

2.1. Técnicas inspiradas en deducción natural

En clases anteriores hemos discutido la deducción natural como sistema formal de demostraciones. En esta clase hablaremos de técnicas de demostración, inspiradas en deducción natural, pero esta vez con foco en la escritura de demostraciones en lenguaje natural. El objetivo acá es que el lector sea capaz de entender y validar las demostraciones más que el hecho de tener inferencia sintáctica.

Veremos entonces varias técnicas de demostración, inspiradas en la deducción natural, para varios conectivos lógicos y cuantificadores.

2.1.1. Técnicas de demostración: implicancia

Demostración directa La demostración directa se usa cuando queremos probar una implicancia de la forma “si P , entonces Q ” avanzando desde las hipótesis hacia la conclusión. La idea es suponer verdadera la premisa y, mediante definiciones o propiedades conocidas, deducir paso a paso propiedades intermedias, hasta llegar a la conclusión.

Proposición. Si $n \in \mathbb{N}$ es par, entonces n^2 es par.

Demostración. Como n es par, existe $k \in \mathbb{N}$ tal que $n = 2k$. Por lo tanto,

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Como $n^2 = 2(2k^2)$, tenemos que n^2 es par. □

Demostración por contrarrecíproca Esta técnica consiste en probar la afirmación lógicamente equivalente: en vez de demostrar “ $P \rightarrow Q$ ”, demostramos “ $\neg Q \rightarrow \neg P$ ”. Suele ser útil cuando trabajar con la negación de la conclusión permite un argumento más natural o da más información.

Proposición. Si $n \in \mathbb{N}$ es tal que n^2 es par, entonces n es par.

Demostración. Por contrarrecíproca, si n es impar, entonces existe $k \in \mathbb{N}$ tal que $n = 2k + 1$. Por lo tanto, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, y de esto tenemos que n^2 es impar. □

2.1.2. Técnicas de demostración: disyunción

Demostración por casos: La demostración por casos se aplica cuando la información disponible se expresa como una disyunción, o cuando podemos particionar el problema en escenarios. Se demuestra la misma conclusión en cada caso y, como no quedan alternativas, la conclusión vale en general.

Proposición. Si $n \in \mathbb{N}$ no es múltiplo de 3, entonces 3 divide a $n^2 - 1$.

Demostración. Tenemos dos casos: o $n = 3k + 1$ para algún $k \in \mathbb{N}$, o $n = 3k + 2$ para algún $k \in \mathbb{N}$. En el primer caso,

$$n^2 - 1 = (3k + 1)^2 - 1 = (3k + 2)3k.$$

De esto, tenemos que 3 divide a $n^2 - 1$. En el segundo caso,

$$n^2 - 1 = (3k + 2)^2 - 1 = (3k + 3)(3k + 1) = 3(k + 1)(3k + 1).$$

De esto, tenemos que 3 divide a $n^2 - 1$. □

2.1.3. Técnicas de demostración: negación

Reescritura de la negación. Cuando el objetivo es una negación, muchas veces conviene reescribirla en una forma equivalente más manejable “en positivo”. Esto se debe a que, en general, la negación de una afirmación es más difícil de trabajar que una “afirmación positiva”.

Proposición. Sean A, B, C conjuntos tales que $A \cap C \subseteq B$. Sea $a \in C$. Pruebe que $a \notin A \setminus B$.

Demostración. Notemos que $a \notin A \setminus B$ es equivalente a

$$a \notin A \vee a \in B \equiv a \in A \implies a \in B.$$

Por lo tanto, supongamos que $a \in A$. De esto y de que $a \in C$ se sigue que $a \in A \cap C$. Como $A \cap C \subseteq B$, tenemos que $a \in B$. □

Contradicción En una demostración por contradicción suponemos temporalmente que la afirmación que queremos probar es falsa y derivamos una contradicción. Por reducción al absurdo, podemos entonces concluir que la afirmación original es verdadera.

Teorema. $\sqrt{2}$ es irracional.

Demostración. Supongamos, en busca de una contradicción, que $\sqrt{2}$ es racional. Entonces, existe $p, q \in \mathbb{N}$ con $q \neq 0$ y $\gcd(p, q) = 1$ tal que $\sqrt{2} = \frac{p}{q}$. Concluimos que $2 = \frac{p^2}{q^2}$, y por lo tanto, $p^2 = 2q^2$. De esto obtenemos que p^2 es par y por lo demostrado anteriormente, p es par. Como p es par, existe $k \in \mathbb{N}$ tal que $p = 2k$. Luego, $2q^2 = p^2 = (2k)^2 = 4k^2$, y por lo tanto, $q^2 = 2k^2$. Obtenemos que q^2 es par, y por ende, q es par. Concluimos que p y q son pares, lo cual es una contradicción, ya que $\gcd(p, q) = 1$. □

2.1.4. Demostraciones con equivalencias

Separación de la equivalencia. Cuando el objetivo es una equivalencia $P \leftrightarrow Q$, una estrategia común es separar la demostración en dos implicancias: “ $P \rightarrow Q$ ” y “ $Q \rightarrow P$ ”.

Proposición. Sean $x, y \in \mathbb{Z}$. Demuestre que x y y tienen la misma paridad si y sólo si $x + y$ es par.

Demostración. Primero, demostraremos que si x y y tienen la misma paridad, entonces $x + y$ es par. Si x y y son ambos pares, entonces existen $k, l \in \mathbb{Z}$ tales que $x = 2k$ y $y = 2l$, y por lo tanto, $x + y = 2(k + l)$ es par. Si x y y son ambos impares, entonces existen $k, l \in \mathbb{Z}$ tales que $x = 2k + 1$ y $y = 2l + 1$, y por lo tanto, $x + y = 2(k + l + 1)$ es par.

Ahora, demostraremos que si $x + y$ es par, entonces x y y tienen la misma paridad. Por contrarrecíproca, si x e y no tienen la misma paridad, entonces, sin pérdida de generalidad, supongamos que x es par y y es impar. Entonces, existen $k, l \in \mathbb{Z}$ tales que $x = 2k$ y $y = 2l + 1$, y por lo tanto, $x + y = 2(k + l) + 1$ es impar. $\square$

Cadena de equivalencias Algo que sirve a veces para demostrar algunas equivalencias es escribir una cadena de equivalencias, es decir, una secuencia de enunciados $P_1, P_2, \dots, P_n$ tal que P_1 y P_n son los enunciados que queremos demostrar equivalentes y, para cada i , $P_i \leftrightarrow P_{i+1}$.

Proposición. Sean A, B, C conjuntos. Entonces $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Demostración. Sea x un elemento arbitrario. Notemos que nos piden probar que $x \in A \setminus (B \cup C)$ es equivalente a $x \in (A \setminus B) \cap (A \setminus C)$. Por lo tanto, escribamos una cadena de equivalencias:

$$\begin{aligned} x \in A \setminus (B \cup C) &\leftrightarrow x \in A \wedge x \notin (B \cup C) \\ &\leftrightarrow x \in A \wedge x \notin B \wedge x \notin C \\ &\leftrightarrow x \in A \setminus B \wedge x \in A \setminus C \\ &\leftrightarrow x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

Como x era arbitrario, concluimos que los conjuntos son iguales. $\square$

2.1.5. Demostraciones con cuantificadores

Cuantificador universal Cuando un enunciado tiene cuantificadores, la estrategia depende de su forma lógica. Para probar “ $\forall x \in A, P(x)$ ”, tomamos un elemento arbitrario $x \in A$ y demostramos $P(x)$.

Proposición. Para todo $x, y \in \mathbb{Q}$, tenemos que $x + y \in \mathbb{Q}$.

Demostración. Sean $x, y \in \mathbb{Q}$. Entonces, existen $a, b, c, d \in \mathbb{Z}$ con $b, d \neq 0$ tales que $x = \frac{a}{b}$ y $y = \frac{c}{d}$. Por lo tanto,

$$x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Como $ad + bc \in \mathbb{Z}$ y $bd \in \mathbb{Z} \setminus \{0\}$, tenemos que $x + y \in \mathbb{Q}$. $\square$

Cuantificador existencial Para probar un enunciado de la forma “ $\exists x \in A, P(x)$ ”, basta con encontrar un elemento específico $x \in A$ que satisfaga $P(x)$ y demostrar que efectivamente lo hace.

Proposición. Existe $m \in \mathbb{Z}$ tal que $\frac{m-7}{2m+4} = 5$.

Demostración. Tomamos $m = -3$. Entonces,

$$\frac{m-7}{2m+4} = \frac{-3-7}{2(-3)+4} = \frac{-10}{-2} = 5.$$

Por lo tanto, existe un entero m que satisface la ecuación. $\square$

Notemos que usualmente obtenemos el candidato a ser el elemento que satisface la afirmación buscando propiedades que nos indiquen quién o cómo debe ser dicho elemento. Por ejemplo, en el caso anterior, podríamos haber despejado m de la ecuación dada para encontrar el candidato a ser el elemento que satisface la afirmación.

Ejercicios

1. Demuestre las siguientes afirmaciones:

- a) Para todo $a, b, k \in \mathbb{Z}$, tenemos que a divide a b si y sólo si a divide a $b + ak$.
- b) Para todo $n \in \mathbb{Z}$, tenemos que $n(n + 1)$ es par.
- c) Si 4 divide a n^2 , entonces n es par.
- d) Para tres conjuntos A, B, C , tenemos que $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.
- e) Si x^2 es irracional, entonces x es irracional.
- f) $\sqrt{3}$ es irracional.
- g) El conjunto de los números racionales positivos no tiene un elemento mínimo.

2. Diremos que una función $f: \mathbb{R} \rightarrow \mathbb{R}$ es *par* si $f(-x) = f(x)$ para todo $x \in \mathbb{R}$, e *impar* si $f(-x) = -f(x)$ para todo $x \in \mathbb{R}$.

- a) Demuestre que si $f_i: \mathbb{R} \rightarrow \mathbb{R}$ es impar y $f_p: \mathbb{R} \rightarrow \mathbb{R}$ es par, entonces $f_i \cdot f_p$ es una función impar.
- b) Demuestre que si f y g son impares, entonces $f + g$ es impar y $f \cdot g$ es par.
- c) Demuestre que si $f: \mathbb{R} \rightarrow \mathbb{R}$ es una función, entonces $f(x) + f(-x)$ es una función par.
- d) Demuestre que toda función $f: \mathbb{R} \rightarrow \mathbb{R}$ puede escribirse como suma de una función par y una impar.
- e) Demuestre que la descomposición de una función en suma de una función par y una impar es única.

3. Una *terna pitagórica* es una terna (a, b, c) de enteros positivos que satisface $a^2 + b^2 = c^2$. Diremos que la terna es *primitiva* si no existe un entero $d > 1$ que divida simultáneamente a a , b y c .

- a) Demuestre que, para todo $n \in \mathbb{Z}$, se cumple que n^2 es congruente con 0 o 1 módulo 4.
- b) Deduzca que ningún cuadrado entero puede escribirse como $4q + 2$ con $q \in \mathbb{Z}$ y que, si $4 \mid n^2$, entonces n es par.
- c) Sea (a, b, c) una terna pitagórica. Demuestre por contradicción que a y b no pueden ser ambos impares.
- d) Suponga ahora que la terna es primitiva. Demuestre por contradicción que a y b tampoco pueden ser ambos pares.
- e) Concluya que exactamente uno de a, b es par y demuestre que c es impar.