Orientaciones para la construcción y la escritura de una demostración

Mahsa Allahbakhshi[1], Duvan Henao[1], Ricardo Menares[1] y Natalia Leiva[2]

[1]Facultad de Matemáticas UC

[2]Proyecto Ciencia 2030 UC

Índice

Introducción

Ser capaz de demostrar verdades es una habilidad esencial en estadística y matemática, por múltiples razones. Algunas veces es porque da sustento a un método práctico, como al demostrar que la distribución de probabilidad de los resultados de un experimento binario, repetido suficientes veces, se acerca tanto como uno quiera a la conocida distribución normal. Este teorema nos hace confiar más en el uso de la distribución normal en mecanismos de decisión que afectan nuestras vidas, por ejemplo, al establecer rangos de valores en exámenes de laboratorio para el diagnóstico y tratamiento de enfermedades. Otras veces es por el valor que tiene una demostración en sí misma, aunque no tuviera aplicaciones prácticas. Un ejemplo es demostrar que el camino más corto entre dos puntos es la línea recta. Sabemos que esto es cierto, y construimos caminos basados en eso, sin que una demostración matemática sea necesaria. Sin embargo, proponerse demostrarlo es un desafío digno de nuestras capacidades mentales como seres humanos. El que hace más de 150 años lo hayamos conquistado es notable y la experiencia de comprobar (también) matemática y rigurosamente que es algo cierto resulta siempre una experiencia fascinante.

Asimismo, hay verdades que solo podemos ver con los ojos de la lógica, como que hay infinitos números primos; que hay infinitos más grandes que otros; o que las funciones tienen doble personalidad, como propuso Fourier[1]. Sobre este último punto, el debate en la primera mitad del siglo XIX fue dramáticamente intenso, por la sencilla razón de que no había forma de ver de antemano si la afirmación era verdadera. Laplace, Lagrange, Lacroix, Monge y Poisson (¡grandes héroes!) descartaron de plano el artículo enviado por Fourier al Institut de France el 20 de diciembre de 1807, haciendo eco de las críticas de Euler a Bernoulli quien había osado sugerir algo similar 50 años antes. Solo con los teoremas que resultaron del arduo trabajo de décadas de Fourier, Dirichlet y Riemann, entre otros, se hizo evidente que la doble personalidad era cierta. Y no se trata de algo sin importancia práctica, pues el método de Fourier se usa y se ha usado en muchas partes, como en la instalación del primer cable transatlántico (que le mereció el título nobiliario a Lord Kelvin), en las cavas subterráneas de nuestras viñas o en innumerables desarrollos de las telecomunicaciones y el procesamiento de señales.

En Matemáticas, establecemos que una proposición es verdadera escribiendo una demostración matemática. En consecuencia, quien cultiva las Matemáticas debe ser capaz de descubrir y construir demostraciones. Además, una vez encontrada la estructura de la demostración, se debe ser capaz de comunicarla a otras personas que hablen el lenguaje de las matemáticas. Un recurso común es hacer de antemano una conjetura sobre si la afirmación es verdadera o falsa, a menudo mediante la exploración.

[1] Que una función, además de verse como una f(x) que a cada x le asigna un valor, también puede representarse como una serie trigonométrica (una superposición de infinitas ondas viajando a distintas frecuencias). Ver, p.ej., D. Bressoud, *A radical approach to real analysis*, MAA, 2º ed. (2007).

El papel de la exploración en Matemáticas suele ser difícil, porque el objetivo no es encontrar una respuesta concreta, sino simplemente investigar.

En términos generales, se puede considerar que hacer matemáticas tiene dos etapas distintas. La primera etapa consiste en convencerse de que se ha resuelto el problema. Esta etapa es creativa y a menudo es la forma en que se hacen las matemáticas. La segunda etapa, igualmente importante, consiste en convencer a otras personas de que se ha resuelto el problema por medio de una demostración, es decir, un argumento convincente de que una determinada afirmación matemática es necesariamente cierta. Esta segunda etapa es diferente de la primera, en el sentido de que no se comunica necesariamente el proceso a través del cual se ha resuelto el problema. Una demostración generalmente utiliza el razonamiento deductivo y la lógica, pero también contiene cierta cantidad de lenguaje natural (como el español o el iraní). En el ejercicio de escribir una demostración, puede ocurrir que se adviertan elementos que en la etapa creativa se habían pasado por alto e incluso que se descubra que la solución a la que se había llegado estaba incompleta.

Escribir demostraciones es todo un arte. Este documento no pretende explicar cómo se cultiva este arte, el cual irán madurando y puliendo durante sus estudios. Pero, al momento de hacer demostraciones, ayuda tener presente que estas tienen siempre una cierta estructura general. El hecho mismo de recordar esta estructura entrega ciertas pistas sobre cómo deben hilarse los argumentos, orienta y da una dirección de partida, una cierta luz, para al menos identificar cuáles son las piezas del rompecabezas que hay que armar. El propósito de este documento es describir en general esa estructura, y en base a ella brindar recomendaciones tanto para el proceso de pensar una demostración, como para el ejercicio de escribirla, pasando en limpio las ideas encontradas para poder comunicarlas.

El documento se organiza en dos grandes capítulos. En el primero, se presenta y ejemplifica la estructura general de una demostración. En el segundo, se presentan ocho recomendaciones generales para la escritura de demostraciones. En el primer capítulo, las dos últimas secciones ("Los axiomas" y "El lenguaje de las conexiones lógicas") puede que requieran de mayor madurez para una comprensión cabal. Si en una primera lectura sientes que no estás comprendiendo estas partes, no te desanimes y avanza al apartado de recomendaciones generales.

I. ¿Cómo se hace una demostración?

Este capítulo aborda la pregunta de cómo se hace una demostración a partir de cinco secciones: la estructura general de las demostraciones, la demostración de una proposición condicional, las conexiones lógicas discursivas, los axiomas y el lenguaje de las conexiones lógicas.

1. La estructura general de las demostraciones

Esta sección se refiere a la estructura general de las demostraciones. Para comenzar, se muestra un ejemplo de una demostración.

Demuestre que el producto de dos números impares es impar

Solución:

Supongamos que x e y son números impares. Demostremos que el producto xy es impar.

Como x es impar, entonces puede escribirse como

$x = 2n + 1$,

para algún entero n. En forma similar, que y sea impar implica que y puede escribirse como

$y = 2m + 1$,

para algún entero m. Se sigue que

$xy = (2n+1)(2m+1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1$.

Concluimos que xy puede escribirse como

$xy = 2k + 1$,

para un cierto entero k, a saber, k=2nm+n+m. Por lo tanto, xy es impar, que es lo que queríamos demostrar.

Independientemente del proceso intuitivo y creativo mediante el cual a alguien se le ocurre una demostración -el producto final de ese ejercicio de pensamiento-, la demostración misma es un *razonamiento deductivo*. En una demostración, unas verdades se van deduciendo de otras. Va creciendo, paso a paso, el conjunto de los recursos de los que disponemos para seguir avanzando en la demostración. El punto de partida es todo aquello que ya habíamos establecido que era cierto, desde antes de comenzar la demostración. Por ejemplo, al comienzo de la demostración usamos dos veces que

si un número es impar, entonces puede escribirse como 2r+1 *para algún entero* r,

y al final de la demostración usamos que

si un número puede escribirse como 2k+1 *para algún entero* k, *entonces es impar*.

Esas dos afirmaciones las sabíamos desde antes. Formaban parte de los recursos que podíamos emplear para fabricar la nueva demostración pedida. ¿Por qué sabíamos que esas afirmaciones eran ciertas? Estas se obtuvieron (como un teorema anterior) a partir de *la definición* de número impar ("un número que no es el doble de ningún número entero") unida al algoritmo de la división. Otras verdades que desde antes habíamos establecido que eran ciertas, y que usamos en la demostración, son:

- que $(2n+1)(2m+1) = 4nm + 2n + 2m + 1$ para cualquier par de enteros n y m;
- que $4nm + 2n + 2m = 2\,(2nm + n + m)$ para cualquier par de enteros n y m;
- y que si dos cantidades, en este caso $4nm + 2n + 2m$ y $2\,(2nm + n + m)$, son iguales, entonces al sumar una unidad a cada una de ellas, las cantidades obtenidas también resultan ser iguales, esto es, que

  si $a = b$, entonces $a + 1 = b + 1$,

  lo cual nos permitió descubrir que

  $$4nm + 2n + 2m + 1 = 2\,(2nm + n + m) + 1.$$

Esas eran verdades establecidas desde antes. Por otra parte, la demostración comenzó generando dos nuevas verdades, de un tipo particular:

- que durante toda la demostración el símbolo x representaría a un cierto número debidamente individualizado, el cual es impar,
- y que el símbolo y representaría también a un número particular, que podría ser diferente al que representa x, pero del cual también se asumirá como cierto que es impar.

Esas dos nuevas verdades, las cuales son hipótesis de la demostración, fueron generadas mediante la frase "Supongamos que x e y son números impares", recurso lingüístico utilizado con frecuencia cuando lo que se quiere demostrar es que alguna propiedad se cumple *para todos* los elementos, o, por ejemplo, para *todo par* de elementos de un conjunto (en este caso, el conjunto de los números impares).

Durante la demostración aparecieron después nuevas verdades intermedias que fueron *deducidas* de las anteriores, y de *las suposiciones iniciales* mencionadas anteriormente:

- que xy puede escribirse como $(2n+1)(2m+1)$ para algún par de enteros n y m,
- que $xy = 4nm + 2n + 2m + 1$,
- que $xy = 2(2nm + n + m) + 1$,
- que xy puede escribirse como $2k+1$ para algún entero k.

Finalmente, se deduce que xy es impar, que es la conclusión a la que se quiere llegar.

En resumen, la estructura de una demostración es la de una concatenación (lineal) de afirmaciones, cada una de las cuales es consecuencia de verdades anteriores, que culmina con la afirmación que se quiere demostrar. Cada paso de la demostración debe justificarse: es preciso mostrar por qué cada afirmación se desprende de las verdades anteriores (tanto las verdades que se conocían desde antes de empezar la demostración, como aquellas que corresponden a suposiciones o hipótesis realizadas en el argumento y aquellas verdades intermedias, auxiliares, que se establecieron durante la demostración).

2. La demostración de una proposición condicional

En el ejemplo anterior demostramos que:

si x *e* y *son impares, entonces* xy es impar.

Esta es una proposición condicional (a veces denominada, simplemente, "condicional"), es decir, una proposición de la forma "si P, entonces Q", donde P y Q son, a su vez, proposiciones[2]. Para que la proposición "si P, entonces Q" sea verdadera, Q debe ser verdadera cada vez que P es verdadera. La proposición A se llama hipótesis de la proposición condicional, y la proposición B se llama conclusión o tesis del condicional.

Las proposiciones condicionales $P \rightarrow Q$ cumplen un rol clave en el razonamiento matemático. Podemos encontrarlas expresadas de una variedad de maneras, que se muestran y ejemplifican en la siguiente tabla:

Expresión	Ejemplo (asumiendo que x es un número real cualquiera)
P implica Q	$x>1$ implica $x^2>1$
Si P, entonces Q	Si $x>1$, entonces $x^2>1$
$P \rightarrow Q$	$x>1 \rightarrow x^2>1$
P si Q	$x^2>1$ si $x>1$
Si P, Q	Si $x>1$, $x^2>1$
Si P, concluimos que Q	Si $x>1$, concluimos que $x^2>1$
Q se sigue de P	Que $x^2>1$ se sigue de $x>1$
P es suficiente para Q	Basta que $x>1$ para que x^2 sea mayor que 1.
Q siempre que P	$x^2>1$ siempre que $x>1$.

[2] Por "proposición" entendemos una oración declarativa que debe tener un valor de verdad definido, ya sea verdadero o falso, pero no ambos. Para ser una proposición, una frase debe ser verdadera o falsa, y no puede ser ambas cosas. Por tanto, una frase como 'El cielo es hermoso' no es una proposición, ya que si la frase es verdadera o no es una cuestión de opinión. Una pregunta como '¿Está lloviendo?' no es una proposición porque es una pregunta y no está declarando o afirmando que algo es cierto.

Q es necesario para P	Es necesario que $x^2>1$ si queremos que x sea mayor que 1.
P solo si Q (Esta forma de expresar el condicional es menos frecuente[3])	x será mayor que 1 solo si $x^2>1$.

Desafortunadamente, con frecuencia no es fácil descubrir la secuencia lógica de pasos buscada en una demostración, descubrir cómo obtener que la conclusión Q es verdadera. El siguiente método exploratorio puede ayudar a descubrir los pasos de una demostración. En este método trabajamos hacia adelante desde la hipótesis P, y hacia atrás desde la conclusión Q. Podemos usar una tabla como la siguiente, e ir llenándola poco a poco, para ayudar a organizar nuestras ideas y los pasos de la demostración.

El primer paso es identificar la hipótesis, P, y la conclusión, Q, de la proposición condicional. En el ejemplo estudiado, tenemos las siguientes:

P representa la afirmación "x e y son impares",
Q representa la afirmación "xy es impar".

Ahora tratamos a P como aquello que sabemos (lo que hemos asumido como cierto), y tratamos a Q como lo que queremos mostrar (esto es, la meta). Organizamos esto usando P como el primer paso en la parte de la tabla que corresponde a *verdades sabidas*, y a Q como el último paso en la parte de la tabla que corresponde a *verdades por mostrar*. Usaremos la parte de arriba de la tabla para lo sabido, y la parte de abajo para lo que aún debemos mostrar.

Paso	Lo que ya sabemos	Razón
P	x e y son enteros impares	Hipótesis
$P1$		
$\vdots$	$\vdots$	$\vdots$
$Q1$		
Q	$x{\cdot}y$ es un entero impar	?
Paso	A lo que queremos llegar	Razón

[3] Podría aparecer, por ejemplo, si queremos calcular el valor de |x-1| y al principio solo sabemos que x es positivo y sabemos algo sobre x^2.

Todavía no hemos rellenado la razón del último paso porque aún no sabemos cómo vamos a alcanzar el objetivo. La idea ahora es hacernos preguntas sobre lo que sabemos y lo que intentamos demostrar. Por lo general, empezamos con la conclusión que intentamos demostrar formulando la llamada 'pregunta retrospectiva'. La forma básica de la pregunta es: "¿Bajo qué condiciones podemos concluir que Q es verdadera?". La manera de formular la pregunta es crucial, ya que debemos ser capaces de responderla. Primero debemos tratar de formular y responder la pregunta de forma abstracta y luego aplicarla a la forma particular del enunciado Q.

En este caso, estamos tratando de demostrar que algún número entero es un número entero impar. Así que nuestra pregunta inversa podría ser: "¿Cómo demostramos que un número entero es impar?". En este momento, la única manera que tenemos de responder a esta pregunta es utilizar la definición de un número entero impar. Así que nuestra respuesta podría ser: "Tenemos que demostrar que existe un número entero q tal que el número entero en consideración puede escribirse como $2q + 1$". Aplicamos esta respuesta al enunciado Q y la insertamos como la penúltima línea en la tabla de conocimientos.

Paso	Sé	Razón
P	x e y son enteros impares	Hipótesis
$P1$		
$\vdots$	$\vdots$	$\vdots$
$Q1$	Existe un entero q tal que $x \cdot y = 2q + 1$	
Q	$x \cdot y$ es un entero impar	Definición de un entero impar
Paso	Muestro	Razón

Ahora centramos nuestro esfuerzo en demostrar el enunciado Q1, ya que sabemos que si podemos demostrar Q1, entonces podemos concluir que Q es verdadero. Hacemos una pregunta retrospectiva sobre Q1 como: "¿Cómo podemos demostrar que existe un entero q tal que $x \cdot y = 2q + 1$?" Es posible que no tengamos una respuesta preparada para esta pregunta, por lo que miramos la parte conocida de la tabla e intentamos conectar la parte conocida con la parte demostrada. Para ello, trabajamos hacia adelante desde el paso P, y esto implica hacer una pregunta hacia adelante. La forma básica de este tipo de pregunta es: "¿Qué podemos concluir del hecho de que P es verdadero?". En este caso, podemos utilizar la definición de número entero impar para concluir que existen números enteros m y n tales que $x = 2m + 1$ e $y = 2n + 1$. Llamaremos a esto Paso P1 en la tabla de conocimientos. Es importante notar que hemos tenido cuidado de no utilizar la letra q para denotar estos enteros. Si hubiéramos usado q de nuevo, estaríamos afirmando que el mismo número entero que da $x{\cdot}y = 2q + 1$ también da $x = 2q + 1$. Por eso usamos m y n para los enteros x e y, ya que no hay garantía de que x sea igual a y. La regla básica es usar un símbolo diferente para cada objeto nuevo que introducimos en una demostración. Así que en este punto, tenemos:

- Paso P1. Sabemos que existen enteros m y n tal que $x = 2m + 1$ e $y = 2n + 1$.

- Paso Q1. Necesitamos probar que existe un entero q tal que $x{\cdot}y = 2q + 1$.

Siempre debemos buscar una manera de vincular la parte “sé” con la parte “muestro”. Podemos sacar conclusiones a partir de $P1$, pero a medida que avanzamos, debemos tener siempre presente la forma del enunciado de $Q1$. La siguiente pregunta es: "¿Qué podemos concluir sobre $x{\cdot}y$ a partir de lo que sabemos?". Una forma de responder a esto es utilizar nuestros conocimientos previos de álgebra. Es decir, primero podemos usar la sustitución para escribir $x{\cdot}y = (2m + 1)\,(2n + 1)$. Aunque esta ecuación no demuestra que $x{\cdot}y$ es impar, podemos usar el álgebra para intentar reescribir el lado derecho como alguna otra expresión que podamos reconocer como un entero impar, para poder llegar al paso $Q1$. Primero expandimos el lado derecho de la ecuación para obtener

$$\begin{aligned} x{\cdot}y &= (2m + 1)\,(2n + 1) \\ &= 4mn + 2m + 2n + 1. \end{aligned}$$

Ahora comparamos el lado derecho de la última ecuación con el lado derecho de la ecuación del paso Q1. A veces la parte difícil en este punto es darse cuenta de que q representa algún número entero (cualquiera) y que lo que tenemos que demostrar es que $x{\cdot}y$ es igual a dos veces algún número entero más uno. ¿Podemos ahora llegar a esa conclusión? La respuesta es sí, porque podemos factorizar el número 2 desde los tres primeros términos del lado derecho de la ecuación y obtener

$$\begin{aligned} x{\cdot}y &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1. \end{aligned}$$

Ahora podemos completar, como sigue, la tabla que muestra el esquema de la demostración:

Paso	Sé	Razón
P	x e y son enteros impares	Hipótesis
$P1$	Existen enteros m y n tal que $x = 2m + 1$ e $y = 2n + 1$	Definición de un entero impar
P2	$xy = (2m + 1)(2n + 1)$	Sustitución
$P3$	$xy = 4mn + 2m + 2n + 1$	Álgebra
$P4$	$xy = 2\,(2mn + m + n) + 1$	Álgebra
$P5$	$2mn + m + n$ es un entero	Clausura del conjunto de números enteros
$Q1$	Existe un entero q tal que $xy = 2q + 1$	Usa $q = (2mn + m + n)$
Q	$x{\cdot}y$ es un entero impar	Definición de un entero impar
Paso	Muestro	Razón

Es muy importante notar que solo hemos construido *el bosquejo* de lo que será después una demostración. Las demostraciones matemáticas no se escriben como una tabla, sino utilizando frases completas y una estructura de párrafos. Además, la mayoría de las demostraciones se escriben desde lo ya sabido hacia adelante y no en la dirección contraria. Es decir, aunque el uso del proceso hacia atrás fue esencial para construir la demostración, cuando la escribimos utilizamos el proceso hacia adelante descrito en la tabla anterior. La demostración completa es la que se encuentra al comienzo de la sección, en la página 4.

3. Las conexiones lógicas discursivas

Hemos visto que una demostración tiene una estructura lineal en donde progresivamente se deducen nuevas verdades. Para conectar un eslabón con el siguiente en esta cadena de afirmaciones, para hilar este discurso razonado, debemos mostrar cómo se deduce la nueva verdad obtenida a partir de las verdades anteriores. Al hacer esto usamos ciertas palabras clave. En nuestro ejemplo, recurrimos a las siguientes expresiones (destacadas en negrita):

- *Como* x *es impar, entonces puede escribirse como* $x = 2n + 1$*, para algún entero* n.
- *Que* y *sea impar implica que* y *puede escribirse como* $y = 2m + 1$, para algún entero m.

- *Se sigue que* $xy = (2n+1)(2m+1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1$.
- *Concluimos que* xy *puede escribirse como* $xy = 2k + 1$ donde $k=2nm+n+m$.

En definitiva, hacemos uso de lo que denominaremos como conexiones lógicas discursivas. Estas no son exclusivas de la matemática, podemos encontrarlas también, por ejemplo, en un contrato legal o un discurso filosófico. Las siguientes son algunas expresiones mediante las que pueden representarse:

Por A, B
Por todo lo anterior (A), vemos que B
Como A, B
Como A, sabemos que B
A, entonces, B
A. Por lo tanto, B
A. Luego, B
A. En consecuencia, B
A. Se desprende que B
A. Se sigue que B
A. Tenemos que B
A. Se deduce que B
A. Lo anterior implica que B
A. Se concluye que B
A. Obtenemos que B

Vemos que las expresiones se parecen a las que encontramos en las proposiciones condicionales (las de la sección anterior, los enunciados de la forma "A implica B"). Sin embargo, aunque se trate de las mismas palabras, es conveniente tener presente que juegan roles diferentes. Discutiremos esto en la sección "El lenguaje de las conexiones lógicas" al final de este capítulo.

4. Los axiomas

En el ejemplo del producto de impares usamos, como verdad sabida antes de comenzar la demostración, que un número impar no es el doble de ningún número entero. Esto lo sabemos porque es *la definición* del concepto de número impar. En otras palabras, la afirmación:

si x *es impar, entonces no existe ningún entero* q *tal que* $x=2q$

es cierta porque *nos habíamos puesto de acuerdo* en que la palabra *impar* iba a tener un cierto significado. De alguna manera, la afirmación es cierta "por decreto".

Lo anterior plantea, sin embargo, una dificultad. Así como para dar por verdadero que x no puede escribirse como $2q$ fue innecesario construir una demostración, podríamos decir que la afirmación "el producto de impares es impar" tampoco requiere demostración, que también podemos declararla verdadera por decreto. ¿Para qué esforzarse en construir razonamientos, si cualquier resultado que necesitemos usar podemos simplemente declararlo como cierto? A esta pregunta daremos dos respuestas: por un lado, si bien cada persona es libre de construir su propia teoría, y de aceptar como verdades, sin demostración, el número de afirmaciones que desee, es importante que la teoría sea consistente. Por otra parte, el ejercicio de desarrollar una teoría matemática aceptando como primeras verdades la menor cantidad posible de afirmaciones, con frecuencia nos lleva a una comprensión más plena de cuáles son los aspectos esenciales de la teoría, cuáles son los cimientos que hacen que todo funcione.

Sobre lo primero: podríamos, con la misma facilidad, declarar por decreto que "el producto de impares de ahora en adelante siempre será par". En principio, parece absurdo. ¿Pero por qué no soñar con un mundo donde esto sea cierto?[4] El problema es que el número 1 puede escribirse como 1 por 1, y además el número 1 es impar (es posible demostrar que no puede escribirse como el doble de otro número, usando el orden de los números enteros). Por lo tanto, si el producto de impares fuera siempre par, entonces 1, al ser el producto de los impares 1 y 1, sería par. Esto contradice que 1 no es par (que, como dijimos, se demuestra usando el orden de los enteros). Se concluye que no habrá ningún universo donde los números enteros gocen de esa propiedad, y que, al construir una teoría, la libertad de declarar una afirmación como verdadera no es absoluta: no pueden declararse como verdaderas afirmaciones que lleven a una contradicción con las demás.

Respecto a lo segundo: pareciera que una afirmación como

"$0 \cdot x = 0$ *para todo número real* x"

puede darse por sabida desde siempre, es decir, que podemos aceptarla como verdadera sin tener que dar una justificación. Lo mismo sucede con la afirmación:

"*Si* $w = w + w$ *para algún número* w, *entonces* $w = 0$."

Sin embargo, resulta que ambas pueden deducirse de otras verdades más elementales. Consideremos, por ejemplo, la siguiente demostración de la segunda afirmación:

> *Supongamos que* $w = w + w$ *para algún número real* w.
> *Podemos sumar a cada lado el inverso aditivo de* w. *Obtenemos que:*
>
> $$w + (-w) = (w + w) + (-w).$$
>
> *Por definición de inverso aditivo, el lado izquierdo es cero. El lado derecho, por la asociatividad de la suma, puede escribirse como*
>
> $$w + (w + (-w)),$$
>
> *número que, a su vez, es igual a*

[4] Después de todo, hay contextos, como el de la geometría hiperbólica, donde algo tan disparatado como que "por cualquier punto fuera de una recta dada hay al menos dos paralelas a esa recta" resulta ser verdadero.

$\mathrm{w} + 0$

porque w *sumado a su inverso aditivo es cero (por definición de inverso aditivo).*
Se tiene entonces que

$0 = \mathrm{w} + 0,$

pero el lado derecho es w*, porque el cero es el neutro aditivo. Por lo tanto,*

$0 = \mathrm{w},$

que es lo que queríamos demostrar.

La primera afirmación puede demostrarse del modo siguiente:

Sea x *cualquier número real.*
Sabemos que $0 + 0 = 0$. *Multiplicando a ambos lados por* x *se observa que*

$(0 + 0)\cdot x = 0\cdot x.$

Como el producto se distribuye sobre la suma, se sigue que:

$0\cdot x + 0\cdot x = 0\cdot x.$

Usando la propiedad demostrada anteriormente, con $w = 0\cdot x$*, descubrimos que*

$0\cdot x = 0,$

que es lo que queríamos demostrar.

Que cosas tan básicas como que "cero por cualquier número da cero" no estén entre las verdades más elementales tiene implicaciones muy importantes. De alguna manera, establece que las verdades no son todas iguales, sino que es posible establecer una jerarquía entre ellas. A aquellas que ya no pueden deducirse de otras más elementales los griegos les dieron un estatus especial (y lo seguimos haciendo hasta nuestros días). Consideraron que eran las verdades que con mayor razón merecían ser llamadas verdades. Consideraron que, entre las verdades, ellas tenían más dignidad. Entonces, las llamaron dignidades, que es, *grosso modo*, lo que traduce la palabra griega axioma.

En Matemática y Estadística se hace especial énfasis en reconocer esta jerarquía entre verdades. Desde primer semestre se pone en práctica la habilidad de construir una teoría, mediante demostraciones, tomando como punto de partida solo unos pocas verdades fundantes: los postulados de Euclides en Geometría; verdades sobre la lógica proposicional y la teoría de conjuntos, y axiomas sobre la factorización de números en Álgebra; axiomas sobre las operaciones aritméticas y el orden de números reales en Cálculo.

5. El lenguaje de las conexiones lógicas

Como mencionamos en la sección 3 ("Las conexiones lógicas discursivas"), aunque ellas se expresen usando palabras que muchas veces aparecen también al formular proposiciones condicionales, es útil tomar conciencia de que juegan roles diferentes. Por ejemplo, en nuestra demostración de que el producto de impares es impar, es posible apreciar que las expresiones "entonces", "implica que", "se sigue que", "concluimos que", no fueron usadas para expresar un enunciado condicional, tal como:

Si z es impar, entonces puede escribirse como $z=2r+1$ *para algún entero* r, sino que se usaron de un modo ligeramente distinto. El enunciado condicional es verdadero: es cierto que si un número es impar, entonces puede escribirse como $z=2r+1$. Es cierto que

$$A \rightarrow B$$

donde A representa a la afirmación:

"z es impar"

y B representa a la afirmación:

"z puede escribirse como $z=2r+1$ para algún entero r".

Es una verdad que sabíamos, desde antes, que era cierta (es un teorema obtenido a partir de la definición de número impar y el algoritmo de la división). Pero en la demostración no dijimos que

$$A \rightarrow B.$$

Lo que hicimos fue *aprovechar que ya sabíamos que*

$$A \rightarrow B$$

para concluir que la afirmación B tiene que ser cierta. Lo que hicimos fue *generar una nueva verdad*, la verdad B, a partir de dos cosas que ya sabíamos que eran ciertas:

- por un lado, que $A \rightarrow B$, propiedad que desde antes sabíamos que era cierta gracias a la definición de número impar y el algoritmo de la división;
- por otro lado, la afirmación A, esto es, que "z es impar", la cual ya sabíamos que era cierta porque la estamos tomando como hipótesis (comenzamos la demostración diciendo: "Supongamos que x e y son números impares", y estamos deduciendo algo tanto cuando reemplazamos z por x como cuando reemplazamos z por y.)

En definitiva, detrás de la primera frase de la demostración:

> *Como* x *es impar, entonces puede escribirse como*
>
> $x = 2n + 1,$
>
> *para algún entero* n*,*

lo que tenemos es la siguiente *regla de deducción*:

> si sabemos que la propiedad $A \rightarrow B$ es verdadera y también sabemos que la afirmación A es verdadera, entonces podemos *concluir* que también la afirmación B es verdadera.

Esta regla de deducción forma parte de los recursos con los que funciona nuestra mente para determinar si algo es cierto. Esta regla, que puede representarse mediante el siguiente esquema:

$A \rightarrow B$

A

B

conocida tradicionalmente como *modus ponendo ponens* (y comúnmente abreviada simplemente como *modus ponens*) es parte de la lógica que usamos cotidianamente, y de la cual nos valemos, en particular, en los argumentos matemáticos.

En resumen, uno de los desafíos al estudiar Cálculo, Álgebra o Geometría, y en todos los cursos de Matemática y de Estadística, es aprender a reconocer cuándo las expresiones “implica que”, “se sigue que”, etc., se usan para expresar un *enunciado condicional*, y cuándo se usan como *conexiones lógicas discursivas* para hilar un conjunto de argumentos con una nueva proposición al escribir una demostración.

II. Recomendaciones generales de escritura

Una demostración matemática debe convencer a un público adecuado de que el resultado que se está proponiendo es efectivamente cierto. Por tanto, no consideramos que una demostración esté completa hasta que esté <u>bien escrita</u>. Por eso es importante introducir algunas recomendaciones generales de escritura. Este capítulo presenta nueve orientaciones para hacer demostraciones matemáticas. Cada orientación incluye uno o más ejemplos de ejercicios que podrían aparecerles en una prueba, junto con un análisis de aspectos importantes de considerar a la hora de pensar una estrategia para resolverlos.

1) Decodifica los símbolos matemáticos, el significado de las hipótesis y el significado de la afirmación que se quiere demostrar.

Dedica algunos minutos previos a la escritura a entender el problema, decodificando los conceptos que están involucrados.

Ejemplo 1:

Demuestre que la función $f:[0,\infty)\mapsto\mathbb{R}^2$, $f(x)=x^2$ es inyectiva.

Análisis:

En este caso, decodificar el significado de “función inyectiva” nos dará una pista para comenzar la demostración:

Definición: decimos que una función f *es inyectiva si dado cualquier par de números distintos* x *e* y *en el dominio de la función, sus imágenes* $f(x)$ *y* $f(y)$ *son distintas.*

Esto sugiere que nuestra demostración ha de comenzar de la siguiente manera:

Sean $x,\ y \in [0,\infty),\ x \neq y$

y que el paso siguiente consiste en mostrar que $x^2 \neq y^2$. Como vemos, el solo hecho de tener presente que deben decodificarse los conceptos involucrados, nos muestra el camino para comenzar la demostración. Llegados a este punto, es más fácil que se nos ocurra que podemos continuar separando la demostración en dos casos, uno en que $x < y$, otro en que $x > y$. Una vez se nos ocurre esto, el problema se reduce al ejercicio más asequible de mostrar que, dados dos números positivos, el cuadrado del número menor es más pequeño que el cuadrado del número mayor.

Ejemplo 2:

Demuestre que -(-3)=3.

Análisis:

En este ejemplo, decodifiquemos el significado del signo -

dado cualquier número x *el símbolo* -x *denota al inverso aditivo de* x

y

el "inverso aditivo" de un número x se define como el único número cuya suma con x da cero.

Entonces descubrimos, reemplazando x por el número *-3*, que para resolver el ejercicio *basta* con mostrar que

$$(-3) + 3 = 0.$$

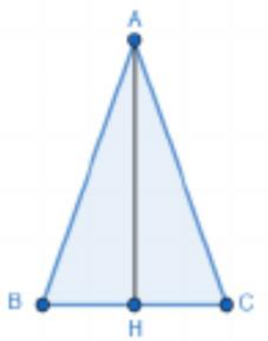
Esto último ya es más fácil reconocer que es una afirmación verdadera (es consecuencia de la definición de *-3*: una vez más, es un ejercicio de decodificación de la notación).

Ejemplo 3:

Demuestre que en un triángulo isósceles, la bisectriz del ángulo opuesto a la base, corta a la base en su punto medio y es perpendicular a ella.

Análisis:

En este ejercicio es importante decodificar tanto las hipótesis como las afirmaciones a las que se quiere llegar como resultado de la demostración. Para darle nombre a los distintos elementos del triángulo isósceles en consideración, conviene dibujar una figura como la siguiente:



En este caso hemos llamado A, B y C a los vértices, y H al punto en que la bisectriz en A corta a la base BC. A continuación, la hipótesis "AH es bisectriz" la decodificamos reescribiéndola como:

$$\angle BAH = \angle CAH$$

y la hipótesis de que el triángulo es isósceles la expresamos ahora usando nuestra notación:

$$AB = AC.$$

Las afirmaciones que se quieren demostrar, a saber, "la bisectriz corta a la base en su punto medio" y "la bisectriz es perpendicular a la base", se convierten (al haber hecho la figura e introducido nuestra notación) en:

$$BH = HC$$

$$\angle BHA = 90º.$$

Este proceso de reescribir las hipótesis y las conclusiones buscadas (usando una notación más concreta) ayuda a "asir mejor" las afirmaciones involucradas y a ver más claramente maneras posibles de conectarlas. En este ejercicio concreto, el anterior proceso de decodificación hace más factible que uno se dé cuenta de que, en virtud del criterio "lado-ángulo-lado", los triángulos BAH y CAH son congruentes. De partida, esto inmediatamente implica que $BH=HC$, que es una de las afirmaciones que queríamos demostrar. Por otra parte, al ver que los triángulos son congruentes, es más fácil observar que, en consecuencia, los ángulos $\angle BHA$ y $\angle BHA$ miden lo mismo. Como sumados forman 180º, cada uno de ellos mide 90º, que es lo que queríamos demostrar.

1.1) Decodificando los cuantificadores existenciales y universales

El principio (1) también es útil de emplear ante la presencia de cuantificadores lógicos.

Ejemplo:

Demuestre que si n y m son números enteros de la misma paridad (ambos pares o ambos impares), entonces n - m es par.

Análisis:

En este ejercicio es preciso decodificar que la conclusión "*n - m* es par" debe ser demostrada para todo par de números enteros *n* y *m* de la misma paridad, no sólo para algunos pares de enteros *n* y *m* que se ofrezcan como ejemplos. Es común encontrar entre los alumnos del primer semestre respuestas como la siguiente:

> *Hay que considerar por separado el caso en que ambos son pares y el caso en que ambos son impares. Para el caso par, sean* n=6 *y* m=4*. Entonces* n - m = 2, *que es par. Para el caso impar, sean* n=9 *y* m=7*. Entonces* n - m = 2 *que es par*[5]*.*

Que este error sea frecuente, muestra que una dificultad no menor del ejercicio consiste en hacer el proceso de decodificación mencionado anteriormente: descubrir que, "entre líneas" en el enunciado, hay un "para todo" (en vez de algo de la forma "Demuestre que existe un par de enteros cuya resta es par".) Una vez se descubre esto, ese descubrimiento da una pista de cómo comenzar la demostración:

> *Sean* n *y* m *dos números enteros cualesquiera con la misma paridad. Consideremos por separado el caso en que ambos son impares y el caso en que ambos son pares*

Llegado a este punto, es más fácil que se nos ocurra que el paso siguiente consiste en decodificar los conceptos de número par y de número impar:

> *Si ambos son pares, entonces existen enteros* j *y* k *tales que*
>
> n=2j *y* m=2k*.*
>
> *En consecuencia,* n - m = 2(j-k)*. Al ser múltiplo de* 2, *se concluye que* n - m *es par.*
>
> *Si ambos son impares, entonces existen enteros* j *y* k *tales que*
>
> n = 2j - 1 *y* m = 2k - 1*.*
>
> *En consecuencia,* n - m = 2(j-k)*. Al ser múltiplo de* 2, *se concluye que* n - m *es par.*
>
> *Habiendo visto todos los casos, se concluye que la diferencia de números enteros de la misma paridad es siempre par, que es lo que queríamos demostrar.*

2) Explicita cuáles son tus hipótesis y qué es lo que quieres demostrar.

Comienza la demostración escribiendo qué estás suponiendo como cierto. Por ejemplo, es muy común que una demostración comience con las palabras "Supongamos que ...", o bien "Sean ... tales que". Esto, por lo general, hace que el problema se reduzca a demostrar una proposición más sencilla que la inicial, como una sucesión de "muñecas rusas" en donde para fabricar una demostración grande hay que pasar por construir sub-demostraciones de resultados más pequeños. Al llegar a estos sub-problemas,

[5] Esta solución presenta el error #2 "Hacer casos especiales y pretender que constituyen una demostración" del documento "Lista de errores comunes".

escribe qué es lo que hay que demostrar una vez hechos esos supuestos. Es importante que la estructura de la demostración sea reconocible, al menos que sea posible distinguir entre lo que son suposiciones, las afirmaciones que hay que demostrar y los resultados intermedios.

Ejemplo:

Demuestre que el cuadrado de todo impar es impar.

Análisis:

En este ejemplo, una manera adecuada de empezar sería la siguiente:

Supongamos que x es un impar cualquiera. Lo que queremos demostrar es que x^2 es impar (...)

3) Antes de usar una variable, o una cierta notación, asegúrate de haberla definido.

En tu demostración, debes dejar claro lo que representan todos los símbolos empleados, tal como se muestra (en azul) en los siguientes ejemplos:

- Ejemplo 1: Demuestre que todo triángulo isósceles tiene dos ángulos iguales.

  Inicio de solución: Sea ABC un triángulo isósceles con $AB=AC$. Sean α, β y γ, respectivamente, los ángulos opuestos a los vértices A, B y C [...]

- Ejemplo 2: Demuestre que todo polinomio de grado impar con coeficientes reales tiene al menos una raíz real.

  Inicio de solución: Dado
  $$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$
  un polinomio cualquiera de grado impar, el teorema fundamental del álgebra nos garantiza que este polinomio tiene n raíces complejas (contando multiplicidades) [...]

- Ejemplo 3: Demuestre que para todo n mayor que 10, $1/3^n$ *es menor que* $1/19$.

  Solución #1: Supongamos que n es un entero mayor que 10. Entonces

$$3^n > 3^{10} > 3^3 = 27 > 19.$$

Por lo tanto, $1/3^n$ es menor que $1/19$, como queríamos demostrar.

Solución #2: Supongamos que n es un entero mayor que 10. Usando la desigualdad de Bernoulli[6], a saber:

$$(1+x)^n \geq 1 + nx \quad \text{para cualquier } x \geq -1.$$

reemplazando x por 2, descubrimos que

$$3^n \geq 1 + 2n > 21 > 19.$$

En consecuencia, $1/3^n < 1/19$, que es lo que queríamos demostrar.

4) Justifica los pasos en la demostración, particularmente los casos especiales a los que el razonamiento general no aplica.

En una demostración, debe ser posible identificar, en cada línea, qué se deduce y por qué esta deducción es lógica. Debemos explicar lo que queremos hacer y justificar cualquier hecho que no sea obvio. Por ejemplo, si queremos dividir el problema en dos casos, debemos declararlo al principio diciendo que: *Consideramos dos casos y demostramos la afirmación en cada caso*. Si invocamos un resultado que se demostró anteriormente en el curso, debemos citar el resultado y verificar explícitamente que se cumplen sus hipótesis. Por ejemplo: *Por teorema 2.3 sabemos que …o por la proposición demostrada en la clase que dice "raíz cuadrado de 2 no es un número racional", podemos concluir que….*

Como pauta general, los argumentos de la demostración deben ser lo suficientemente detallados como para convencer a alguien con la formación de un(a) estudiante del curso en el que estás haciendo la demostración.

Ejemplo:

Sean $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}$. Demuestre que si ab=0 entonces a=0 o bien b=0.

Solución: Sean a,b números reales tal que ab=0. Se quiere probar que $a = 0 \lor b = 0$. Sin pérdida de generalidad, supongamos que $b \neq 0$. Según las propiedades del cuerpo de números reales b posee inverso multiplicativo y multiplicando la ecuación ab=0 por b^{-1}se obtiene:

[6] Esta es una de las maneras de demostrar la propiedad más general: *Dado cualquier número real* z *tal que* $0 < z < 1$, *la cantidad* z^n se hace *arbitrariamente pequeña si* n *se elige lo suficientemente grande.* En este caso, estamos adaptando la demostración al caso particular en que $z = 1/3$. También en el caso general, la conclusión se obtiene al escribir z como $z = 1/(1+x)$ para algún $x > 0$.

$(ab).b^{-1} = 0.b^{-1}$. Por una proposición que demostramos en la clase, $0.b^{-1}$=0. Entonces tenemos $a(b.b^{-1}) = 0$. Por lo tanto $a.1 = 0$. Como 1 es el neutro multiplicativo, se concluye que a=0. □

5) Para establecer que una proposición es falsa, basta encontrar un *contraejemplo*.

Se puede refutar una afirmación encontrando un solo ejemplo en el que las hipótesis se cumplan pero la afirmación falla. A tal ejemplo lo llamaremos *contraejemplo*. Los contraejemplos nos ayudan a entender los límites de la verdad. A veces, encontrar un contraejemplo necesita mucho esfuerzo y creatividad. Sin embargo, como la creación del arte, cuanto más practicas, mejor te vuelves. Puedes empezar preguntándote ¿falta alguna hipótesis para llegar a la conclusión?

Ejemplo:

¿Es verdad que la suma de dos números reales siempre es mayor que ambos números?

Análisis:

La respuesta es no. Para justificar esta respuesta, debemos demostrar que la afirmación "la suma de dos números reales siempre es mayor que ambos números" es falsa. Para justificar esto, basta con presentar un contraejemplo, como el siguiente:

5 y -3 son números reales. Sin embargo, su suma no es mayor que 5.

6) Verifica que usaste todas las hipótesis.

Una vez presentado un razonamiento, es una buena práctica verificar que se han usado todas las hipótesis. Este proceso puede ayudarnos a entender mejor el contenido matemático del análisis expuesto y eventualmente detectar errores.

Ejemplo:

Suponga que $\boldsymbol{x > 11}$. Demuestre que $\boldsymbol{2x > \sqrt{x^2 + 5x + 12}}$.

Análisis:
Una manera de demostrar lo pedido es:

- Primero, observar que las raíces del polinomio $3x^2 - 5x - 12$ son -4/3 y 3.
- A continuación, tomar algún x que satisfaga la hipótesis (algún x mayor que 11):

  Sea x *un número real cualquiera mayor que 11.*
- Observar que aunque no sepamos el valor exacto de x, sí podemos tener certeza de que el número $3x^2 - 5x - 12$ es positivo. Esto podemos deducirlo gracias a la hipótesis $x > 11$, y a la propiedad demostrada en clase:

  Si tanto el discriminante como el coeficiente principal de un polinomio cuadrático son positivos, entonces al evaluar el polinomio en un número x *mayor que las dos raíces se obtiene un valor positivo*
- Deducir que, necesariamente,
$$4x^2 > x^2 + 5x + 12.$$
- Invocar la propiedad demostrada en clase:

  si a *y* b *son positivos y $a^2 > b^2$, entonces $a > b$*

  con
$$a = 2x, \qquad b = \sqrt{x^2 + 5x + 12}.$$
  Para hacer esto es necesario mostrar que b está bien definido[7] y explicitar claramente que la mencionada propiedad puede ser invocada gracias a que tanto $2x$ como $\sqrt{x^2 + 5x + 12}$ son positivos. El número $\sqrt{x^2 + 5x + 12}$ es positivo porque las raíces cuadradas, por definición, siempre son positivas. En cambio, para justificar que $2x$ es negativo, lo que usamos es la hipótesis que nos dieron:

  Como $x > 11$ *(por hipótesis), entonces* $2x > 0$.

En este ejercicio fue fundamental usar la hipótesis $x > 11$. Se usó en dos pasos de la demostración: primero, para concluir que $3x^2 - 5x - 12 > 0$. Segundo, para “tomar la raíz cuadrada a los dos lados” de la desigualdad
$$4x^2 > x^2 + 5x + 12.$$
Sin la hipótesis, ambas afirmaciones podrían haber sido falsas. Por ejemplo, para $x = 0$ no se cumple ninguna de las dos, y para $x = -2$ se cumple la primera pero no la segunda.

7) Indica cuándo se ha completado la demostración.

Aunque pueda parecer repetitivo, es una buena práctica terminar una demostración con una frase que indique con precisión lo que se ha demostrado. Una manera de hacerlo es simplemente escribir: "Esto completa la demostración". También ayuda utilizar algún "símbolo de fin de demostración" como “el punto cuadrado”: □

[7] Esto es, que $x^2+5x+12 > 0$. Esta afirmación, a su vez, hay que justificarla debidamente. Uno de los argumentos posibles es que se trata de una cuadrática con coeficiente principal positivo y discriminante negativo.

8) Revisa que esté claro el orden en que debe leerse la demostración.

El propósito principal de escribir una demostración es comunicar tu razonamiento a un lector o una lectora. Por lo tanto, debes escribir con un orden lineal sensato y evitar a toda costa que tu demostración se transforme en un conjunto de ideas sin contexto conectadas por flechas. En este sentido, las demostraciones en los textos que componen la bibliografía del curso y en clase son buenos modelos para un formato adecuado. Al terminar de escribir tu demostración, es recomendable que la leas imaginando cómo la entendería otra persona. Puedes usar las siguientes preguntas para revisar lo que has escrito:

- ¿Está claro en qué orden debe leerse la demostración?
- ¿Está claro el propósito de cada línea?
- ¿Está claro cuáles afirmaciones son suposiciones del enunciado, cuáles son las que estás a punto de demostrar y cuáles son deducciones?
- ¿La demostración comienza con hechos conocidos y avanza hacia la conclusión deseada?

También es una buena práctica pedirle a otra persona que revise tu demostración, para que te diga qué aspectos necesitan aclaración.

9) En ocasiones es de ayuda destacar las ecuaciones y expresiones matemáticas importantes desplegándolas en un renglón aparte.

Cambiar entre el lenguaje coloquial y el lenguaje simbólico es, de hecho, alternar entre dos lenguajes (como hablar "*spanglish*") y puede dificultar la comprensión. Por lo general es necesario hacerlo, para no ocupar tanto espacio. Pero hay momentos en donde los cálculos son tan importantes que es mejor escribirlos con líneas en blanco antes y después de ellos, aunque la demostración quede más larga. Si el lado izquierdo de las ecuaciones no cambia, no lo repetimos.

Ejemplo:

[...] *Escribimos x=2m+1, y=2n+1 y luego desarrollamos*

$$\begin{aligned} x \cdot y &= (2m+1)(2n+1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1. \end{aligned}$$

Dado que m y n son enteros, concluimos que....

Referencias

- Sundstrom, Ted (2021). *Mathematical Reasoning: Writing and Proof*. Version 2.1 https://scholarworks.gvsu.edu/books/9/, visto el 26/11/2021.
- Wilson, Jenny (s/a). *A Primer on Mathematical Proof*. http://www.math.lsa.umich.edu/~jchw/PrimerOnProof.pdf, visto el 4/01/2022.