterior se concluye que $0 = 0 \cdot x$.
La demostración es análoga para $x \cdot 0$.
Para (4), debemos verificar que $x + (-1) \cdot x = 0$ (gracias a que Aes abeliano).
En efecto:

$$\begin{aligned} x + (-1) \cdot x &= 1 \cdot x + (-1) \cdot x \\ &= (1 + (-1)) \cdot x \quad \text{Por distributividad.} \\ &= 0 \cdot x \\ &= 0 \quad \text{Gracias a (1).} \end{aligned}$$

Luego $(-1) \cdot x$ es el opuesto de x y se concluye.

La demostración es también análoga para $x \cdot (-1)$.

$\mathbb{Z}_n$ como anillo

Sea $n \geq 2$. Recordemos que $(\mathbb{Z}_n, +_n)$ es un grupo abeliano. Si ahora consideramos $(\mathbb{Z}_n, +_n, \cdot_n)$, tenemos:

Proposición 10.4. *$(\mathbb{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo con unidad.*

DEMOSTRACIÓN. Demostraremos que $\cdot_n$ distribuye con respecto a $+_n$, y que $[1]_n$ es neutro para $\cdot_n$ (el resto de la demostración queda propuesta al lector).

Distributividad: Sean $[x]_n, [y]_n, [z]_n \in \mathbb{Z}_n$. Se tiene que

$$\begin{aligned} [x]_n \cdot_n ([y]_n +_n [z]_n) &= [x]_n \cdot_n [y+z]_n \\ &= [x \cdot (y+z)]_n \end{aligned}$$

Observamos que $x, y, z \in \mathbb{Z}$, por lo que $x \cdot (y+z) = x \cdot y + x \cdot z$. Entonces

$$\begin{aligned} [x]_n \cdot_n ([y]_n +_n [z]_n) &= [x \cdot y + x \cdot z]_n \\ &= [x \cdot y]_n +_n [x \cdot z]_n \\ &= [x]_n \cdot_n [y]_n +_n [x]_n \cdot_n [z]_n \end{aligned}$$

El cálculo para $([y]_n +_n [z]_n) \cdot_n [x]_n$ se hace de forma análoga.

Unidad: Sea $[x]_n \in \mathbb{Z}_n$. Se tiene

$$\begin{aligned} [x]_n \cdot_n [1]_n = [x \cdot 1]_n = [x]_n \\ [1]_n \cdot_n [x]_n = [1 \cdot x]_n = [x]_n \end{aligned}$$

por lo que $[1]_n$ es neutro para $\cdot_n$.

Divisores de cero

Sea $(A, +, \cdot)$ un anillo. Si existen $x, y \in A \setminus \{0\}$ tales que $x \cdot y = 0$, entonces llamaremos a x e y **divisores de cero**.
Esta noción 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:

$$[2]_6 \cdot_6 [3]_6 = [6]_6 = [0]_6$$

Propiedad 19. *Sea $(A, +, \cdot)$ un anillo. Sea $a \in A \setminus \{0\}$. Entonces*

$$a \text{ es divisor de cero} \iff a \text{ no es cancelable}$$

DEMOSTRACIÓN. Sea $a \in A$ divisor de cero, esto equivale a:

$$(\exists y \in A)\ (a \cdot y = 0 \wedge y \neq 0) \ \Leftrightarrow\ (\exists y \in A)\ (a \cdot y = a \cdot 0 \wedge y \neq 0)$$

Lo que es precisamente la negación de la proposición:

$$(\forall x, y \in A)\ (a \cdot x = a \cdot y\ \Rightarrow x = y).$$

O sea, a es cancelable.

10.7. Cuerpos

Definición 10.9 (Cuerpo). *Sea $(K, +, \cdot)$ una estructura algebraica. Le llamaremos* **cuerpo** *si cumple*

- *$(K, +, \cdot)$ es anillo conmutativo con unidad.*
- *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 $+$.

Así, observamos que $(\mathbb{R}, +, \cdot)$ es un cuerpo.

Cuerpos y divisores de cero

Propiedad 20. *Un cuerpo no tiene divisores de cero.*

Demostración. Sea $(K, +, \cdot)$ un cuerpo. Supongamos que tuviera divisores de cero, es decir, que existen $x, y \in K \setminus \{0\}$ tales que $x \cdot y = 0$.
Como $y \neq 0$ y K es cuerpo, entonces existe su inverso $y^{-1} \in K$. Así

$$x = x \cdot (y \cdot y^{-1}) = (x \cdot y) \cdot y^{-1} = 0 \cdot y^{-1} = 0$$

lo que es una contradicción.

Lamentablemente, no todo anillo conmutativo con unidad y sin divisores de cero es un cuerpo. Un ejemplo es $(\mathbb{Z}, +, \cdot)$: no tiene divisores de cero, pero sus únicos elementos que poseen inverso multiplicativo son 1 y -1.
Sin embargo, el caso de anillos de cardinal finito es distinto.

Propiedad 21. *Sea $(A, +, \cdot)$ un anillo conmutativo con unidad tal que $|A|$ es finito. Entonces*

$$(A, +, \cdot) \text{ no tiene divisores de cero} \iff (A, +, \cdot) \text{ es cuerpo}$$

Demostración. La implicancia $\Leftarrow$ es directa. Para la implicancia $\Rightarrow$, dado $x \in A \setminus \{0\}$, definamos por recurrencia:

$$\begin{aligned} x^0 &= 1 \\ x^k &= x \cdot x^{k-1}, \quad \forall k \geq 1. \end{aligned}$$

Es decir la noción de potencia para la operación $\cdot$. Se tiene que existen $i, j \geq 1$ distintos tales que $x^i = x^j$. De lo contrario el conjunto $\{x^k \mid k \in \mathbb{N}\}$ sería un subconjunto de A infinito. Contradiciendo que $|A|$ es finito.
Luego:

$$\begin{aligned} x^i = x^j &\Leftrightarrow x^i = x^{j-i} \cdot x^i \quad \text{Suponiendo, sin perder generalidad que } i < j. \\ &\Leftrightarrow 1 \cdot x^i = x^{j-i} \cdot x^i \end{aligned}$$

Y como $(A, +, \cdot)$ no tiene divisores de cero, todo elemento en A es cancelable. En particular x^i lo es, luego:

$$1 = x^{j-i} \Leftrightarrow 1 = x \cdot x^{j-i-1}.$$

Por lo que como $(A, +, \cdot)$ es conmutativo, $x^{-1} = x^{j-i-1}$.
Esto prueba que $(A, +, \cdot)$ es cuerpo, pues todo elemento $x \in A \setminus \{0\}$ posee inverso.

Ejemplo: $\mathbb{Z}_n$ como cuerpo

Teorema 10.3. *Sea $n \in \mathbb{N}$ con $n \geq 2$. Las siguientes afirmaciones son equivalentes:*

1. *$(\mathbb{Z}_n, +_n, \cdot_n)$ es un cuerpo*
2. *$(\mathbb{Z}_n, +_n, \cdot_n)$ no tiene divisores de cero*
3. *n es un número primo*

DEMOSTRACIÓN.

- $1 \Rightarrow 2$ sale de una propiedad anterior.
- $2 \Rightarrow 3$ queda propuesto como ejercicio. Es recomendable demostrar la contrarecíproca.
- Para $3 \Rightarrow 1$, sabemos que $(\mathbb{Z}_n, +_n, \cdot_n)$ es un anillo conmutativo con unidad. Sólo basta verificar que todo elemento no nulo tiene inverso para el producto.

  Sea $[k]_n \in \mathbb{Z}_n \setminus \{[0]_n\}$. Podemos considerar que $1 \leq k \leq n-1$.

  Como n es un número primo (hipótesis), entonces k y n son primos relativos: El máximo común divisor entre ellos es 1.

  Una consecuencia no muy difícil de probar del Teorema de la división en $\mathbb{Z}$ es la "Igualdad de Bezout", que dice que existen enteros $r, s \in \mathbb{Z}$ tales que $1 = rk + sn$.

  De aquí, sale que:

$$\begin{aligned} rk = 1 + sn &\Leftrightarrow [rk]_n = [1]_n \\ &\Leftrightarrow [r]_n \cdot_n [k]_n = [1]_n. \end{aligned}$$

  Es decir, $[r]_n$ es el inverso de $[k]_n$.

Usando la transitividad de $\Rightarrow$, se concluyen las equivalencias.

11. Números complejos

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 ecuación

$$x^2 = -1$$

no tiene soluciones. 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 11.1 (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 $z = (z_1, z_2), w = (w_1, w_2) \in \mathbb{C}$*

$$\begin{aligned} z + w &= (z_1 + w_1, z_2 + w_2) \\ z \cdot w &= (z_1 w_1 - z_2 w_2, z_1 w_2 + w_1 z_2) \end{aligned}$$

Teorema 11.1. $(\mathbb{C}, +, \cdot)$ *es un cuerpo.*

DEMOSTRACIÓN. Demostraremos algunas de las propiedades necesarias, el resto quedan de ejercicio para el lector.
Neutro aditivo: $(0,0)$ es el neutro para $+$. En efecto, si $z = (z_1, z_2) \in \mathbb{C}$

$$z + (0,0) = (z_1 + 0, z_2 + 0) = (z_1, z_2) = z$$
$$(0,0) + z = (0 + z_1, 0 + z_2) = (z_1, z_2) = z$$

Opuestos aditivos: Sea $z = (z_1, z_2) \in \mathbb{C}$. Entonces

$$z + (-z_1, -z_2) = (z_1 - z_1, z_2 - z_2) = (0,0)$$
$$(-z_1, -z_2) + z = (-z_1 + z_1, -z_2 + z_2) = (0,0)$$

por lo que $-z = (-z_1, -z_2)$.
Conmutatividad de $\cdot$: Sean $z = (z_1, z_2), w = (w_1, w_2) \in \mathbb{C}$.

$$\begin{aligned} z \cdot w &= (z_1 w_1 - z_2 w_2, z_1 w_2 + w_1 z_2) \\ &= (w_1 z_1 - w_2 z_2, w_1 z_2 + w_2 z_1) \\ &= w \cdot z \end{aligned}$$

Distributividad: Sean $z = (z_1, z_2), w = (w_1, w_2), v = (v_1, v_2) \in \mathbb{C}$.

$$\begin{aligned} z \cdot (w + v) &= z \cdot (w_1 + v_1, w_2 + v_2) \\ &= (z_1(w_1 + v_1) - z_2(w_2 + v_2), z_1(w_2 + v_2) + z_2(w_1 + v_1)) \\ &= ((z_1 w_1 - z_2 w_2) + (z_1 v_1 - z_2 v_2), (z_1 w_2 + z_2 w_1) + (z_1 v_2 + z_2 v_1)) \\ &= (z_1 w_1 - z_2 w_2, z_1 w_2 + z_2 w_1) + (z_1 v_1 - z_2 v_2, z_1 v_2 + z_2 v_1) \\ &= z \cdot w + z \cdot v \end{aligned}$$

(no hace falta calcular $(w + v) \cdot z$ pues ya demostramos que $\cdot$ es conmutativa)

Inverso multiplicativo: Sea $z = (z_1, z_2) \in \mathbb{C} \backslash \{(0,0)\}$. Definamos $w = \left(\frac{z_1}{z_1^2 + z_2^2}, \frac{-z_2}{z_1^2 + z_2^2} \right)$. Entonces

$$z \cdot w = \left(\frac{z_1^2}{z_1^2 + z_2^2} - \frac{-z_2^2}{z_1^2 + z_2^2}, \frac{-z_1 z_2}{z_1^2 + z_2^2} + \frac{z_1 z_2}{z_1^2 + z_2^2} \right) = (1,0)$$

(verificar que $(1,0)$ es el neutro de $\cdot$)

Al igual que en $\mathbb{R}$, asumiremos las notaciones siguientes: para $z, w \in \mathbb{C}$

$$\begin{aligned} z - w &= z + (-w) \\ \frac{z}{w} &= z \cdot w^{-1} \quad \text{si } w \neq 0 \end{aligned}$$

En $\mathbb{C}$ también valen algunas fórmulas que cumplen los números reales, como

Propiedad 22.

$$\begin{aligned} (z + w)^2 &= z^2 + 2zw + w^2 \\ (z + w)(z - w) &= z^2 - w^2 \\ \sum_{k=a}^{b} z^k &= \frac{z^a - z^{b+1}}{1 - z} \quad si\ z \neq 1 \end{aligned}$$

11.1. Relación con $\mathbb{R}$

Nuestro deseo original era que $\mathbb{C}$ resultara ser una extensión de $\mathbb{R}$. Pues bien, resulta que $\mathbb{C}$ contiene un subconjunto R tal que $(R, +, \cdot)$ es isomorfo a los números reales.

Proposición 11.1. *Sea* $R = \{(z_1, z_2) \in \mathbb{C} : z_2 = 0\} \subseteq \mathbb{C}$. *Entonces* $(R, +, \cdot)$ *es isomorfo a* $(\mathbb{R}, +, \cdot)$.

Demostración. Sea la función $\phi : \mathbb{R} \to R$ dada por

$$\phi(x) = (x, 0)$$

Es fácil demostrar que ϕ es biyectiva. Veamos que es morfismo (para ambas operaciones).
Sean $x, y \in \mathbb{R}$. Se tiene que

$$\phi(x + y) = (x + y, 0) = (x, 0) + (y, 0) = \phi(x) + \phi(y)$$

y también

$$\phi(x \cdot y) = (x \cdot y, 0) = (x \cdot y - 0 \cdot 0, x \cdot 0 + 0 \cdot y) = (x, 0) \cdot (y, 0) = \phi(x) \cdot \phi(y)$$

Como cada real x se identifica con el complejo $(x, 0)$, entonces el complejo $(-1, 0)$ corresponde al -1 de $\mathbb{R}$. Notemos que la ecuación $z^2 = (-1, 0)$ sí tiene solución:

$$(0, 1)^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$$

Aunque no lo demostraremos, es importante señalar que $(\mathbb{C}, +, \cdot)$ resulta ser el cuerpo más pequeño que contiene a $(\mathbb{R}, +, \cdot)$ en el cual la ecuación $x^2 = -1$ posee solución.

11.2. Notación $a + bi$

Como los complejos de la forma $(x, 0)$ se identifican con los reales, entonces asumiremos la notación $(x, 0) = x$. Además, al complejo $(0, 1)$ le llamaremos i.

De esta forma, a un $(a, b) \in \mathbb{C}$ lo podemos escribir como

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + b \cdot i = a + bi$$

tomando la misma convención de $\mathbb{R}$ que dice que si entre dos números no hay ningún símbolo, entonces se multiplican.

Es importante notar que cuando se dice "sea $z = a + bi \in \mathbb{C}$", se da por entendido que $a, b \in \mathbb{R}$.

Habiendo dicho esto, tenemos que $i^2 = -1$, es decir, i es una solución de la ecuación con la que abrimos el capítulo.

La notación $a + bi$ permite multiplicar complejos con mucha facilidad:

$$\begin{aligned} (a + bi)(x + yi) &= ax + ayi + bxi + byi^2 \\ &= (ax - by) + (ay + bx)i \end{aligned}$$

11.3. Partes real e imaginaria

Definición 11.2 (Partes real e imaginaria). *Sea $z = a + bi \in \mathbb{C}$. Definimos su* **parte real** *como el real*

$$\mathbb{R}e(z) = a$$

y su **parte imaginaria** *como el real*

$$\mathbb{I}m(z) = b$$

Así, un complejo $z \in \mathbb{C}$ se puede escribir como

$$z = \mathbb{R}\mathrm{e}(z) + i\mathbb{I}\mathrm{m}(z)$$

Las partes real e imaginaria cumplen las siguientes propiedades:

Propiedades 16. *Para $z_1, z_2 \in \mathbb{C}$ y $\alpha \in \mathbb{R}$:*

1. $\mathbb{R}e(z_1 + z_2) = \mathbb{R}e(z_1) + \mathbb{R}e(z_2)$
2. $\mathbb{I}m(z_1 + z_2) = \mathbb{I}m(z_1) + \mathbb{I}m(z_2)$
3. $\mathbb{R}e(\alpha z) = \alpha\mathbb{R}e(z)$
4. $\mathbb{I}m(\alpha z) = \alpha\mathbb{I}m(z)$
5. $z_1 = z_2 \iff \mathbb{R}e(z_1) = \mathbb{R}e(z_2) \wedge \mathbb{I}m(z_1) = \mathbb{I}m(z_2)$

Estas propiedades quedan propuestas como ejercicio.

11.4. Conjugación

Definición 11.3 (Conjugado). *Sea $z = a + bi \in \mathbb{C}$. Definimos el* **conjugado** *de z como el complejo*

$$\bar{z} = a - bi$$

Propiedades 17. *Sean $z, w \in \mathbb{C}$. Se tiene:*

1. $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{z - w} = \bar{z} - \bar{w}$
2. $\overline{z \cdot w} = \bar{z} \cdot \bar{w}$
3. *Si $\lambda \in \mathbb{R}$, entonces* $\overline{\lambda z} = \lambda\bar{z}$
4. *Si $w \neq 0$,* $\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$
5. $\bar{\bar{z}} = z$
6. $\mathbb{R}e(z) = \mathbb{R}e(\bar{z})$, $\mathbb{I}m(z) = -\mathbb{I}m(\bar{z})$
7. $\mathbb{R}e(z) = \frac{1}{2}(z + \bar{z})$, $\mathbb{I}m(z) = \frac{1}{2i}(z - \bar{z})$
8. $z \in \mathbb{R} \iff z = \bar{z}$

Demostración. Demostraremos (2) y (8).
Para (2): Sean $z = z_1 + z_2 i, w = w_1 + w_2 i \in \mathbb{C}$. Tenemos la fórmula

$$z \cdot w = (z_1 w_1 - z_2 w_2) + i(z_1 w_2 + z_2 w_1)$$

por lo que

$$\begin{aligned} \overline{z \cdot w} &= (z_1 w_1 - z_2 w_2) - i(z_1 w_2 + z_2 w_1) \\ &= (z_1 - z_2 i)(w_1 - w_2 i) \\ &= \bar{z} \cdot \bar{w} \end{aligned}$$

Para (8): Por doble implicancia.
$\Rightarrow$) Si $z \in \mathbb{R}$, entonces existe $x \in \mathbb{R}$ tal que $z = x = x + 0i$. Entonces

$$\bar{z} = x - 0i = x = z$$

$\Leftarrow$) Si $z = \bar{z}$, entonces (utilizando la propiedad (7)

$$z = \frac{1}{2}(z + \bar{z}) = \mathbb{R}\mathrm{e}(z) \in \mathbb{R}$$

11.5. Módulo

Definición 11.4 (Módulo). *Sea $z = a + bi \in \mathbb{C}$. El* **módulo** *de z es el valor*

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

Así, para cualquier $z \in \mathbb{C}$, se tiene que $|z| \in \mathbb{R}$ y $|z| \geq 0$.

Propiedades 18. *Para $z, w \in \mathbb{C}$, se tiene:*

1. $|z|^2 = z \cdot \bar{z}$
2. $|z| = |\bar{z}|$
3. $|\mathbb{R}e(z)| \leq |z|$, $|\mathbb{I}m(z)| \leq |z|$
4. $z = 0 \iff |z| = 0$
5. $|z \cdot w| = |z| \cdot |w|$
6. *Desigualdad triangular:* $|z + w| \leq |z| + |w|$
7. *Si $z \neq 0$, entonces* $z^{-1} = \frac{\bar{z}}{|z|^2}$
8. *Si $w \neq 0$,* $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$

Demostración. Demostraremos (1) y (7).
Para (1): Sea $z = a + bi \in \mathbb{C}$.

$$z \cdot \bar{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 - b^2 i^2 = a^2 + b^2 = |z|^2$$

Para (7): Sea $z \in \mathbb{C} \setminus \{0\}$, y denotemos $w = \frac{\bar{z}}{|z|^2} \in \mathbb{C}$.

$$z \cdot w = \frac{z \cdot \bar{z}}{|z|^2} = \frac{|z|^2}{|z|^2} = 1$$

por lo que $z^{-1} = w$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ $(A,+,\cdot)$ es un anillo si y sólo si $(A,+)$ es un grupo abeliano.

2. ☐ $(A,+,\cdot)$ es un anillo si y sólo si $(A,+)$ es un grupo abeliano y $\cdot$ es asociativa.

3. ☐ $(A,+,\cdot)$ es un anillo si y sólo si $(A,+)$ es un grupo abeliano, $\cdot$ es asociativa y distribuye con respecto a $+$.

4. ☐ $(\mathbb{Z},+,\cdot)$ es un anillo.

5. ☐ Todo anillo $(A,+,\cdot)$ tiene neutro para la operación $\cdot$.

6. ☐ En todo anillo $(A,+,\cdot)$ la operación $\cdot$ es conmutativa.

7. ☐ Todo anillo $(A,+,\cdot)$ tiene neutro para la operación $+$.

8. ☐ En todo anillo $(A,+,\cdot)$ la operación $+$ es conmutativa.

9. ☐ $(\mathbb{Z},+,\cdot)$ es un anillo conmutativo con unidad.

10. ☐ En todo anillo $(A,+,\cdot)$, el neutro para $\cdot$ y para $+$ son elementos distintos.

11. ☐ En todo anillo $(A,+,\cdot)$, con más de un elemento, el neutro para $\cdot$ y para $+$ son elementos distintos.

12. ☐ Si $(A,+,\cdot)$ es un anillo, se cumple que $(\forall x \in A)\ 0 \cdot x = x \cdot 0 = 0$

13. ☐ Si $(A,+,\cdot)$ es un anillo, $x, y \in A$, entonces $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

14. ☐ $(\mathbb{Z}_9,+,\cdot)$ es un anillo.

15. ☐ $(\mathbb{Z}_9,+,\cdot)$ es un anillo conmutativo con unidad.

16. ☐ $(\mathbb{Z}_9,+,\cdot)$ es un anillo conmutativo con unidad sin divisores del cero.

17. ☐ $(\mathbb{Z}_7,+,\cdot)$ es un anillo conmutativo con unidad sin divisores del cero.

18. ☐ $(\mathbb{Z}_{17},+,\cdot)$ es un anillo conmutativo con unidad sin divisores del cero.

19. ☐ $[1]_p$ es el neutro para $\cdot_p$ en el anillo $(\mathbb{Z}_p,+,\cdot)$.

20. ☐ En $(\mathbb{Z}_9,+,\cdot)$ se cumple que $[3]_9 \cdot_9 [3]_9 = [0]_9$.

21. ☐ Todo cuerpo es un anillo.

22. ☐ $(\mathbb{Z}_9,+,\cdot)$ es un cuerpo.

23. ☐ $(\mathbb{R},+,\cdot)$ es un anillo.

24. ☐ $(\mathbb{R},+,\cdot)$ es un cuerpo.

25. ☐ En todo cuerpo, $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$

26. ☐ Todo anillo finito sin divisores del cero es un cuerpo.

27. ☐ Todo anillo finito conmutativo con unidad sin divisores del cero es un cuerpo.

28. ☐ Para p primo, $(\mathbb{Z}_p,+,\cdot)$ es un cuerpo.

Guía de Ejercicios

Observación: En esta guía se entiende como *plano complejo*, la representación como $\mathbb{R} \times \mathbb{R}$ de $\mathbb{C}$.

1. **(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.

2. Demuestre, para un anillo $(A, +, \cdot)$, las siguientes propiedades propuestas en la tutoría:

(a) $(\forall x, y \in A)\ -(x \cdot y) = (-x) \cdot y = x \cdot (-y)$.

(b) $(\forall x, y \in A)\ (-x) \cdot (-y) = x \cdot y$.

3. Pruebe que en un anillo con más de dos elementos, el neutro para la operación $\cdot$ y para la operación $+$ son necesariamente distintos.

4. 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 $I = \{x \in A : f(x) = 0'\}$.

(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 $A = I$.

5. Pruebe que si $(\mathbb{Z}_n, +_n, \cdot_n)$ no tiene divisores de cero, entonces n es un número primo.

6. Demuestre, dados $z_1, z_2 \in \mathbb{C}$ y $\alpha \in \mathbb{R}$, las siguientes propiedades propuestas en la tutoría:

(a) $\mathbb{R}\mathrm{e}(z_1 + z_2) = \mathbb{R}\mathrm{e}(z_1) + \mathbb{R}\mathrm{e}(z_2)$.

(b) $\mathbb{I}\mathrm{m}(z_1 + z_2) = \mathbb{I}\mathrm{m}(z_1) + \mathbb{I}\mathrm{m}(z_2)$.

(c) $\mathbb{R}\mathrm{e}(\alpha z) = \alpha \mathbb{R}\mathrm{e}(z)$.

(d) $\mathbb{I}\mathrm{m}(\alpha z) = \alpha \mathbb{I}\mathrm{m}(z)$.

(e) $z_1 = z_2 \iff \mathbb{R}\mathrm{e}(z_1) = \mathbb{R}\mathrm{e}(z_2) \wedge \mathbb{I}\mathrm{m}(z_1) = \mathbb{I}\mathrm{m}(z_2)$.

7. Demuestre las siguientes propiedades, dados $z, w \in \mathbb{C}$

(a) $\overline{z + w} = \bar{z} + \bar{w}$, $\overline{z - w} = \bar{z} - \bar{w}$.

(b) Si $w \neq 0$, $\overline{\left(\frac{z}{w}\right)} = \frac{\bar{z}}{\bar{w}}$.

(c) $\mathbb{R}\mathrm{e}(z) = \frac{1}{2}(z + \bar{z})$, $\mathbb{I}\mathrm{m}(z) = \frac{1}{2i}(z - \bar{z})$.

8. 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) $\overline{\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)}\left(\frac{\sqrt{3}}{2}+\frac{1}{2}i\right)$.

9. Demuestre, dados $z, w \in \mathbb{C}$, las siguientes propiedades:

(a) $|z|^2 = z \cdot \bar{z}$.

(b) $z = 0 \iff |z| = 0$.

(c) $|z \cdot w| = |z| \cdot |w|$.

(d) Si $w \neq 0$, $\left|\frac{z}{w}\right| = \frac{|z|}{|w|}$.

10. Encuentre la intersección de las siguientes regiones del plano complejo

$$R_1 = \{z \in \mathbb{C} : |z-1| \leq 1\} \qquad R_2 = \{z \in \mathbb{C} : |z-2| \leq 1\}.$$

Indicación: Grafique.

Guía de Problemas

P1. **(a)** 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	

1.1) (30 min.) Considerando las propiedades generales del anillo, complete las tablas anteriores justificando cada relleno. (Ind.: complete primero la tabla para $\oplus$ y para $\odot$ utilice adecuadamente la distributividad).

2.2) (10 min.) ¿Es $(A, \oplus, \odot)$ conmutativo?. ¿Posee $(A, \oplus, \odot)$ unidad?. ¿Tiene divisores del cero?

(b) (30 min.) Si $(A, +, \cdot)$ es un anillo tal que $x \cdot x = x \quad \forall x \in A$. Demuestre que

c.1) $x = -x \quad \forall x \in A$ ($-x$ es inverso aditivo de x)

c.2) $(A, +, \cdot)$ es anillo conmutativo.

c.3) $(x \cdot y) \cdot (x + y) = 0 \quad \forall x, y \in A$.

P2. Considere en $\mathbb{R}^2$ las operaciones $(a, b) \oplus (c, d) = (a + c, b + d)$ y $(a, b) \odot (c, d) = (a \cdot c, b \cdot d)$

a) (30 min.) Pruebe que $(\mathbb{R}^2, \oplus, \odot)$ es un anillo conmutativo con unidad.

b) (15 min.) Pruebe que $(\mathbb{R}^2, \oplus, \odot)$ posee divisores del cero.

c) (15 min.) Demuestre que $(\mathbb{R}^2, \oplus, \odot)$ no es isomorfo a $(\mathbb{C}, +, \cdot)$.

P3. **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 $|z_2| < 1$ se tiene

$$\frac{|z_1 - z_2|}{|1 - z_2\overline{z}_1|}$$

P4. (10 min.) Sea $z \in \mathbb{C}$ tal que $|z| \neq 1$ y considere $n \geq 1$. Probar que

$$\frac{1}{1 + z^n} + \frac{1}{1 + \overline{z}^n} \in \mathbb{R}$$

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

12. Números Complejos

12.1. Forma polar de los complejos

Introducción

Recordemos que definimos $\mathbb{C}$ a partir de $\mathbb{R}^2$. Es por esto que podemos dar a los complejos una interpretación de vectores en dos dimensiones, como muestra la siguiente figura.

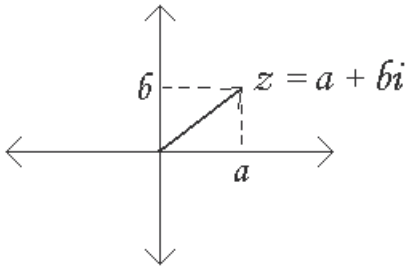

Figura 11: Representación del "plano" complejo.

Si $z = a+bi \in \mathbb{C}$, entonces $-z = -a-bi$ y $\bar{z} = a-bi$. De este modo, geométricamente $-z$ es el vector opuesto a z, y $\bar{z}$ es el vector reflejado de z con respecto al eje horizontal, al cual se le llama **eje real**. Al eje vertical se le llama **eje imaginario**.

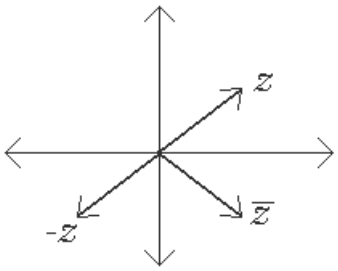

Figura 12: Representación gráfica de z, $-z$ y $\bar{z}$.

12.2. El complejo $e^{i\theta}$

De este modo, interpretamos la suma de dos números complejos como la suma de vectores en $\mathbb{R}^2$. ¿Cómo interpretar el producto entre complejos?
Para ello utilizaremos la llamada **notación polar**.

Definición 12.1 (Definición). *Sea $\theta \in \mathbb{R}$. Definimos el complejo que denotaremos $e^{i\theta}$ como*

$$e^{i\theta} = \cos\theta + i\sin\theta$$

Utilizamos la notación de potencias pues el objeto $e^{i\theta}$ cumple las siguientes propiedades:

Propiedades 19. *1.* $e^{i\cdot 0} = 1$.

2. $(\forall \theta \in \mathbb{R})\ |e^{i\theta}| = 1$.

3. $(\forall \theta \in \mathbb{R})\ \overline{e^{i\theta}} = (e^{i\theta})^{-1} = e^{i(-\theta)}$ *(y lo denotaremos* $e^{-i\theta}$*).*

4. $(\forall \theta, \varphi \in \mathbb{R})\ e^{i\theta}e^{i\varphi} = e^{i(\theta+\varphi)}$.

5. $(\forall n \in \mathbb{Z})(\forall \theta \in \mathbb{R})\ (e^{i\theta})^n = e^{in\theta}$ *(a este resultado se le conoce como fórmula de Moivre).*

Demostración.

- (1), (2) y (3) quedan propuestos como ejercicios. Para la segunda igualdad de (3), usar (2) y la fórmula para z^{-1} vista en la tutoría anterior.
- Para (4) Sean $\theta, \varphi \in \mathbb{R}$.

$$\begin{aligned} e^{i(\theta+\varphi)} &= \cos(\theta+\varphi) + i\sin(\theta+\varphi) \\ &= (\cos\theta\cos\varphi - \sin\theta\sin\varphi) + i(\sin\theta\cos\varphi + \cos\theta\sin\varphi) \\ &= (\cos\theta + i\sin\theta)(\cos\varphi + i\sin\varphi) \\ &= e^{i\theta}e^{i\varphi} \end{aligned}$$

- Para (5) definamos inductivamente *potencias* de elementos en $\mathbb{C}$.

  Para $n \in \mathbb{N}$,

$$\begin{cases} z^0 = 1 \\ z^{n+1} = z^n \cdot z. \end{cases}$$

  Y para $n < 0$ en $\mathbb{Z}$, $z^n = (z^{-1})^{-n} = (z^{-n})^{-1}$. Esto siempre que z^{-1} exista, que en nuestro caso significa $z \neq 0$, lo cual es cierto para $e^{i\theta}$ gracias a (2).

  Ahora, para $n \in \mathbb{N}$ probamos la propiedad por inducción. El caso $n = 0$ sale de que por definición, $z^0 = 1$, y la propiedad (1).

  Para el paso inductivo, usamos (4). En efecto, si para $n \in \mathbb{N}$ es cierto que $(e^{i\theta})^{n+1} = e^{i(n\theta)}$, entonces

$$(e^{i\theta})^{n+1} = e^{i(n\theta)}e^{i\theta} = e^{i(n\theta+\theta)} = e^{i(n+1)\theta}.$$

  El caso $n < 0$, queda propuesto como ejercicio.

12.3. Definición de forma polar

En términos geométricos, $e^{i\theta}$ es el complejo de módulo 1 que forma un ángulo θ con el eje real, medido en sentido antihorario.

Propiedad 23. *Todo complejo* $z \in \mathbb{C}$ *se puede escribir de la forma* $z = re^{i\theta}$*, con* $r \geq 0$ *y* $\theta \in \mathbb{R}$*. A esta escritura se le llama* **forma polar**.

DEMOSTRACIÓN. Si $z = 0$, entonces $z = re^{i\theta}$ tomando $r = 0$ y $\theta \in \mathbb{R}$ cualquiera.

Si $z \neq 0$, entonces tomamos $r = |z|$, y θ el ángulo que forma z (visto como vector de $\mathbb{R}^2$) con el eje real. Este ángulo cumple

$$\cos\theta = \frac{\mathbb{R}\mathrm{e}(z)}{|z|} \quad \wedge \quad \sin\theta = \frac{\mathbb{I}\mathrm{m}(z)}{|z|}$$

De esta forma

$$re^{i\theta} = r(\cos\theta + i\sin\theta) = |z|\left(\frac{\mathbb{R}\mathrm{e}(z)}{|z|} + i\frac{\mathbb{I}\mathrm{m}(z)}{|z|}\right) = \mathbb{R}\mathrm{e}(z) + i\mathbb{I}\mathrm{m}(z) = z$$

A modo de ejemplo, calculemos la forma polar del complejo $z = 2 + 2i$.

$$r = |z| = \sqrt{2^2 + 2^2} = \sqrt{8}$$

Observando que z representa al vector $(2, 2) \in \mathbb{R}^2$, elegimos el ángulo $\theta = \pi/4$, con lo que

$$2 + 2i = \sqrt{8}\ e^{i\pi/4}$$

Es fácil ver que todo complejo posee una infinidad de posibles formas polares. Continuemos con el ejemplo $z = 2 + 2i$. El ángulo podría haber sido elegido como $2\pi + \pi/4$, con lo que

$$e^{i(2\pi+\pi/4)} = e^{i\ 2\pi}e^{i\pi/4} = (\cos(2\pi) + i\sin(2\pi))e^{i\pi/4} = (1 + i\cdot 0)e^{i\pi/4} = e^{i\pi/4}$$

por lo que también

$$2 + 2i = \sqrt{8}\ e^{i(2\pi+\pi/4)}$$

Más en general, el ángulo θ puede ser cambiado por $\theta + 2k\pi$ para cualquier $k \in \mathbb{Z}$ sin alterar el número complejo representado. Por esto, se acostumbra escoger el ángulo θ que cae en el rango $(-\pi, \pi]$.

Definición 12.2 (Módulo y argumento). *Si $z = re^{i\theta}$:*

- *Al valor r se le llama módulo, y se nota $|z|$.*
- *Al valor θ se le llama* **argumento**, *y se nota* $\arg(z)$.

Interpretación geométrica de la forma polar

Propiedad 24. *Sean $z, w \in \mathbb{C} \setminus \{0\}$.*

$$z = w \iff |z| = |w| \wedge (\exists k \in \mathbb{Z})\ \ \arg(z) = \arg(w) + 2k\pi$$

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 $w = \alpha \in \mathbb{R}$, entonces $z \cdot w = (\alpha r)e^{i\theta}$, es decir $z \cdot w$ es un estiramiento o contracción 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 ángulo $\varphi = \arg(w)$.
- De este modo, si $w = \rho e^{i\varphi}$, entonces $z \cdot w$ representa un estiramiento o contracción de z en un factor $|w|$, además de rotarlo en un ángulo $\arg(w)$.

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 $\cos\theta + i\,\mathrm{sen}\,\theta$.

19. ☐ El complejo $e^{i\theta}$ está definido como $\mathrm{sen}\,\theta - i\cos\theta$.

20. ☐ El complejo $e^{i\theta}$ está definido como $\mathrm{sen}\,\theta + \cos\theta$.

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. ☐ $2e^{i\frac{\pi}{2}} = 2e^{-i\frac{\pi}{2}}$.

Guía de Ejercicios

1. Demuestre las siguientes propiedades, propuestas en la tutoría:

(a) $e^{i0} = 1$.

(b) $(\forall \theta \in \mathbb{R})\ |e^{i\theta}| = 1$.

(c) $(\forall \theta \in \mathbb{R})\ \overline{e^{i\theta}} = (e^{i\theta})^{-1} = e^{i(-\theta)}$.

(d) Si $n \in \mathbb{Z}$, $n < 0$, entonces $(\forall \theta \in \mathbb{R})\ (e^{i\theta})^n = e^{in\theta}$ (es decir, complete la demostración de la Fórmula de Moivre para n negativo).

2. 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) $\dfrac{(2 + i)}{(2 - i)}$

3. 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) $\dfrac{(3e^{i\frac{\pi}{8}})}{(-4e^{i\frac{\pi}{4}})}$

4. 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) $|\frac{4i-z}{z-1+i}| = 1$

Guía de Problemas

P1. **(a)** (20 min.) Demuestre que $\forall z_1, z_2 \in \mathbb{C}$

$$z_1 \cdot \bar{z_2} + \bar{z_1} \cdot z_2 = 2|z_1 \cdot z_2| \cos\phi$$

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 $s = u - v$ y ϕ es el ángulo entre los complejos u y v. Demuestre que

$$|s|^2 = |u|^2 + |v|^2 - 2|u||v| \cos\phi$$

P2. (20 min.) Se define la relación $\mathcal{R} \subseteq \mathbb{C} \times \mathbb{C}$ por

$$z_1 \mathcal{R} z_2 \Leftrightarrow |z_1| = |z_2|$$

Demuestre que $\mathcal{R}$ es relación de equivalencia y determine y grafique la clase de equivalencia del complejo $z_0 = 2 + i\sqrt{5}$

P3. (20 min.) Pruebe que $\forall n \in \mathbb{N}$ y $\rho \in \mathbb{R}$, el complejo

$$z = (1 + \rho e^{i\pi/2})^n + (1 - \rho e^{i\pi/2})^n \in \mathbb{R}$$

P4. (15 min.) Sea $z \in \mathbb{C}$, entonces pruebe que

$$|z + i| = |z - i| \Leftrightarrow z \in \mathbb{R}$$

P5. (15 min.) Muestre que el conjunto de todos los $z \in \mathbb{C}$ tales que

$$\left|\frac{z-2}{z+1}\right| = 2$$

es una circunferencia en el plano complejo. Determine su centro y su radio.

P6. (15 min.) Expresar de la forma $a + bi$ los siguientes complejos

$$(1-i)^4(1+i)^4, \quad \text{y} \quad 1 + i + \frac{i-1}{|1-i|^2 + i}$$

P7. Considere los números reales $S = \sum_{k=0}^{n} \binom{n}{k} \cos(k \cdot \alpha)$ y $S' = \sum_{k=0}^{n} \binom{n}{k} \sin(k \cdot \alpha)$, donde $\alpha \in \mathbb{R}$.

(a) (30 min.) Probar la igualdad de números complejos

$$S + iS' = (1 + \cos(\alpha) + i \sin(\alpha))^n$$

(b) (30 min.) Escriba el número complejo $1 + \cos(\alpha) + i \sin(\alpha)$ en forma polar y deduzca que

$$S = 2^n(\cos(\alpha/2))^n \cdot \cos(n \cdot \alpha/2) \text{ y } S' = 2^n(\cos(\alpha/2))^n \cdot \sin(n \cdot \alpha/2)$$

(recuerde que: $\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha)$ y $\cos(2\alpha) = cos^2(\alpha) - \sin^2(\alpha)$)

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

12.4. Raíces de la unidad

Definición 12.3 (Raíz n-ésima de la unidad). *Sean $z \in \mathbb{C}$ y $n \geq 2$. Diremos que z es una* **raíz n-ésima de la unidad** *si*

$$z^n = 1$$

Si escribimos en forma polar $z = re^{i\theta}$, entonces (gracias a la fórmula de Moivre)

$$z^n = r^n e^{in\theta}$$

Entonces, para que z sea raíz n-ésima de la unidad, debe cumplirse

$$r^n = 1 \quad \wedge \quad (\exists k \in \mathbb{Z})\ n\theta = 2k\pi$$

Como $r \geq 0$ es un número real, debe tenerse que $r = 1$. La condición sobre θ es:

$$(\exists k \in \mathbb{Z})\ \theta = \frac{2k\pi}{n}$$

Obtenemos que todos los complejos de la forma $z = e^{i\frac{2k\pi}{n}}$ son raíces n-ésimas de la unidad. ¿Cuántos números complejos cumplen esto? Elijamos $r \in \{0, \ldots, n-1\}$ tal que $k \equiv_n r$, es decir que $k = r + nl$ con $l \in \mathbb{Z}$. Entonces

$$e^{i\frac{2k\pi}{n}} = e^{i(\frac{2r\pi}{n} + 2l\pi)} = e^{i\frac{2r\pi}{n}} e^{i\ 2l\pi} = e^{i\frac{2r\pi}{n}} \cdot 1 = e^{i\frac{2r\pi}{n}}$$

Así, todos los posibles valores de θ dados anteriormente definen sólo n números complejos distintos: éstos son

$$e^{i\frac{2r\pi}{n}} \qquad (r = 0, \ldots, n-1)$$

Estos valores son las exactamente n raíces n-ésimas de la unidad.

12.5. Raíces de un complejo cualquiera

Definición 12.4 (Raíces de un complejo cualquiera). *Sean $w \in \mathbb{C} \setminus \{0\}$ y $n \geq 2$. Diremos que z es una raíz n-ésima de w si*

$$z^n = w$$

Escribiendo las formas polares $z = re^{i\theta}$ y $w = Re^{i\phi}$, entonces debe cumplirse

$$r^n e^{in\theta} = Re^{i\phi}$$

Como $r \geq 0$ es real, esta vez obtenemos que $r = \sqrt[n]{R}$, y la condición se reduce a

$$e^{in\theta} = e^{i\phi}$$

lo que equivale a

$$\left(e^{i(\theta - \frac{\phi}{n})}\right)^n = 1$$

es decir, $v = e^{i(\theta - \frac{\phi}{n})}$ debe ser una raíz n-ésima de la unidad. Así, existe $r \in \{0, \ldots, n-1\}$ tal que

$$\theta - \frac{\phi}{n} = \frac{2r\pi}{n}$$

Nuestra condición para θ es, finalmente,

$$(\exists r \in \{0, \ldots, n-1\})\ \theta = \frac{\phi + 2r\pi}{n}$$

Concluimos que w tiene también exactamente n raíces n-ésimas, las cuales son

$$\sqrt[n]{R}\ e^{i\frac{\phi+2r\pi}{n}} \qquad (r = 0, \ldots, n-1)$$

Gracias a este análisis, sabemos ahora que la ecuación $z^2 = -1$ posee exactamente dos soluciones en $\mathbb{C}$: las dos raíces cuadradas de -1.
La forma polar de -1 es $e^{i\pi}$, por lo que las mencionadas raíces son

$$e^{i\frac{\pi}{2}} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$$

y

$$e^{i\frac{\pi+2\pi}{2}} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i$$

Propiedad 25. *Sea $n \geq 2$. La suma de las n raíces n-ésimas de la unidad vale cero.*

Demostración. Las raíces n-ésimas de la unidad son

$$e^{i\frac{2r\pi}{n}} \qquad (r = 0, \ldots, n-1)$$

Su suma es, entonces,

$$S = \sum_{r=0}^{n-1} e^{i\frac{2r\pi}{n}}$$

Observamos que $e^{i\frac{2r\pi}{n}} = \left(e^{i\frac{2\pi}{n}}\right)^r$, por lo que

$$S = \sum_{r=0}^{n-1} \left(e^{i\frac{2\pi}{n}}\right)^r$$

Como $n \geq 2$, tenemos que $e^{i\frac{2\pi}{n}} \neq 1$, y así

$$S = \frac{\left(e^{i\frac{2\pi}{n}}\right)^0 - \left(e^{i\frac{2\pi}{n}}\right)^n}{1 - e^{i\frac{2\pi}{n}}} = \frac{1-1}{1-e^{i\frac{2\pi}{n}}} = 0$$

13. Polinomios

13.1. Definición

Definición 13.1 (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*

$$\begin{aligned} p : \mathbb{K} &\to \mathbb{K} \\ x &\to p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \\ &\qquad = \sum_{k=0}^{n} a_k x^k \end{aligned}$$

donde $a_0, a_1, a_2, \ldots, a_n$ *son constantes en* $\mathbb{K}$*. Se llaman* **coeficientes** *del polinomio* p*.*

Al conjunto de todos los polinomios con coeficientes en $\mathbb{K}$ se le denota $\mathbb{K}[x]$.

13.2. Igualdad de polinomios

Proposición 13.1. *Sean* p, q *dos polinomios en* $\mathbb{K}[x]$*. Se tiene que*

$$p \text{ y } q \text{ son iguales} \iff \text{Sus coeficientes son iguales}$$

Demostración. Por doble implicancia.
$\Leftarrow$) Ésta es directa, y queda de ejercicio para el lector.
$\Rightarrow$) Supongamos que

$$\begin{aligned} p(x) &= a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \\ q(x) &= b_0 + b_1 x + b_2 x^2 + \ldots + b_m x^m \end{aligned}$$

Notemos que podemos suponer que $m = n$. En efecto, si $m < n$, entonces podemos escribir $q(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$ tomando $b_{m+1} = 0, b_{m+2} = 0, \ldots, b_n = 0$. Se procede de modo similar si $m > n$.
Debemos demostrar, entonces, que $(\forall k = 0, \ldots, n)\ a_k = b_k$. Lo haremos siguiendo un argumento de tipo inductivo (similar a la segunda forma del principio de inducción):
Caso base $k = 0$: Sabemos que los polinomios p y q son iguales (como funciones), por lo que $p(0) = q(0)$. Pero $p(0) = a_0$ y $q(0) = b_0$, con lo que concluimos que $a_0 = b_0$.
Paso inductivo: Sea $k \in \{1, \ldots, n\}$, y supongamos que $a_0 = b_0, a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$. Debemos demostrar que $a_k = b_k$.
Como p y q son iguales, entonces para cualquier $x \in \mathbb{K}$:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n$$

Usando la hipótesis inductiva, podemos cancelar los primeros k términos a cada lado, y obtener

$$a_k x^k + \ldots + a_n x^n = b_k x^k + \ldots + b_n x^n$$

Podemos a ambos lados factorizar x^k:

$$x^k (a_k + \ldots + a_n x^{n-k}) = x^k (b_k + \ldots + b_n x^{n-k})$$

Así, para todo $x \in \mathbb{K} \setminus \{0\}$ tenemos

$$a_k + \ldots + a_n x^{n-k} = b_k + \ldots + b_n x^{n-k}$$

pues podemos dividir por x^k.
Recordando que $\mathbb{K}$ es $\mathbb{R}$ ó $\mathbb{C}$, podemos tomar el límite $x \to 0$ a ambos lados de la última igualdad, y así $a_k = b_k$.
Por lo tanto, los coeficientes de ambos polinomios son iguales.

13.3. Grado de un polinomio

Definición 13.2 (Grado de un polinomio). *Sea $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ un polinomio. Diremos que es de* **grado** *n si $a_n \neq 0$, 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 a_k es no nulo.

Respecto de $-\infty$, se usa las siguientes convenciones: para cualquier $n \in \mathbb{N}$

$$n + (-\infty) = -\infty \quad \wedge \quad n > -\infty$$

y además

$$(-\infty) + (-\infty) = -\infty$$

Ejemplos:

- $\text{gr}(1 + 5x + 18x^4) = 4$
- $\text{gr}(x + 3) = 1$
- $\text{gr}(37) = 0$
- $\text{gr}(0) = -\infty$

Observación: Los polinomios de grado 0 son exactamente los polinomios constantes (que no dependen de x) $p(x) = a_0$ con $a_0 \neq 0$.

Sea $p \in \mathbb{K}[x]$ un polinomio. Diremos que p es **mónico** si

$$a_n = 1 \quad \text{donde } n = \text{gr}(p)$$

es decir, si el coeficiente asociado a la potencia de x más grande vale 1.

Ejemplos:

Son polinomios mónicos:

- $25 + 32x + x^3$
- $5 + x^2$
- $x^5 + 5x^2 - 25$

13.4. Operaciones entre polinomios

Sean $p, q \in \mathbb{K}[x]$ dos polinomios:

$$p(x) = \sum_{k=0}^{n} a_k x^k, \qquad q(x) = \sum_{k=0}^{n} b_k x^k$$

(recordar que eventualmente hay que "rellenar" con ceros para que ambos polinomios tengan la misma cantidad de coeficientes)
Definimos la suma y multiplicación de polinomios del modo siguiente:

Definición 13.3 (Suma y multiplicación de polinomios).

- *El polinomio suma se define como el polinomio formado por la suma de los coeficientes de p y q.*

$$(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$$

- *El polinomio producto tiene una definición en apariencia más complicada.*

$$(p \cdot q)(x) = \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Sin embargo, ésta corresponde a la forma intuitiva de multiplicar distribuyendo:

$$\begin{aligned} (1 - x + 3x^2) \cdot (x^2 - x^4) &= 1(x^2 - x^4) - x(x^2 - x^4) + 3x^2(x^2 - x^4) \\ &= x^2 - x^4 - x^3 + x^5 + 3x^4 - 3x^6 \\ &= x^2 - x^3 + 2x^4 + x^5 - 3x^6 \end{aligned}$$

Estas operaciones cumplen:

$$\begin{aligned} \operatorname{gr}(p+q) &\leq \operatorname{máx}\{\operatorname{gr}(p), \operatorname{gr}(q)\} \\ \operatorname{gr}(p \cdot q) &= \operatorname{gr}(p) + \operatorname{gr}(q) \end{aligned}$$

Es importante recalcar que en el caso de la suma sólo tenemos una desigualdad, y no una igualdad. Un posible ejemplo es considerar $p(x) = 1 + 5x + 7x^2$ y $q(x) = 2 + 8x - 7x^2$. Se tiene que $\operatorname{gr}(p) = \operatorname{gr}(q) = 2$, pero $\operatorname{gr}(p+q) = \operatorname{gr}(3 + 13x) = 1$.

Observemos que la fórmula para calcular el grado de un producto también es válida cuando alguno de los polinomios es el polinomio nulo: en efecto, si $p(x) = 0$, entonces $(p \cdot q)(x) = 0$, por lo que

$$\operatorname{gr}(0) = \operatorname{gr}(p \cdot q) = \operatorname{gr}(p) + \operatorname{gr}(q) = (-\infty) + \operatorname{gr}(q)$$

y ambos lados valen $-\infty$.

13.5. Estructura de $\mathbb{K}[x]$

Propiedad 26. $(\mathbb{K}[x], +, \cdot)$ *es un anillo conmutativo con unidad, que no posee divisores de cero.*

Demostración. Esta demostración queda como ejercicio para el lector, aquí revisaremos sólo algunas partes.
La unidad de $(\mathbb{K}[x], +, \cdot)$ es el polinomio constante $p(x) = 1$. Observemos que los coeficientes de este polinomio son

$$a_k = \begin{cases} 1 & k = 0 \\ 0 & k \neq 0 \end{cases}$$

Así, si $q = b_0 + b_1 x + \ldots + b_n x^n \in \mathbb{K}[x]$ es de grado n

$$\begin{aligned} (p \cdot q)(x) &= \sum_{k=0}^{2n} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k \\ &= \sum_{k=0}^{2n} \left(a_0 b_k + \sum_{i=1}^{k} a_i b_{k-i} \right) x^k \\ &= \sum_{k=0}^{2n} \left(1 \cdot b_k + \sum_{i=1}^{k} 0 \cdot b_{k-i} \right) x^k \\ &= \sum_{k=0}^{2n} b_k x^k \end{aligned}$$

Como q es de grado n, entonces $b_k = 0$ para $k = n+1, \ldots, 2n$. Entonces

$$\begin{aligned} (p \cdot q)(x) &= \sum_{k=0}^{n} b_k x^k \\ &= q(x) \end{aligned}$$

$(\mathbb{K}[x], +, \cdot)$ no posee divisores de cero. En efecto, si $p, q \in \mathbb{K}[x]$ son tales que $p \cdot q = 0$, entonces obtenemos que

$$\mathrm{gr}(p) + \mathrm{gr}(q) = -\infty$$

Dadas las reglas de suma que definimos, al menos uno de los dos grados debe valer $-\infty$, es decir al menos uno de los dos polinomios debe ser igual a cero.

¿Es $(\mathbb{K}[x], +, \cdot)$ cuerpo?

Veremos que $(\mathbb{K}[x], +, \cdot)$ es un ejemplo de un anillo conmutativo con unidad sin divisores de cero, que sin embargo **no es cuerpo**.

(¿Qué anillos conmutativos con unidad sin divisores de cero sí son cuerpos?)

Proposición 13.2. *En $(\mathbb{K}[x], +, \cdot)$, los únicos polinomios que poseen inverso son las constantes no nulas, es decir los polinomios de grado 0.*

Demostración. Sea $p \in \mathbb{K}[x]$ de grado 0. Entonces $p(x) = a_0$ con $a_0 \neq 0$. Es fácil ver que p posee inverso, el cual es $q(x) = \frac{1}{a_0}$.
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

$$\mathrm{gr}(p) + \mathrm{gr}(q) = 0$$

Como el grado de un polinomio es siempre positivo (con la excepción de que valga $-\infty$), debe tenerse en particular que $\mathrm{gr}(p) = 0$.

Guía Básica

Determinar la veracidad de las siguientes afirmaciones:

1. ☐ $\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}$.

2. ☐ $|\overline{z_1 + z_2}| \geq |\bar{z_1}| + |\bar{z_2}|$.

3. ☐ $|\overline{z_1 + z_2}| \leq |\bar{z_1}| + |\bar{z_2}|$.

4. ☐ $\bar{z} + z = 2i \cdot \mathbb{I}\text{m}(z)$.

5. ☐ $\bar{z} + z = 2\mathbb{R}\text{e}(z)$.

6. ☐ $\bar{z} + z = -2\mathbb{R}\text{e}(z)$.

7. ☐ $\bar{z} + z = -2\mathbb{I}\text{m}(z)$.

8. ☐ $\bar{z} - z = -2\mathbb{R}\text{e}(z)$.

9. ☐ $\bar{z} - z = -2i \cdot \mathbb{I}\text{m}(z)$.

10. ☐ $\bar{z} - z = -2\mathbb{I}\text{m}(z)$.

11. ☐ $\bar{z} - z = 2\mathbb{R}\text{e}(z)$.

12. ☐ $\overline{z_1 z_2} = \bar{z_1}\bar{z_2}$.

13. ☐ $|\overline{z_1 z_2}| = |z_1 \overline{z_2}|$.

14. ☐ $|\overline{z_1 z_2}| > |\bar{z_1}||\bar{z_2}|$.

15. ☐ $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$.

16. ☐ $|z|^2 > z\bar{z}$.

17. ☐ $|z| = z\bar{z}$.

18. ☐ $|z|^2 = z\bar{z}$.

19. ☐ $z \neq 0 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2}$.

20. ☐ $i^{-1} = i$.

21. ☐ $i^{-1} = -i$.

22. ☐ Dados $z \in \mathbb{C}, n \geq 2$ tales que $z^n = 1$, decimos que 1 es raíz n-ésima de z.

23. ☐ Dados $z \in \mathbb{C}, n \geq 2$ tales que $z^n = 1$, decimos que z es raíz n-ésima de la unidad.

24. ☐ Existen infinitas raíces n-ésimas de la unidad distintas en $\mathbb{C}$.

25. ☐ Hay exactamente $n + 1$ raíces n-ésimas de la unidad en $\mathbb{C}$.

26. ☐ Hay exactamente n raíces n-ésimas de la unidad en $\mathbb{C}$.

27. ☐ El complejo $\sqrt{5}e^{i\frac{6\pi}{5}}$ es raíz quinta de la unidad.

28. ☐ El complejo $e^{i\frac{6\pi}{5}}$ es raíz quinta de la unidad.

29. ☐ El complejo $e^{i\frac{6\pi}{5}}$ es raíz sexta de la unidad.

30. ☐ Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son de la forma $e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in \{0, \ldots, n-1\}$.

31. ☐ Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son de la forma $\sqrt[n]{\rho}e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in \{0, \ldots, n-1\}$.

32. ☐ Las raíces n-ésimas de un complejo $\rho e^{i\varphi} \neq 0$ son de la forma $\rho e^{i\frac{\varphi+2r\pi}{n}}$, para $r \in \{0, \ldots, n-1\}$.

33. ☐ Hay exactamente 2 raíces n-ésimas de un complejo cualquiera $w \neq 0$.

34. ☐ Hay exactamente $n+1$ raíces n-ésimas de un complejo cualquiera $w \neq 0$.

35. ☐ Hay exactamente n raíces n-ésimas de un complejo cualquiera $w \neq 0$.

36. ☐ Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale i.

37. ☐ Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale cero.

38. ☐ Dado $n \geq 2$, la suma de las n raíces n-ésimas de la unidad vale 1.

Guía de Ejercicios

1. Calcule las raíces de $z^2 = -i$ y expréselas de la forma $a + bi$.

2. Exprese en forma $a + bi$ las raíces cuartas de $z_0 = \frac{1+i\sqrt{3}}{1-i\sqrt{3}}$

3. 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) $z^7 = 5e^{i\frac{\pi}{8}}$

4. 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 $q(x) = 2(x^4-1)-(x^3-x)+3(x^2-x)+4x+3$

5. Determine un caso en el que, dados dos polinomios $p, q \in \mathbb{K}[x]$, se tenga que $\mathrm{gr}(p+q) < \mathrm{máx}\{\mathrm{gr}(p), \mathrm{gr}(q)\}$. ¿Por qué nunca sucede que $\mathrm{gr}(p\cdot q) < \mathrm{gr}(p)+\mathrm{gr}(q)$.

6. 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

P1. (20 min.) Sean $1, w_1, w_2, w_3$ y w_4 las raices quintas de la unidad. Demuestre que

$$(1-w_1)(1-w_2)(1-w_3)(1-w_4) = 5$$

P2. (20 min.) Demostrar utilizanto las propiedades de las raíces de la unidad que $\forall n \geq 2$

$$\cos\frac{2\pi}{n} + \cos\frac{4\pi}{n} + \cos\frac{6\pi}{n} + ... + \cos\frac{2(n-1)\pi}{n} = -1$$

$$y \qquad \operatorname{sen}\frac{2\pi}{n} + \operatorname{sen}\frac{4\pi}{n} + \operatorname{sen}\frac{6\pi}{n} + ... + \operatorname{sen}\frac{2(n-1)\pi}{n} = 0$$

P3. Se define el grupo abeliano $S \subseteq \mathbb{C}$ por $S = \{z \in \mathbb{C} / |z| = 1\}$.

(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 $U = \{z \in \mathbb{C} \mid \text{para algún } n \in \mathbb{N},\ n \geq 2,\ z \text{ es raíz } n\text{-ésima de la unidad}\}$. Mostrar que $(U, \cdot)$ es subgrupo del grupo $(S, \cdot)$.

P4. (30 min.) Dado un polinomio $p(x) = \sum_{k=0}^{n} a_k x^k$ se define:

$$L(p)(x) = \sum_{k=1}^{n} k a_k x^{k-1}$$

(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 $L(p)(x) = n \cdot (x-d)^{n-1}$.

P5. Sea $J_2 = \{p(x) \in \mathbb{R}[x] \mid \operatorname{gr}(p) \leq 2,\ a_0 = 0,\ a_1 \neq 0\}$. En J_2 se define la l.c.i. $\triangle$ a través de $p(x) \triangle q(x) = \sum_{i=1}^{2} c_i x^i$ 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 $f(a_1 \cdot x + a_2 \cdot x^2) = a_1$. Probar que f es un morfismo sobreyectivo de $(J_2, \triangle)$ en $(\mathbb{R} \setminus \{0\}, \cdot)$.

(c) (20 min.) Sea $H = \{p(x) \in J_2 \mid a_2 = 1\}$. Probar que $(H, \triangle)$ es subgrupo abeliano de $(J_2, \triangle)$.

Importante: Visita regularmente
`http://www.dim.uchile.cl/~docencia/algebra`
para mantenerte al tanto de las novedades del curso.

SEMANA 14: POLINOMIOS

Usa este margen para consultar más rápido el material. Haz también tus propias anotaciones.
▼

14. Teorema de la división

Al ser $(\mathbb{K}[x], +, \cdot)$ un anillo, ocurre un fenómeno similar al de $\mathbb{Z}$: Las divisiones deben considerar un posible resto.

Teorema 14.1 (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*

1. $p = q \cdot d + r$
2. $gr(r) < gr(d)$

Notación:

- La ecuación (1), se llama **división con resto de p por d.**
- El polinomio q se llama **cuociente**.
- El polinomio r se llama **resto**.
- Cuando $r(x) = 0$, 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 este teorema, usaremos un método de división similar al que conocemos en $\mathbb{Z}$. Lo ejemplificaremos a partir de un ejemplo.

Ejemplo:

Calculemos la división entre $p(x) = 3x^3 + 2x - 2$ y $q(x) = x - 4$.

$$3x^3{+}2x{-}2 : x{-}4 =$$

Para obtener el cuociente, debemos preguntarnos por qué multiplicar el término de mayor exponente de $x - 4$ para obtener el de $3x^3 + 2x - 2$: es decir, por qué multiplicar x para obtener $3x^3$. La respuesta es $3x^2$.

Entonces

$$\begin{array}{l} 3x^3 \quad +2x \quad -2 \ : \ x \ -4 = 3x^2 \\ -(3x^3{-}12x^2) \\ \qquad 12x^2 \ +2x \quad -2 \end{array}$$

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.

$$\begin{array}{l} 3x^3 \quad +2x \quad -2 \quad : \; x-4 = 3x^2+12x \\ -(3x^3-12x^2) \\ \qquad 12x^2 \quad +2x \; -2 \\ \qquad -(12x^2-48x) \\ \qquad\qquad 50x \; -2 \end{array}$$

En cada etapa vamos calculando un nuevo resto parcial, y detenemos el proceso cuando este resto tiene grado menor que el de $x-4$:

$$\begin{array}{l} 3x^3 \quad +2x \quad -2 \quad : \quad x-4 = 3x^2+12x+50 \\ -(3x^3-12x^2) \\ \qquad 12x^2 \quad +2x \quad -2 \\ \qquad -(12x^2-48x) \\ \qquad\qquad 50x \quad -2 \\ \qquad\qquad -(50x-200) \\ \qquad\qquad\qquad 198 \end{array}$$

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

$$3x^3 + 2x - 2 = (x-4)(3x^2 + 12x + 50) + 198.$$

Demostración. (Teorema de la División) Primero probaremos la **existencia** de q y r.
Veamos dos casos posibles:

- Si $\text{gr}(d) > \text{gr}(p)$. Basta notar que

  $$p = 0 \cdot d \; + \; p.$$

  De donde $q = 0$ y $r = p$, satisfacen las condiciones del Teorema.

- Si $\text{gr}(d) \leq \text{gr}(p)$. Ocupamos el procedimiento de división ejemplificado anteriormente, obteniendo:

  $$\begin{aligned} p &= q_1 \cdot d + r_1 \\ r_1 &= q_2 \cdot d + r_2 \\ r_2 &= q_3 \cdot d + r_3 \\ &\vdots \\ r_n &= q_{n+1} \cdot d + r_{n+1}, \quad \text{con } \text{gr}(r_{n+1}) < \text{gr}(d). \end{aligned}$$

  ¿Por qué $\text{gr}(r_{n+1}) < \text{gr}(d)$? Porque el grado de los restos r_i disminuye en al menos 1 en cada etapa y $\text{gr}(d) \geq 0$ (pues $d \neq 0$).

Reemplazamos ahora en la primera ecuación, las posteriores:

$$\begin{aligned} p &= q_1 \cdot d + r_1 \\ &= (q_1 + q_2) \cdot d + r_2 \\ &= (q_1 + q_2 + q_3) \cdot d + r_3 \\ &\vdots \\ &= (q_1 + q_2 + \cdots + q_{n+1}) \cdot d + r_{n+1}, \quad \text{con } \text{gr}(r_{n+1}) < \text{gr}(d). \end{aligned}$$

Basta entonces definir $q = q_1 + q_2 + \cdots + q_{n+1}$, y $r = r_{n+1}$. Estos polinomios satisfacen el Teorema de la División.
Como ejercicio para el lector, queda formalizar esta demostración como una inducción en el grado de p.

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

$$\text{gr}(d) > \text{gr}((q_1 - q_2) \cdot d) = \text{gr}(q_1 - q_2) + \text{gr}(d),$$

lo cual sólo puede ocurrir si $\text{gr}(q_1 - q_2) = -\infty$, o sea, si

$$q_1 - q_2 = 0 \;\Leftrightarrow\; q_1 = q_2.$$

Como consecuencia, $r_2 - r_1 = 0 \cdot d = 0$ y luego $r_1 = r_2$.

14.1. Raíces y factorización

Teorema 14.2 (Teorema del Resto). *Sean $p \in \mathbb{K}[x]$ y $c \in K$. El resto de dividir p por el polinomio $(x - c)$ es exactamente $p(c)$.*

Demostración. Por el teorema anterior, 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 $r_0 \in K$ 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 14.1 (Raíz). *Diremos que $c \in K$ es una* **raíz** *del polinomio $p \in \mathbb{K}[x]$ si*

$$p(c) = 0.$$

Propiedad 27.

$$c \in \mathbb{K} \text{ es raíz de } p \;\Leftrightarrow\; (x - c) \mid p(x)$$

Demostración. $\Rightarrow$) 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, $p(c) = 0$, 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

$$p(x) = q(x)(x-c)$$

Entonces $p(c) = q(c) \cdot 0 = 0$.

Se tienen las siguientes propiedades:

Propiedades 20. *1. Si $c_1, c_2, \ldots, c_k$ son raíces distintas de p, entonces*

$$(x-c_1)(x-c_2)\ldots(x-c_k) \mid p(x)$$

2. Sea $n \geq 1$. Si $p \in \mathbb{K}[x]$ es tal que $gr(p) = n$, entonces p posee a lo más n raíces distintas.

3. Sean $n \geq 1$, 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).

Demostración. Demostraremos (1) y (2). (3) se obtiene como consecuencia de (2), aplicándola al polinomio $(p-q)$.
Para (1): Por inducción en k.
El caso $k = 1$ está demostrado en el teorema anterior.
Sean $c_1, c_2, \ldots, c_k$ raíces distintas de p. Usando hipótesis inductiva, sabemos que

$$(x-c_1)(x-c_2)\ldots(x-c_{k-1}) \mid p(x)$$

o, equivalentemente, existe $q \in \mathbb{K}[x]$ tal que

$$p(x) = q(x)(x-c_1)(x-c_2)\ldots(x-c_{k-1})$$

Como c_k también es raíz de p,

$$0 = p(c_k) = q(c_k)(c_k-c_1)(c_k-c_2)\ldots(c_k-c_{k-1})$$

Gracias a que los valores c_i son todos distintos, tenemos necesariamente que $q(c_k) = 0$, con lo que 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

$$p(x) = q'(x)(x-c_1)(x-c_2)\ldots(x-c_k)$$

Es decir,

$$(x-c_1)(x-c_2)\ldots(x-c_k) \mid p(x)$$

Para (2): 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

$$p(x) = q(x)(x-c_1)\ldots(x-c_k)$$

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 $i = 1, \ldots, k$.
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 $\mathrm{gr}(q) \geq 0$. Entonces

$$k = n - \mathrm{gr}(q) \leq n - 0 = n$$

es decir, p posee a lo más n raíces distintas.

14.2. Teorema Fundamental del Álgebra

En la sección anterior demostramos 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 14.3 (Teorema Fundamental del Álgebra). *Sea p un polinomio con coeficientes en $\mathbb{C}[x]$, tal que $gr(p) = n \geq 1$. Entonces p posee al menos una raíz en $\mathbb{C}$.*

No demostraremos este teorema, ya que para eso requerimos herramientas más avanzadas. Sin embargo, estudiaremos la siguiente aplicación.

14.3. Factorización en $\mathbb{C}$

Proposición 14.1. *Sea p un polinomio con coeficientes en $\mathbb{C}[x]$, 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*

$$p(x) = \alpha(x - c_1)^{l_1} \ldots (x - c_m)^{l_m}$$

Demostración. Como $\mathrm{gr}(p) \geq 1$, utilizamos el Teorema Fundamental del Álgebra para encontrar $r_1 \in \mathbb{C}$ que es raíz de p. Entonces podemos escribir

$$p(x) = q_1(x)(x - r_1)$$

para algún $q_1 \in \mathbb{C}[x]$.
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 Teorema Fundamental, esta vez a q_1. Así, existe una raíz $r_2 \in \mathbb{C}$ de q_1, y podemos escribir

$$p(x) = q_2(x)(x - r_1)(x - r_2)$$

para algún $q_2 \in \mathbb{C}[x]$.
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 $c_1 \in \mathbb{C}$ aparece l_1 veces.

El valor $c_2 \in \mathbb{C}$ aparece l_2 veces.

...

El valor $c_m \in \mathbb{C}$ aparece l_m veces.

Así

$$p(x) = \alpha(x - c_1)^{l_1} \dots (x - c_m)^{l_m}$$

Notar que si existe una demostración del tipo mencionado, entonces

$$\mathrm{gr}(p) = l_1 + \ldots + l_m$$

Queda como ejercicio para el lector demostrar que el complejo α que aparece en la descomposición de p es exactamente su coeficiente a_n.

14.4. Acerca de las raíces complejas

Proposición 14.2. *Sea $p \in \mathbb{R}[x]$, y sea $z \in \mathbb{C}$ una raíz de p. Entonces, el conjugado $\bar{z}$ también es raíz de p.*

Demostración. Escribamos

$$p(x) = \sum_{k=0}^{n} a_k x^k$$

donde $a_k \in \mathbb{R}$ para $k = 0, \dots, n$.
Se tiene que

$$p(\bar{z}) = \sum_{k=0}^{n} a_k (\bar{z})^k$$

Observemos que, como $a_k \in \mathbb{R}$, entonces $a_k = \overline{a_k}$, y así

$$a_k(\bar{z})^k = \overline{a_k z^k} \qquad (k = 0, \dots, n)$$

Reemplazando esta expresión, obtenemos

$$p(\bar{z}) = \sum_{k=0}^{n} \overline{a_k z^k} = \overline{\sum_{k=0}^{n} a_k z^k} = \overline{p(z)}$$

Como z es raíz de p, entonces $p(z) = 0$, y así $p(\bar{z}) = \bar{0} = 0$, con lo que $\bar{z}$ también es raíz de p.

14.5. Factorización en $\mathbb{R}$

Proposición 14.3. *Sea p un polinomio con coeficientes en $\mathbb{R}[x]$, tal que $gr(p) = n \geq 1$. Entonces existen valores $\alpha, c_1, \dots, c_m, a_1, b_1, a_2, b_2 \dots a_s, b_s \in \mathbb{R}$ tales que*

$$p(x) = \alpha(x-c_1)(x-c_2)\dots(x-c_m)(x^2+a_1x+b_1)(x^2+a_2x+b_2)\dots(x^2+a_sx+b_s).$$

En donde $c_1, \dots, c_m$ son las raíces reales de p y $x^2 + a_1x + b_1,\ \dots,\ x^2 + a_sx + b_s$ son polinomios sin raíces reales (con posible repetición). α es el coeficiente a_n de p.

DEMOSTRACIÓN. La demostración se basa en la descomposición anterior, salvo que consideramos primero todas las raíces reales de p (posiblemente repetidas), obteniendo:

$$p(x) = (x - c_1)(x - c_2)\dots(x - c_m)q(x).$$

Luego por cada raíz compleja $z \in \mathbb{C} \setminus \mathbb{R}$ de p, por la proposición anterior (ya que $p \in \mathbb{R}[x]$) sabemos que $\overline{z}$ es también raíz de p. Así, $(x - z)(x - \overline{z})$ divide a p. Pero esto no nos sirve para factorizar a p en $\mathbb{R}[x]$.
Sin embargo:

$$\begin{aligned}(x - z)(x - \overline{z}) &= x^2 - (z + \overline{z})x + z\overline{z} \\ &= x^2 - 2\mathbb{R}\mathrm{e}(z) \cdot x + |z|^2 \ \in \mathbb{R}[x].\end{aligned}$$

Definimos entonces $a_i = -2\mathbb{R}\mathrm{e}(z)$ y $b_i = |z|^2$, en cada paso (con posible repetición). Obtenemos así la descomposición.
Queda como ejercicio para el lector el formalizar esta demostración.

14.6. Algunos resultados útiles

Polinomios a coeficientes enteros

Proposición 14.4. *Sea $p \in \mathbb{R}[x]$, con coeficientes $a_0, \dots, a_n \in \mathbb{Z}$. Si $\frac{r}{s} \in \mathbb{Q}$ (se asume que r y s son primos relativos) es una raíz de p, entonces:*

$$r|a_0 \quad \wedge \quad s|a_n.$$

DEMOSTRACIÓN. Como $\frac{r}{s}$ es raíz de p, luego

$$\begin{aligned}& p\left(\frac{r}{s}\right) = a_n\left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \dots + a_1\left(\frac{r}{s}\right) + a_0 = 0 \\ \Leftrightarrow\ & r\left(a_n r^{n-1} + a_{n-1} s r^{n-2} + \dots + s^{n-1} a_1\right) = -a_0 s^n.\end{aligned}$$

De aquí, r divide a $-a_0 s^n$. Sin embargo, como r y s son primos relativos, r y s^n también lo son. Luego necesariamente

$$r|a_0.$$

Queda propuesto como ejercicio probar que $s|a_n$.

El siguiente corolario es útil para explorar cuáles son las raíces enteras de un polinomio mónico con coeficientes enteros.

Corolario 14.1. *Sea $p \in \mathbb{R}[x]$ mónico, con coeficientes $a_0, \dots, a_{n-1} \in \mathbb{Z}$. Entonces toda raíz racional de p es entera y divide a a_0.*

Ejemplo:

Consideremos el polinomo (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 $a_0 = 4$.

Luego, si $x \in \mathbb{Q}$ es raíz de p, entonces $x \in \{\pm 1, \pm 2, \pm 4\}$.

Podríamos evaluar p en $x = 1534$ para ver si es raíz. ¿Pero para qué?
Lo anterior nos dice que eso sería tiempo perdido.

Regla de Ruffini y Algoritmo de Horner

A continuación veremos un método para dividir un polinomio p por $(x-c)$, de manera rápida.

1. **Regla de Ruffini**

   Sea $p(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[x]$ y $c \in \mathbb{R}$.

   Para dividir p por $(x-c)$, construimos la siguiente tabla para calcular los números b_i, con $i \in \{0, \dots n-1\}$:

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c					
	$b_{n-1} = a_n$				

   En el paso $i \leq 1$, multiplicamos b_{i+1} por c y sumamos el resultado a a_{i+1}. O sea $b_i = a_{i+1} + b_{i+1}c$.

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c		$b_{n-1}c$	$\cdots$	$b_1 c$	$b_0 c$
	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + b_{n-1}c$	$\cdots$	$b_0 = a_1 + b_1 c$	$r = a_0 + b_0 c$

   Luego, el *cuociente* de dividir p por $(x-c)$ es:

   $$q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0.$$

   Además, el último término calculado en la tabla es el *resto* de dividir p por $(x-c)$:

   $$r(x) = r = a_0 + b_0 c.$$

   O sea,

   $$p(x) = q(x)(x-c) + r(x).$$

   Queda propuesto para el lector probar que el método recién presentado funciona.

2. **Algoritmo de Horner**

   Notemos que gracias al Teorema del Resto, el resto r entregado por la Regla de Ruffini, **es la evaluación de p en c.**

   Así, la Regla de Ruffini puede ser usada para estudiar las raíces reales de un polinomio en $\mathbb{R}[x]$. Este uso es denominado **Algoritmo de Horner**.

   Ejemplo:

   Consideremos el polinomio anterior: $p(x) = x^3 + 6x^2 - 3x - 4$ (aunque la Regla de Ruffini no requiere que sea mónico).

   Dividamos p por $(x-1)$:

	1	6	-3	-4
1		1	7	4
	1	7	4	0

   Es decir $p(x) = (x^2 + 7x + 4)(x-1) + 0$ y luego $x = 1$ es raíz de p.

Sin embargo, al dividir por $(x-2)$:

	1	6	-3	-4
2		2	16	26
	1	8	13	22

Luego $p(x) = (x^2 + 8x + 13)(x-2) + 22$ y por lo tanto $p(2) = 22$ ($x = 2$ no 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. ☐ 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 a_k de p es no nulo.

5. ☐ El grado de un polinomio p, es el k más peque no tal que el coeficiente a_k de p es nulo.

6. ☐ Si dos polinomios tienen grados distintos puede 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 $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$, entonces $(p+q)(x) = \sum_{k=0}^{n} a_k b_k x^k$.

15. ☐ Si $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$, entonces $(p+q)(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$.

16. ☐ Si $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$, entonces $(p \cdot q)(x) = \sum_{k=0}^{n} a_k b_k x^k$.

17. ☐ Si $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$, entonces el k-ésimo coeficiente de $(p \cdot q)(x)$ es $\sum_{i=0}^{k} a_i b_i$.

18. ☐ Si $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{k=0}^{n} b_k x^k$, entonces el k-ésimo coeficiente de $(p \cdot q)(x)$ es $\sum_{i=0}^{k} a_i b_{k-i}$.

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 $(p^2)(x)$ es siempre par.

24. ☐ Dado un polinomio no nulo $p(x)$, el grado del polinomio $(p^2)(x)$ 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 $\cdot$).

33. ☐ Si $p, d \in \mathbb{K}[x]$ y $d \neq 0$, entonces existen $q, r \in \mathbb{K}[x]$ tales que $p = q \cdot d + r$.

34. ☐ Si $p, d \in \mathbb{K}[x]$ y $d \neq 0$, entonces existe $q \in \mathbb{K}[x]$ tales que $p = q \cdot d$.

35. ☐ 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 $\text{gr}(d) > \text{gr}(r)$.

36. ☐ Para cualquier $p \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, entonces el resto de dividir p por $(x - c)$ es siempre cero.

37. ☐ Para cualquier $p \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, entonces el resto de dividir p por $(x - c)$ es $p(c) - c$.

38. ☐ Para cualquier $p \in \mathbb{K}[x]$ y $c \in \mathbb{K}$, entonces el resto de dividir p por $(x - c)$ es $p(c)$.

39. ☐ $c \in \mathbb{K}$ es raíz de $p \in \mathbb{K}[x]$ si y sólo si $p(c) = c$.

40. ☐ $c \in \mathbb{K}$ es raíz de $p \in \mathbb{K}[x]$ si y sólo si $p(c) = 0$.

41. ☐ $c \in \mathbb{K}$ es raíz de $p \in \mathbb{K}[x]$ si y sólo si el resto de dividir p por $(x + c)$ es cero.

42. ☐ $c \in \mathbb{K}$ es raíz de $p \in \mathbb{K}[x]$ si y sólo si el resto de dividir p por $(x - c)$ es cero.

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. Demuestre la siguiente propiedad propuesta en la tutorÃa: Sean $n \geq 1$, y $p, q \in \mathbb{K}[x]$ tales que $\text{gr}(p) \leq n$ y $\text{gr}(q) \leq n$. Si p y q coinciden en $n+1$ puntos distintos, entonces son iguales (como polinomios). Para ello:

(a) Pruebe que dado $n \in \mathbb{N}$, si un polinomio r es tal que $\text{gr}(r) \leq n$ y tiene $n+1$ raíces, entonces $r = 0$. O sea, r es el polinomio nulo.

(b) Concluya la propiedad, considerando el polinomio $r = p - q$ y aplicando lo anterior.

3. Considere $p(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[x]$, pruebe que si $\sum_{k=0}^{n} a_k = 0$ entonces $x = 1$ es raíz de p.

4. 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.

5. 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) Use el Algoritmo de Horner (Regla de Ruffini), para encontrar todas las raíces de p en $\mathbb{Q}$.
Indicación: Le basta buscar en el conjunto A, encontrado en la parte (a).

6. 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) $p(x) = 3x^3 - 5x^2 - x - 2$.

Indicación: Use el Algoritmo de Horner.

Guía de Problemas

P1. (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.

P2. (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.

P3. (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 $x^2 + x + 1$.

P4. (30 min.) Sea $p(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n$, con $a_0, \ldots, a_{n_1} \in \mathbb{C}$, 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 $\bar{z}$ también lo es. Demuestre que $a_0, \ldots, a_{n-1} \in \mathbb{R}$.
Indicación: Estudie el producto de polinomios $(x - z)(x + \bar{z})$ donde $z \in \mathbb{C}$.

P5. (30 min.) Sean $p(x) \in \mathbb{C}[x]$, $\text{gr}(g(x)) \geq 4$, $a, b, c \in \mathbb{R}$, 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 $r(x)$.

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 $c_1, c_2, \ldots, c_k$ son raíces distintas del polinomio p, entonces $(x-c_1)(x-c_2)\ldots(x-c_k) \mid p(x)$.

2. ☐ Si $c_1, c_2, \ldots, c_k$ son raíces distintas del polinomio p, entonces $(x+c_1)(x+c_2)\ldots(x+c_k) \mid p(x)$.

3. ☐ 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.

4. ☐ Un polinomio $p \in \mathbb{K}[x]$ de grado $n \geq 1$, posee a lo más n raíces distintas.

5. ☐ Un polinomio $p \in \mathbb{K}[x]$ de grado $n \geq 1$, posee al menos $n+1$ raíces distintas.

6. ☐ Existen polinomios no nulos de grado $n \geq 1$, con $n+1$ raíces distintas.

7. ☐ Si dos polinomios de grado $n \geq 1$ tienen el mismo valor en $n+1$ puntos, entonces son iguales.

8. ☐ Si dos polinomios de grado $n \geq 1$ tienen el mismo valor en n puntos, entonces son iguales.

9. ☐ Si un polinomio que tiene grado a lo más $n \geq 1$, toma el mismo valor en n puntos, entonces es un polinomio constante.

10. ☐ 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.

11. ☐ El Teorema Fundamental del Álgebra se nala que todo polinomio en $\mathbb{C}[x]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{R}$.

12. ☐ El Teorema Fundamental del Álgebra se nala que todo polinomio en $\mathbb{C}[x]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{C}$.

13. ☐ El Teorema Fundamental del Álgebra se nala que todo polinomio en $\mathbb{R}[x]$, de grado $n \geq 1$, tiene al menos una raíz en $\mathbb{R}$.

14. ☐ 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 $p(x) = (x-c_1)^{l_1}(x-c_2)^{l_2}\ldots(x-c_m)^{l_m}$.

15. ☐ 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 $p(x) = \alpha(x-c_1)^{l_1}(x-c_2)^{l_2}\ldots(x-c_m)^{l_m}$.

16. ☐ 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 $p(x) = \alpha(x+c_1)^{l_1}(x+c_2)^{l_2}\ldots(x+c_m)^{l_m}$.

17. ☐ 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 $p(x) = \alpha(x-c_1)^{l_1}(x-c_2)^{l_2}\ldots(x-c_m)^{l_m}$.

18. ☐ Dado un polinomio $p \in \mathbb{C}[x]$, si $z \in \mathbb{C}$ es raíz de p, entonces $\overline{z}$ también lo es.

19. ☐ Dado un polinomio $p \in \mathbb{R}[x]$, si $z \in \mathbb{C}$ es raíz de p, entonces $\overline{z}$ también lo es.

20. ☐ Dado un polinomio $p \in \mathbb{R}[x]$, si $z \in \mathbb{C}$ es raíz de p, entonces $-z$ también lo es.

21. ☐ Dado un polinomio $p \in \mathbb{C}[x]$, si $z \in \mathbb{C}$ es raíz de p, entonces $-z$ también lo es.

22. ☐ Existe un polinomio $p \in \mathbb{R}[x]$ de grado 3, con 3 raíces en $\mathbb{C} \setminus \mathbb{R}$.

23. ☐ No existe un polinomio $p \in \mathbb{C}[x]$ de grado 3, con 3 raíces en $\mathbb{C} \setminus \mathbb{R}$.

24. ☐ Existe un polinomio $p \in \mathbb{R}[x]$ de grado 4, con 4 raíces en $\mathbb{C} \setminus \mathbb{R}$.

25. ☐ Existe un polinomio $p \in \mathbb{R}[x]$ de grado $n \geq 1$, con exactamente una raíz en $\mathbb{C} \setminus \mathbb{R}$.

26. ☐ Todo polinomio $p \in \mathbb{R}[x]$ de grado $n \geq 1$, tiene un número par de raíces en $\mathbb{C} \setminus \mathbb{R}$.

27. ☐ Todo polinomio $p \in \mathbb{R}[x]$ de grado $n \geq 1$, tiene un número impar de raíces en $\mathbb{C} \setminus \mathbb{R}$.

28. ☐ Todo polinomio $p \in \mathbb{R}[x]$ tiene al menos una raíz real.

29. ☐ Todo polinomio $p \in \mathbb{C}[x]$ tiene al menos una raíz compleja.

30. ☐ Si $a_0, \ldots, a_n \in \mathbb{Z}$, son los coeficientes del polinomio $p \in \mathbb{R}[x]$, entonces el numerador en la escritura $\frac{r}{s}$ de toda raíz $x \in \mathbb{Q}$ de p, divide a a_0.

31. ☐ Si $a_0, \ldots, a_n \in \mathbb{Z}$, son los coeficientes del polinomio $p \in \mathbb{R}[x]$, entonces el denominador en la escritura $\frac{r}{s}$ de toda raíz $x \in \mathbb{Q}$ de p, divide a a_0.

32. ☐ Si $a_0, \ldots, a_n \in \mathbb{Z}$, son los coeficientes del polinomio $p \in \mathbb{R}[x]$, entonces el denominador en la escritura $\frac{r}{s}$ de toda raíz $x \in \mathbb{Q}$ de p, divide a a_n.

33. ☐ Existe un polinomio mónico con coeficientes enteros que tiene a $x = \frac{1}{3}$ como raíz.

34. ☐ Las únicas raíces racionales posibles de un polinomio mónico con coeficientes enteros son números enteros.

35. ☐ $x = \frac{1}{2}$ es raíz del polinomio $p(x) = 17x^{19} + 5x^{11} - 3x^5 + x - 1$.

36. ☐ $x = 2$ es raíz del polinomio $p(x) = x^{16} + 5x^8 - 3x^2 + x - 3$.

Guía de Problemas

P1. (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.

P2. (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.

P3. 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 $\forall j = 1, \ldots, n \quad p(x_j) = y_j$. 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 $j = 1, \ldots, n$ definimos:

$$l_j(x) = \frac{\Pi_{k=1(k\neq j)}^n (x - x_k)}{\Pi_{k=1(k\neq j)}^n (x_j - x_k)} \in \mathbb{K}[x].$$

1. Determine el grado de $l_j(x)$ y pruebe que:

$$l_j(x_r) = \delta_{jr} = \begin{cases} 1, & j = r \\ 0, & j \neq r \end{cases} \qquad \forall j, r = 1, \ldots, n.$$

2. Demuestre que $p(x) = \sum_{j=1}^n y_j l_j(x) \in \mathbb{K}[x]$ es polinomio de interpolación para la familia $(\{x_j\}_{j=1}^n, \{y_j\}_{j=1}^n)$.

P4. Sea $J_2 = \{p(x) \in \mathbb{R}[x] \mid \text{gr}(p) \leq 2, a_0 = 0, a_1 \neq 0\}$. En J_2 se define la l.c.i. $\triangle$ a través de $p(x) \triangle q(x) = \sum_{i=1}^2 c_i x^i$ en que $p(q(x)) = \sum_{i=0}^n c_i x^i$.

(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 $f(a_1 \cdot x + a_2 \cdot x^2) = a_1$. Probar que f es un morfismo sobreyectivo de $(J_2, \triangle)$ en $(\mathbb{R} \setminus \{0\}, \cdot)$.

(c) (20 min.) Sea $H = \{p(x) \in J_2 \mid a_2 = 1\}$. Probar que $(H, \triangle)$ es subgrupo abeliano de $(J_2, \triangle)$.