

# Preámbulo

“Desconfíen vuestras mercedes de quien es lector de un solo libro”, dijo el Capitán Alatriste.

---

Arturo Pérez-Reverte  
*Limpieza de Sangre*, 1997

I prioritise story over science, but not at the expense of being really stupid about it.

---

Alastair Reynolds

Este capítulo contiene material necesario para el resto del texto y debe ser abordado a medida que se necesite. El material en esta sección incluye convenciones y definiciones básicas, y además hace un recuento sucinto sobre la inducción matemática y los sistemas formales.

## 0.1. Preludio

Las matemáticas, y en particular la lógica, se desarrollan usando un código común de términos y una metodología. La *terminología* se refiere a aspectos lingüísticos que se supone son conocidos y están claramente entendidos. Es en este sentido en el cual los textos de matemáticas adoptan algunos términos como “definición”, “proposición” y “teorema”, entre otros, y los usan frecuentemente. La *metodología* permite abordar el estudio de un tema de manera sistemática: primero, definiendo únicamente el objeto de estudio; segundo, estableciendo propiedades sobre el objeto de estudio; tercero, y de manera opcional, utilizando efectivamente el objeto de estudio para resolver un problema de interés. Por objeto de estudio puede entenderse, por ejemplo, “cómo demostrar que un algoritmo es correcto”, “un sistema numérico” o “una teoría de la relatividad”. Esta sección explica cuáles son el código común de términos y la metodología que sigue este texto.

Siempre, en matemáticas, lo más importante son las definiciones: sin definiciones, o sin entenderlas, no es posible hacer matemáticas; mucho menos pretender que sean de

alguna utilidad. El objetivo de una *definición* es “definir” únicamente un objeto matemático y establecer notación para referirse a este. Una definición en este texto hace eso: definir objetos matemáticos y establecer notación para referirse a ellos.

### Definición 0.1

El *conjunto de números naturales* es  $\{0, 1, 2, \dots\}$  y se denota como  $\mathbb{N}$ . Un número  $n$  es un *número natural* si y solo si  $n \in \mathbb{N}$ .

Primero que todo, note que las definiciones vienen identificadas con un código. Así no es necesario referirse a ellas como en “la definición anterior” (puede haber más de una definición antes del texto que la referencia y entonces esta indicación sería ambigua), sino más bien referenciándola directamente como en “la Definición 0.1”. En este último caso la palabra “definición” es un nombre propio y por eso su inicial se escribe en mayúscula.

Los tipos de letra son claves para entender una definición. Por ejemplo, en la Definición 0.1 hay dos tipos de letra. Los sustantivos “conjunto de números naturales” y “número natural” están en letra cursiva, lo cual no es un capricho: estos dos son los nombres de los objetos que están siendo definidos. Esto quiere decir, por ejemplo, que en este texto los números naturales son esos y no otros. Como convención se adopta el símbolo  $\mathbb{N}$  para representar el conjunto de números naturales. En la segunda parte de la Definición 0.1 la expresión “ $n$ ” es una *variable matemática* y por eso también aparece en letra cursiva.

En algunas ocasiones se hacen suposiciones de notación y convención. Por ejemplo, en la Definición 0.1 el autor supone conocimiento del lector acerca de qué es un número, de preferir la notación arábica sobre la romana para escribirlos y de entender el significado del símbolo ‘ $\in$ ’. Es posible tratar de definir todas estas suposiciones formalmente; sin embargo, sería impráctico en el caso de este texto porque desviaría al lector de su objetivo principal.

Una vez un objeto está (únivamente) definido, es posible entonces proceder a identificar y estudiar sus propiedades. Es en este momento, al haber definido el objeto de interés, que se pueden postular y demostrar propiedades acerca del objeto de estudio de manera precisa.

### Teorema 0.2

Sea  $n$  un número. Si  $n \in \mathbb{N}$ , entonces  $(n + 1) \in \mathbb{N}$ .

El Teorema 0.2 (*¡si!, también tiene nombre!*) establece una propiedad inductiva de los números naturales que por lo pronto sirve únicamente de ejemplo. La propiedad enunciada en el Teorema 0.2 indica que el *sucesor* (i.e., el siguiente) de cualquier número natural es un número natural. Claramente, esto debe estar acompañado de una demostración rigurosa. En este texto las demostraciones se presentan en un párrafo que inicia con el sustitutivo “Demostración” en letra negrilla y termina con un cuadro vacío indicando el fin de la demostración, de la siguiente forma:

**Demostración.** ...

□

A diferencia de otras áreas de las matemáticas como el cálculo, el álgebra, etc., el estudio de la lógica se ocupa *simultáneamente* de dos roles de la lógica: como *objeto* de estudio y como *herramienta* para razonar. En este texto se estudian diferentes lógicas y cada una de ellas se define como un *sistema formal* (Sección 0.3). Entonces, dependiendo del ámbito, el tipo de propiedades que se pueden establecer son dos: (i) propiedades *acerca* del sistema formal y (ii) propiedades *dentro* del sistema formal. En el caso (i) la lógica, como sistema formal, es un objeto de estudio y las propiedades demostradas son *meta-teoremas* (i.e., propiedades de la lógica como tal). En el caso (ii) la lógica, como herramienta, está siendo empleada para obtener resultados dentro del sistema formal y las propiedades demostradas son *teoremas* (i.e., propiedades particulares de las expresiones de la lógica). La convención que sigue el texto es clasificar con el nombre de *Metateorema* a cada meta-teorema y con el nombre de *Teorema* a cada teorema. El texto también usa los nombres *Lema* y *Corolario* para referirse a meta-teoremas y teoremas ‘secundarios’: un lema es un resultado intermedio que antecede a un resultado importante, mientras que un corolario es un caso particular de un (meta-)teorema. La intención de usar estos términos para referirse a resultados, tanto al nivel meta-teórico como del objeto de estudio, es facilitar la lectura del texto; dependiendo del contexto en el cual aparezcan, el lector podrá inferir en cuál de los dos roles se enuncian dichos resultados.

Finalmente, el texto hace uso de “notas” para resaltar una idea, introducir notación o simplemente llamar la atención del lector a aspectos que complementan el contenido primordial del texto.

#### Nota 0.3

Para estudiar lógica es necesario entender muy bien las definiciones y hacer demostraciones.

### Ejercicios

1. Investigue y enuncie las convenciones notacionales para identificar cada uno de los siguientes conjuntos, explicando la relación que hay entre cada uno de ellos:
  - a) Números enteros.
  - b) Números racionales.
  - c) Números reales.
  - d) Números complejos.
2. Investigue y enuncie la definición para cada uno de los siguientes objetos matemáticos:
  - a) Número algebraico.
  - b) Número irracional.
  - c) Número trascendental.
3. Investigue y enuncie la definición para cada uno de los siguientes objetos matemáticos:
  - a) Conjunto.
  - b) Conjunto finito.
  - c) Conjunto infinito.

4. Investigue y enuncie la definición para cada uno de los siguientes objetos matemáticos:
  - a) Función parcial.
  - b) Función total.
  - c) Función inyectiva.
  - d) Función sobreyectiva.
  - e) Función biyectiva.
5. Investigue y enuncie la definición para cada uno de los siguientes objetos matemáticos:
  - a) Relación binaria.
  - b) Relación binaria reflexiva.
  - c) Relación binaria irreflexiva.
  - d) Relación binaria simétrica.
  - e) Relación binaria antisimétrica.
  - f) Relación binaria asimétrica.
  - g) Relación binaria transitiva.
6. Investigue y enuncie la definición para cada uno de los siguientes objetos matemáticos:
  - a) Monoide algebraico.
  - b) Grupo algebraico.
  - c) Retículo algebraico.
  - d) Espacio métrico.
  - e) Espacio topológico.
7. Investigue y enuncie los siguientes teoremas (sin demostración):
  - a) Teorema fundamental de la aritmética.
  - b) Teorema fundamental del álgebra.
  - c) Teorema fundamental del cálculo.
8. Para cada una de las siguientes abreviaciones, investigue su origen en latín, su significado en castellano y formule un ejemplo de su uso:
  - a) e.g.
  - b) et al.
  - c) etc.
  - d) i.e.
  - e) ibid.
  - f) Ph.D.
  - g) Q.E.D.
  - h) v.gr.
  - i) viz.
  - j) vs.
9. Para cada una de las siguientes expresiones en latín, investigue su significado en castellano y explique cómo puede ser usada en matemáticas:
  - a) *a fortiori*.
  - b) *a priori*.
  - c) *ad absurdum*.
  - d) *ad infinitum*.
10. Investigue acerca del origen en griego antiguo de la palabra “lema” y su significado en castellano. Además, enuncie tres lemas importantes de las matemáticas.

11. Investigue acerca del origen en griego antiguo de la palabra “corolario” y su significado en castellano. Además, enuncie un corolario importante de las matemáticas.
- 

## 0.2. Inducción

Hay una anécdota acerca del matemático alemán Carl Friedrich Gauss quien, a los 8 años de edad, no prestaba mucha atención en clase. A modo de castigo, una vez su profesor de matemáticas le pidió sumar los números naturales de 0 a 100. La leyenda dice que Gauss respondió correctamente 5050 después de un par de segundos de formulada la pregunta; esto enfureció al profesor. ¿Cómo pudo el “pequeño” Gauss hacer el cálculo con tanta rapidez? Posiblemente Gauss sabía que la *ecuación de los números triangulares*

$$0 + 1 + 2 + 3 + 4 + \dots + n = \frac{n \cdot (n + 1)}{2}$$

es cierta para todo número natural  $n$ . Entonces, al tomar  $n = 100$ , Gauss pudo calcular fácilmente la cantidad consultada por el profesor de la siguiente manera:

$$0 + 1 + 2 + 3 + 4 + \dots + 100 = \frac{100 \cdot 101}{2} = 5050.$$

Sin embargo, para que un cálculo como el anterior sea siempre correcto es necesario demostrar que la ecuación es cierta para todos los valores de  $n$  (algo que posiblemente Gauss ya había hecho). Tenga presente, en general, que si una ecuación es cierta para algunos valores de  $n$ , esto no la hace correcta para todos los valores de  $n$ : en matemáticas no es posible demostrar una afirmación con base en ejemplos. Aún más, en el caso de los números naturales, es imposible pretender demostrar uno a uno una propiedad para todos ellos porque hay una cantidad infinita de números naturales.

El principio de inducción matemática (finita) es una herramienta fundamental para obtener resultados en matemáticas, incluyendo la lógica. Este principio permite, por ejemplo, establecer la veracidad de la ecuación de los números triangulares para cualquier valor de  $n \in \mathbb{N}$ , a pesar de que el conjunto de los números naturales es enorme. De manera general, el principio de inducción matemática permite demostrar que *cualquier* número natural (o una gran cantidad de ellos) tiene una propiedad dada.

### Nota 0.4

Se escribe  $M(k)$  para indicar que  $k \in \mathbb{N}$  tiene la propiedad  $M$ . Por ejemplo,  $M(5)$  indica que 5 tiene la propiedad  $M$ .

### Metateorema 0.5

Considere una propiedad  $M$  sobre los números naturales y los siguientes dos casos:

1. **Caso base:** el número natural 0 satisface la propiedad  $M$ , (i.e., hay una demostración de  $M(0)$ ).
2. **Caso inductivo:** si  $n$  es un número natural para el cual *se supone*  $M$ , entonces *se puede demostrar* que  $n + 1$  tiene la propiedad  $M$  (i.e., se tiene una demostración de que  $M(n)$  implica  $M(n + 1)$ ).

El *principio de inducción matemática* indica que si las condiciones (1) y (2) son ciertas, entonces todo  $n \in \mathbb{N}$  tiene la propiedad  $M$ .

El principio de inducción es una propiedad inherente de los números naturales. Ahora bien, ¿por qué tiene sentido el principio de inducción? Antes de presentar una demostración, considere la siguiente reflexión. Suponga que las condiciones (1) y (2) son ciertas para una propiedad  $M$  sobre los números naturales, y sea  $k$  un número natural (i.e.,  $k \in \mathbb{N}$ ). Si  $k = 0$ , entonces  $k$  tiene la propiedad  $M$  por el caso base (i.e.,  $M(0)$  es cierto). De lo contrario, se puede usar el caso inductivo aplicado a  $n = 0$ , para concluir que  $1 = 1 + 0$  tiene la propiedad  $M$  (i.e.,  $M(1)$  es cierto). El caso inductivo se puede aplicar de la misma forma con  $n = 1$  suponiendo  $M(1)$  y entonces concluyendo  $M(2)$ . Este proceso se puede repetir hasta concluir  $M(k)$ : es como un “efecto dominó” en donde  $k$  es “la primera ficha en caer” o “alguna otra ficha que cae” porque está conectada causalmente con la primera ficha en caer.

A continuación se presenta una demostración del principio de inducción matemática.

**Demostración.** Suponga que las condiciones (1) y (2) son ciertas para  $M$ . Sin embargo, para llegar a una contradicción, suponga que  $M$  no es cierta para todos los  $n \in \mathbb{N}$ . Es decir, hay un  $k \in \mathbb{N}$  que no tiene la propiedad  $M$ . Sin pérdida de generalidad suponga que dicho  $k$  es el más pequeño (i.e., el mínimo) entre todos los números en  $\mathbb{N}$  que no tienen la propiedad  $M$ . Hay dos casos:  $k = 0$  o  $k > 0$ . Pero  $k$  no puede ser 0 porque, por la Condición (1), 0 cumple la propiedad  $M$ . Luego, debe ser  $k > 0$ . Con  $k > 0$ , se tiene que  $k - 1 \in \mathbb{N}$ . Además, como  $k$  es el número natural más pequeño que no tiene la propiedad  $M$ , se sabe que  $k - 1$  tiene la propiedad  $M$ . Dado que  $k - 1$  tiene la propiedad  $M$  se concluye, por la Condición (2), que  $k$  tiene la propiedad  $M$ . Sin embargo, esto contradice el hecho de que  $k$  no tiene la propiedad  $M$ . En conclusión, si las condiciones (1) y (2) son ciertas para  $M$ , necesariamente todos los números naturales tienen la propiedad  $M$ .  $\square$

#### Nota 0.6

La suposición  $M(n)$  que se hace en el caso inductivo del Metateorema 0.5 es denominada *hipótesis inductiva*.

**Ejemplo 0.1**

La ecuación de los números triangulares es cierta para todo número natural  $n$ . Es decir,

$$0 + 1 + 2 + 3 + 4 + \cdots + n = \frac{n \cdot (n + 1)}{2}$$

para  $n \in \mathbb{N}$ .

**Demostración.** Primero que todo, se identifica claramente la propiedad que se quiere demostrar. Sea  $G(n)$  una abreviación para la ecuación  $0 + 1 + 2 + 3 + 4 + \cdots + n = \frac{n \cdot (n + 1)}{2}$ , lo cual se escribe así:

$$G(n) : 0 + 1 + 2 + 3 + 4 + \cdots + n = \frac{n \cdot (n + 1)}{2}.$$

Note que  $n$  es el parámetro de  $G$  así como  $n$  es el parámetro en la ecuación de los números triangulares. El objetivo es demostrar  $G(n)$  para  $n \in \mathbb{N}$ . Por el principio de inducción matemática (Metateorema 0.5) basta con demostrar las condiciones (1) y (2) para  $G$ .

**Caso base:** se quiere demostrar que 0 tiene la propiedad  $G$ . Note que  $G(0)$  abrevia la ecuación  $0 = \frac{0 \cdot (0 + 1)}{2}$ , que es directamente una identidad. Entonces 0 tiene la propiedad  $G$ , i.e.,  $G(0)$ .

**Caso inductivo:** se quiere demostrar que si  $n$  tiene la propiedad  $G$ , entonces  $(n + 1)$  tiene la propiedad  $G(n + 1)$  (i.e.,  $G(n)$  implica  $G(n + 1)$ ). Se supone como hipótesis inductiva  $G(n)$  (i.e., que  $n \geq 1$  tiene la propiedad  $G$ ) y con esta información se busca una demostración de  $G(n + 1)$ . La expresión  $G(n + 1)$  abrevia la ecuación

$$0 + \cdots + n + (n + 1) = \frac{(n + 1) \cdot ((n + 1) + 1)}{2}.$$

Por la hipótesis inductiva (i.e., suponiendo  $G(n)$ ), la parte izquierda de la igualdad se puede escribir como  $\frac{n \cdot (n + 1)}{2} + (n + 1)$ . Factorizando  $(n + 1)$ , esta expresión es igual a  $\frac{(n + 1)(n + 2)}{2}$ , que a su vez es igual a  $\frac{(n + 1) \cdot ((n + 1) + 1)}{2}$ . Entonces, si  $n$  tiene la propiedad  $G$ , necesariamente  $(n + 1)$  tiene la propiedad  $G$ . Es decir,  $G(n)$  implica  $G(n + 1)$ .

Dado que los casos (1) y (2) son ciertos para  $G$ , por el principio de inducción matemática (Metateorema 0.5), se sigue que todo  $n \in \mathbb{N}$  tiene la propiedad  $G$ .  $\square$

El principio de inducción matemática tiene muchas variantes. Por ejemplo, es posible contar con una versión en la cual el caso base no sea necesariamente  $n = 0$  (Ejercicio 0.2.3). A continuación se presenta un ejemplo del uso de la inducción matemática para demostrar una desigualdad cuyo caso base es  $n = 1$ .

**Ejemplo 0.2**

La siguiente desigualdad es cierta para todos los números naturales  $n \geq 1$ :

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n} < 1.$$

**Demostración.** Inicialmente se identifica la propiedad que se desea demostrar. Sea  $H(n)$  una abreviación para la desigualdad  $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n} < 1$ , es decir,

$$H(n) : \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n} < 1.$$

Por el principio de inducción matemática (Metateorema 0.5) basta con demostrar las condiciones (1) y (2) para  $H$ .

**Caso base:** se quiere demostrar que 1 tiene la propiedad  $H$ , es decir,  $H(1)$ . En este caso,  $H(1)$  abrevia la propiedad  $\frac{1}{2} < 1$ , la cual es verdadera. Luego, 1 tiene la propiedad  $H$ .

**Caso inductivo:** se quiere demostrar que  $n+1$  tiene la propiedad  $H$  si  $n$  tiene la propiedad  $H$  (i.e.,  $H(n+1)$  es consecuencia de  $H(n)$ ). Entonces se supone  $H(n)$  como hipótesis inductiva y se procede a buscar una demostración para  $H(n+1)$ . La expresión  $H(n+1)$  abrevia la desigualdad

$$H(n+1) : \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots + \frac{1}{2^n} + \frac{1}{2^{n+1}} < 1.$$

Al suponer la hipótesis inductiva  $H(n)$  se tiene que la desigualdad

$$\frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots + \frac{1}{2^{n+1}} < \frac{1}{2}$$

es cierta porque resulta de multiplicar por  $\frac{1}{2}$  cada uno de los dos lados de la desigualdad en  $H(n)$ . Ahora, sumando  $\frac{1}{2}$  a cada uno de los dos lados de esta última desigualdad, se obtiene

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \dots + \frac{1}{2^{n+1}} < \frac{1}{2} + \frac{1}{2} = 1.$$

Es decir,  $H(n+1)$ . En conclusión, si  $n$  tiene la propiedad  $H$ , entonces  $n+1$  también tiene la propiedad  $H$ .

Dado que las condiciones (1) y (2) son ciertas para  $H$ , por el principio de inducción matemática (Metateorema 0.5), se sigue que todo  $n \in \mathbb{N}$  con  $n \geq 1$  tiene la propiedad  $H$ .  $\square$

Como se verá en algunas secciones de este texto, el principio de inducción matemática se puede adaptar para hacer demostraciones sobre estructuras diferentes a los números naturales como, por ejemplo, fórmulas y demostraciones en un sistema formal. En cada variante del principio de inducción matemática que se use, lo más importante es identificar las condiciones base (pueden ser más de uno) y los casos inductivos (los cuales también pueden ser más de uno). En la práctica, en muchas ocasiones, es posible y natural reducir un principio de inducción matemática al principio de inducción matemática para números naturales estudiado en esta sección. Esto hace del principio de inducción matemática para números naturales una herramienta efectiva en las matemáticas.

En algunas ocasiones hay más de una posibilidad en el enunciado de un problema para decidir cómo hacer inducción. Se presenta a continuación un ejemplo que ilustra cómo escribir claramente la propiedad que se desea demostrar facilita el uso del principio de inducción matemática.

**Ejemplo 0.3**

La siguiente ecuación es cierta para todos los números naturales  $n$  y  $r$ , con  $r \neq 1$ :

$$r^0 + r^1 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

**Demostración.** Considere la propiedad  $I$  sobre los números naturales definida por

$$I(n) : r^0 + r^1 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

El objetivo es demostrar  $I(n)$  para  $n \in \mathbb{N}$ .

**Caso base:** Se quiere demostrar  $I(0)$ , que abrevia  $r^0 = \frac{1-r^{0+1}}{1-r}$ . Por un lado,  $r^0 = 1$ . Por el otro y como  $r \neq 0$ , se tiene que  $\frac{1-r^{0+1}}{1-r} = 1$ . Es decir, 0 tiene la propiedad  $I$ .

**Caso inductivo:** Se usa como hipótesis inductiva  $I(n)$  y se demuestra  $I(n + 1)$ . Es decir, el objetivo es demostrar

$$r^0 + r^1 + \cdots + r^n + r^{n+1} = \frac{1 - r^{n+2}}{1 - r}.$$

Considere el siguiente cálculo, en el cual se supone  $r \neq 1$ :

$$\begin{aligned} r^0 + r^1 + \cdots + r^n + r^{n+1} &= \frac{1 - r^{n+1}}{1 - r} + r^{n+1} && \text{(por la hipótesis inductiva)} \\ &= \frac{1 - r^{n+1}}{1 - r} + \frac{(1 - r) \cdot r^{n+1}}{1 - r} && \text{(aritmética)} \\ &= \frac{1 - r^{n+1} + r^{n+1} - r \cdot r^{n+1}}{1 - r} && \text{(aritmética)} \\ &= \frac{1 - r^{n+2}}{1 - r} && \text{(aritmética).} \end{aligned}$$

Es decir, al suponer  $I(n)$  se puede demostrar  $I(n + 1)$ .

Por el principio de inducción matemática (Metateorema 0.5) se obtiene que todo  $n \in \mathbb{N}$  tiene la propiedad  $I$ .  $\square$

El Ejemplo 0.3 presenta un caso particular de una propiedad de la *serie geométrica* (ver Ejercicio 0.2.13). Este ejemplo, además de ilustrar el uso del principio de inducción matemática, es interesante porque hay dos variables involucradas en el enunciado del problema, es decir,  $n$  y  $r$ . En la demostración incluida como parte de este ejemplo se optó por hacer inducción sobre  $n$  y no sobre  $r$  (note que la propiedad  $I$  es definida con parámetro  $n$ ). Como la única suposición que se hace sobre  $r$  es que no puede ser 1, entonces la demostración en el Ejemplo 0.3 justifica que la propiedad dada es cierta para cualesquiera números naturales  $n$  y  $r$  siempre y cuando  $r \neq 1$ . Es más, como la única condición sobre  $r$  es esa, esta propiedad es cierta para  $r$  siendo, por ejemplo, un número real.

Antes de finalizar la sección se presenta un ejemplo clásico sobre el uso del principio de inducción matemática para establecer propiedades de los números de Fibonacci.

**Ejemplo 0.4**

Los *números de Fibonacci* se definen para todo  $n \in \mathbb{N}$  por:

$$F(0) = 0$$

$$F(1) = 1$$

$$F(n+2) = F(n) + F(n+1) \quad , \text{para } n \geq 0.$$

Demuestre que la siguiente ecuación es cierta para todo  $n \in \mathbb{N}$ :

$$F(0) + F(1) + \cdots + F(n) = F(n+2) - 1.$$

**Demostración.** El objetivo es demostrar, para cualquier  $n \in \mathbb{N}$ , la propiedad  $J(n)$ :

$$J(n) : F(0) + F(1) + \cdots + F(n) = F(n+2) - 1.$$

**Casos base:** para demostrar  $J(0)$  (i.e.,  $F(0) = F(2) - 1$ ), considere el siguiente cálculo:

$$\begin{aligned} F(0) &= 0 && (\text{definición de } F \text{ para } n = 0) \\ &= 1 - 1 && (\text{aritmética}) \\ &= F(0) + F(1) - 1 && (\text{definición de } F \text{ para } n = 0, 1) \\ &= F(2) - 1 && (\text{definición de } F \text{ para } n = 2). \end{aligned}$$

La demostración de  $J(1)$  se propone como ejercicio para el lector.

**Caso inductivo:** se supone  $J(n)$  y se demuestra  $J(n+1)$ :

$$\begin{aligned} F(0) + F(1) + \cdots + F(n) + F(n+1) &= (F(n+2) - 1) + F(n+1) && (\text{por la hipótesis inductiva}) \\ &= (F(n+1) + F(n+2)) - 1 && (\text{aritmética}) \\ &= F(n+3) - 1 && (\text{definición de } F \text{ para } n \geq 0). \end{aligned}$$

Por el principio de inducción matemática (Metateorema 0.5) se obtiene que todo  $n \in \mathbb{N}$  tiene la propiedad  $J$ .  $\square$

Note que la demostración en el Ejemplo 0.4 consta de dos casos base. Esto se debe a que la definición de la función  $F$  indica, en el caso general, que el valor  $F(n)$  corresponde a la suma de los *dos* valores inmediatamente anteriores. Por esa misma razón, se plantean dos casos base para la definición de  $F$ , más precisamente,  $F(0)$  y  $F(1)$ .

**Ejercicios**

1. Investigue sobre Carl Friedrich Gauss y describa sus principales aportes a las matemáticas.
2. Investigue y explique por medio de dibujos por qué la ecuación usada por el “pequeño” Gauss, enunciada al inicio de esta sección, recibe el nombre de ecuación de los números triangulares.

3. Considere una propiedad  $M$  sobre los números naturales y un número  $m \in \mathbb{N}$ . Además, considere las siguientes dos condiciones:

- (1) El número  $m$  tiene la propiedad  $M$  (i.e.,  $M(m)$ ).
- (2) Si el número natural  $n \geq m$  tiene la propiedad  $M$ , entonces  $m+1$  tiene la propiedad  $M$  (i.e.,  $M(n)$  implica  $M(n+1)$ ).

Demuestre que si las condiciones (1) y (2) son ciertas, entonces todo número natural  $n \geq m$  tiene la propiedad  $M$ .

4. Use el principio de inducción matemática, indicando cada uno de los casos y el uso de la hipótesis inductiva, para demostrar

$$A(n) : (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + \cdots + (2 \cdot n - 1) = n^2$$

para todo  $n \in \mathbb{N}$  con  $n \geq 1$ .

5. Explique por medio de dibujos por qué la ecuación del Ejercicio 4 es conocida como la ecuación de los números cuadrados.

6. Use el principio de inducción matemática, indicando cada uno de los casos y el uso de la hipótesis inductiva, para demostrar

$$B(n) : 0^2 + 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n \cdot (n+1) \cdot (2 \cdot n + 1)}{6}$$

para todo  $n \in \mathbb{N}$ .

7. Use el principio de inducción matemática para demostrar

$$C(n) : 8 + 13 + 18 + 23 + \cdots + (3 + 5n) = \frac{5n^2 + 11n}{2}$$

para todo  $n \in \mathbb{N}$  con  $n \geq 1$ . ¿Qué sucede cuando  $n = 0$ ?

8. Demuestre que  $2^n \geq n + 12$  para todo número natural  $n \geq 4$ . En este problema el caso base es  $n = 4$ . ¿Es cierta esta propiedad para  $n < 4$ ? Justifique su respuesta.

9. Use el principio de inducción matemática para demostrar

$$D(n) : (1 + 2 + \cdots + n)^2 = 1^3 + 2^3 + \cdots + n^3.$$

10. Use el principio de inducción matemática para demostrar

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

11. Use el principio de inducción matemática para demostrar

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}.$$

12. Use el principio de inducción matemática para demostrar

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

13. Use el principio de inducción matemática para demostrar la siguiente propiedad de la *serie geométrica*:

$$ar^0 + ar^1 + \cdots + ar^n = \frac{a(1 - r^{n+1})}{1 - r}$$

para todo  $a, n, r \in \mathbb{N}$  con  $r \neq 1$ .

14. Complete el Ejemplo 0.4 con la demostración del segundo caso base.

15. Investigue y explique el significado asociado a la secuencia  $F(0), F(1), \dots$  por Fibonacci en el libro Liber Abaci (1202).
16. Demuestre que la función  $F$  de Fibonacci satisface las siguientes igualdades:
- $F(1) + F(3) + \dots + F(2(n-1)+1) = F(2n)$ , para  $n \geq 1$ .
  - $F(0) + F(2) + \dots + F(2n) = F(2n+1) - 1$ , para  $n \geq 0$ .

17. Demuestre que la función  $F$  de Fibonacci satisface, para  $n \in \mathbb{N}$ , la siguiente igualdad:

$$F(0)^2 + F(1)^2 + \dots + F(n)^2 = F(n)F(n+1).$$

18. Demuestre que la función  $F$  de Fibonacci satisface, para  $n \in \mathbb{N}$ , la siguiente igualdad:

$$F(n)^2 - F(n+1)F(n-1) = (-1)^{n+1}.$$

19. El producto entre dos matrices de dimensión  $2 \times 2$  se define como:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \times \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} + a_{01}b_{10} & a_{00}b_{01} + a_{01}b_{11} \\ a_{10}b_{00} + a_{11}b_{10} & a_{10}b_{01} + a_{11}b_{11} \end{pmatrix}.$$

Dada una matriz  $A$  de  $2 \times 2$ , se define  $A^n$  para  $n \geq 1$  de la siguiente manera:

$$A^1 = A$$

$$A^{n+1} = A \times A^{n-1}, \quad n \geq 2.$$

Usando el principio de inducción matemática demuestre, para  $n \geq 1$ , la siguiente igualdad relacionada con la función  $F$  de Fibonacci:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F(n+1) & F(n) \\ F(n) & F(n-1) \end{pmatrix}.$$

20. Demuestre que la función  $F$  de Fibonacci, para  $n \geq 1$ , satisface

$$F(n) \geq \left(\frac{3}{2}\right)^{n-2}.$$

21. Considere la función *factorial* definida de la siguiente manera para cualquier  $n \in \mathbb{N}$ :

$$0! = 1,$$

$$n! = n \cdot (n-1)! \quad , \text{ si } n > 0.$$

Proponga un caso base  $m \in \mathbb{N}$  y demuestre por el principio de inducción matemática la desigualdad

$$2^n < n! \quad , \text{ para } n \geq m.$$

¿Cuál es el mínimo  $m$  que satisface esta desigualdad?

22. El coeficiente binomial  $\binom{n}{k}$  se define para  $0 \leq k \leq n$  de la siguiente manera:

$$\binom{n}{0} = 1$$

$$\binom{n}{n} = 1$$

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \quad , \text{ para } 1 \leq k \leq n.$$

Demuestre para  $n$  y  $k$  números naturales:

- $\binom{n}{k} = \binom{n}{n-k}$ , con  $0 \leq k \leq n$ .

- b)  $\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$ , con  $1 \leq k \leq n$ .
23. Demuestre para  $n, k \in \mathbb{N}$  con  $0 \leq k \leq n$ :
- $$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$
24. Demuestre para  $n \in \mathbb{N}$ :
- $$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$
25. Demuestre para  $n \in \mathbb{N}$ :
- $$0\binom{n}{0} + 1\binom{n}{1} + \cdots + n\binom{n}{n} = n2^{n-1}.$$
26. Demuestre para  $n \in \mathbb{N}$ :
- $$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$
27. Sean  $n, x \in \mathbb{N}$ . Demuestre que si  $1 + x > 0$  y  $n \geq 1$ , entonces  $(1 + x)^n \geq 1 + nx$ .
28. Sea  $h(n) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ . Demuestre, para todo  $n \geq 1$  que
- $$h(1) + h(2) + h(3) + \cdots + h(n) = (n+1) \cdot h(n) - n.$$
29. Sea  $f$  una función definida para todo  $n \in \mathbb{N}$  por:
- $$\begin{aligned} f(0) &= 0, \\ f(1) &= 1, \\ f(n) &= f(f(n-1)) + f(n-f(n-1)) \quad , \text{ si } n > 1. \end{aligned}$$
- Calcule  $f(10000)$ .
30. Proponga una fórmula para calcular la siguiente suma y demuestre que dicha fórmula es correcta:
- $$0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1).$$
31. Sean  $k$  y  $l$  números naturales. Se dice que  $k$  es *divisible* por  $l$  si y solo si existe un  $p \in \mathbb{N}$  tal que  $k = p \cdot l$  (en este caso,  $p$  se llama el *testigo* de la divisibilidad de  $k$  entre  $l$ ). Por ejemplo, 15 es divisible por 3 con testigo 5 porque  $15 = 5 \cdot 3$ . Use el principio de inducción matemática para demostrar que  $11^n - 4^n$  es divisible por 7 para todo  $n \in \mathbb{N}$ .
32. Demuestre que  $x^n - 1$  es divisible por  $x - 1$  para todos  $n, x \in \mathbb{N}$ .
33. Demuestre que las siguientes afirmaciones son ciertas para cualquier  $n \in \mathbb{N}$ :
- $n^3 - n$  es divisible por 3.
  - $n^5 - n$  es divisible por 5.
34. Demuestre o refute:  $n^4 - n$  es divisible por 4, para todo  $n \in \mathbb{N}$ .
35. Demuestre usando el principio de inducción matemática que un número natural en representación decimal es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.
36. Demuestre usando el principio de inducción matemática que:
- El cuadrado de un número natural impar es de la forma  $8m+1$ , para algún  $m \in \mathbb{N}$ .
  - La cuarta potencia de un número natural impar es de la forma  $16m+1$ , para algún  $m \in \mathbb{N}$ .

37. Suponga que una oficina postal vende estampillas de \$2 y \$3. Demuestre que cualquier cantidad de dinero  $n \geq \$2$  puede ser pagada con estampillas de estas denominaciones. Ayuda: use inducción matemática sobre  $n$ . En el caso inductivo considere dos posibilidades: primero, que  $n$  puede pagarse usando únicamente estampillas de \$2; segundo, que  $n$  puede pagarse usando al menos una estampilla de \$3.
38. Demuestre que dada una cantidad ilimitada de monedas de \$6, \$10 y \$15, se puede obtener cualquier suma de dinero mayor que \$29.
39. Este ejercicio ilustra por qué el caso base es importante en el principio de inducción matemática. Considere la siguiente afirmación:
- ‘El número  $n^2 + 5n + 1$  es par para todo  $n \in \mathbb{N}$ .’
- Demuestre el caso inductivo para esta afirmación.
  - Demuestre que el caso base falla para esta afirmación.
  - Concluya que la afirmación es falsa.
  - Use inducción para demostrar que  $n^2 + 5 \cdot n + 1$  es impar para todo  $n \in \mathbb{N}$ .
40. Considere un tablero de ajedrez de  $2^n \times 2^n$  en el cual ha sido eliminada arbitrariamente una de sus celdas ( $n \geq 1$ ). Demuestre que dicho tablero puede ser cubierto, sin omitir celdas ni con sobrelapamientos, con fichas en forma de  $L$  que cubren exactamente 3 celdas.
41. El *principio del palomar*, en su versión más sencilla, corresponde a la siguiente afirmación para  $n \geq 1$ : si  $n + 1$  canicas se distribuyen en  $n$  cajas, entonces al menos una caja contiene más de una canica. Demuestre por el principio de inducción matemática esta formulación del principio del palomar.
42. Considere un grupo de  $n \in \mathbb{N}$  parejas. Usando el principio del palomar (ver Ejercicio 41) determine cuántas de las  $2n$  personas del grupo deben ser seleccionadas para garantizar que se ha seleccionado al menos una pareja?
43. De la colección  $1, 2, \dots, 200$  son seleccionados 101 números. Demuestre que entre los números seleccionados hay dos tales que uno divide al otro.
44. Considere un conjunto  $C$  de  $n + 1$  números tomados del conjunto  $\{1, 2, \dots, 2n\}$ , con  $n \geq 1$ . Demuestre que en  $C$  hay dos números tales que uno divide al otro.
45. Un maestro de ajedrez tiene 11 semanas de preparación para un torneo. Para ello decide jugar al menos una partida todos los días. Sin embargo, para no cansarse más de la cuenta decide no jugar más de 12 partidas en una semana calendario. Demuestre que hay una sucesión (consecutiva) de días en los cuales el maestro de ajedrez juega *exactamente* 21 partidas.
- 

### 0.3. Sistemas formales

Un sistema formal es el marco matemático apropiado para definir y aclarar conceptos fundamentales como *proposición matemática*, *axioma*, *demonstración* y *teorema*. Antes que todo, se introduce la terminología comúnmente usada en el estudio de sistemas formales.

**Definición 0.7**

Sea  $S$  un conjunto de símbolos. Una *expresión en  $S$*  (o *palabra en  $S$* ) es una secuencia finita (posiblemente vacía) de símbolos de  $S$ .

Por ejemplo, si  $S = \{a, b, c\}$ , entonces *baca* y *cba* son expresiones en  $S$ .

En la descripción de un lenguaje formal primero se especifica el conjunto de símbolos  $S$  y luego se seleccionan ciertas expresiones construidas con base en los símbolos que se designan como *fórmulas*. No necesariamente toda expresión es una fórmula del sistema formal. Por ejemplo, si  $S$  es el conjunto de letras del alfabeto castellano con sus acentos (i.e.,  $S = \{a, b, c, \dots, \tilde{n}, \dots, z\}$ ) entonces *niño* y *qwerty* son expresiones en  $S$ . Si se declaran como fórmulas aquellas expresiones que aparecen en el *diccionario de la lengua española* (<http://rae.es>), entonces *niño* es una fórmula pero *qwerty* no.

**Definición 0.8**

Un *sistema formal* tiene tres componentes:

- un *lenguaje formal* que consiste en un conjunto de símbolos y fórmulas construidas a partir de los símbolos,
- un conjunto de *axiomas* que corresponde a algunas fórmulas,
- unas *reglas de inferencia* que permiten obtener una fórmula a partir de un conjunto de fórmulas.

Para el lenguaje del sistema formal debe siempre existir un algoritmo para decidir (i.e., que responda *si* o *no* en un número finito de pasos) si una expresión arbitraria es o no una de sus fórmulas. Es importante recalcar que todos los lenguajes estudiados en este texto tienen esta propiedad.

**Nota 0.9**

A lo largo de este texto las letras griegas minúsculas  $\phi, \psi, \alpha, \beta, \gamma, \delta, \dots$  (incluyendo sus versiones primadas o con subíndices) se usan para denotar fórmulas de un sistema formal, mientras que las letras griegas mayúsculas  $\Phi, \Psi, \Gamma, \Delta, \dots$  se usan para denotar conjuntos de fórmulas.

Los *axiomas* de un sistema formal son algunas fórmulas especialmente seleccionadas. En muchos casos el lenguaje formal se escoge con cierta interpretación inicial en mente y los axiomas entonces son algunas fórmulas “obviamente ciertas”. Un sistema formal debe contar con un algoritmo que decida si una de sus fórmulas es o no un axioma.

Una *regla de inferencia* es un mecanismo que permite obtener una fórmula (llamada *conclusión*) a partir de un conjunto finito de fórmulas (llamadas *premisas*). Suponga

que  $\phi_0, \phi_1, \dots, \phi_k, \phi$  son fórmulas. Una regla de inferencia con premisas  $\phi_0, \phi_1, \dots, \phi_k$  (es común que  $k = 0, 1, 2$ ) y conclusión  $\phi$  se escribe esquemáticamente como

$$\frac{\phi_0 \quad \phi_1 \quad \cdots \quad \phi_k}{\phi}.$$

En cualquier sistema formal hay una cantidad finita de reglas de inferencia.

#### Ejemplo 0.5

A continuación se define el sistema formal ADD:

**Lenguaje:** los símbolos son ‘+’, ‘=’ y ‘|’. Una fórmula es una expresión de la forma  $x + y = z$ , en donde  $x, y$  y  $z$  son secuencias no vacías en las cuales únicamente aparece el símbolo ‘|’.

**Axiomas:** el único axioma es la fórmula  $| + | = ||$ .

**Reglas de inferencia:** hay dos reglas de inferencia

$$\frac{x + y = z}{x| + y = z|} \text{ R1} \qquad \frac{x + y = z}{y + x = z} \text{ R2.}$$

Un sistema formal usualmente se propone con una *interpretación* o intuición en mente. Es decir, el lenguaje y los axiomas son seleccionados para estudiar un tema específico como la lógica proposicional, la aritmética, la teoría de conjuntos, etc. Sin embargo, es importante aclarar que una interpretación no hace parte de un sistema formal. Aquellos conceptos de un sistema formal que se definen sin hacer referencia a una interpretación son llamados elementos *sintácticos*. A su vez, conceptos que dependen del significado o interpretación de los símbolos son llamados elementos *semánticos*. La interacción entre los conceptos sintácticos y semánticos es fundamental en el estudio de la lógica matemática vista como un sistema formal. Por ejemplo, en la lógica proposicional existe el concepto sintáctico de *teorema* y el semántico de *tautología*. Un objetivo frecuente en el estudio de la lógica proposicional es demostrar que una fórmula es un teorema si y solo si es una tautología; en este texto, este tipo de propiedades se demuestra, cuando llegue el momento, tanto para la lógica proposicional como para la lógica de predicados.

Al contar con el concepto de sistema formal, ahora es posible dar definiciones precisas de lo que son una *demonstración* y un *teorema*.

#### Definición 0.10

Sea  $F$  un sistema formal. Una *demonstración* en  $F$  es una secuencia finita de fórmulas  $\phi_0, \phi_1, \dots, \phi_n$  de  $F$  tal que, para cada  $0 \leq k \leq n$ , una de las siguientes condiciones es cierta:

1.  $\phi_k$  es un axioma de  $F$ , o

2.  $k > 0$  y  $\phi_k$  es la conclusión de una regla de inferencia de  $F$  cuyas premisas aparecen en la secuencia  $\phi_0, \dots, \phi_{k-1}$ .

Si  $\phi_0, \phi_1, \dots, \phi_n$  es una demostración en  $F$ , entonces se dice que  $\phi_n$  es un *teorema* de  $F$ , lo cual se escribe como

$$\vdash_F \phi_n.$$

Las definiciones de demostración y teorema carecen de semántica alguna y es así como estos dos conceptos son netamente elementos sintácticos de cualquier sistema formal.

#### Nota 0.11

Una demostración  $\phi_0, \phi_1, \dots, \phi_n$  en un sistema formal  $F$  se puede diagramar esquemáticamente de la siguiente forma

- |             |                             |
|-------------|-----------------------------|
| 0. $\phi_0$ | (explicación <sub>0</sub> ) |
| 1. $\phi_1$ | (explicación <sub>1</sub> ) |
| ...         |                             |
| n. $\phi_n$ | (explicación <sub>n</sub> ) |

en la cual *explicación<sub>i</sub>* es un texto explicando cómo se obtiene la fórmula  $\phi_i$  a partir de  $\phi_0, \dots, \phi_{i-1}$ . Adicionalmente, cuando el sistema formal bajo discusión esté claramente identificado, se puede obviar el subíndice y escribir  $\vdash \phi$  en lugar de  $\vdash_F \phi$  para cualquier teorema  $\phi$  de  $F$ .

A continuación, en el Ejemplo 0.6, se muestra cómo el formato de demostración puede ser usado en el sistema ADD. En particular, es importante notar el papel importante que juegan las explicaciones en cada uno de los renglones de una demostración para que un lector pueda seguirla y entender por qué es correcta.

#### Ejemplo 0.6

La fórmula  $\| + \| = \|\|\|$  es un teorema del sistema formal ADD:

- |                           |                    |
|---------------------------|--------------------|
| 0. $  +   = \ $           | (axioma de ADD)    |
| 1. $\  +   = \  $         | (R1 con premisa 0) |
| 2. $\   +   = \ \ \ $     | (R1 con premisa 1) |
| 3. $  + \ \  = \ \ \ $    | (R2 con premisa 2) |
| 4. $\  + \ \  = \ \ \ \ $ | (R1 con premisa 3) |

En conclusión  $\vdash_{ADD} \| + \| = \|\|\|$ .

La noción de demostración formal es clave en el desarrollo de las matemáticas. De hecho, los sistemas formales fueron inicialmente planteados por Hilbert con el objetivo de estudiar y analizar las demostraciones matemáticas. Así como la geometría estudia objetos en un espacio geométrico y la aritmética estudia los números, *la teoría de demostraciones* estudia las demostraciones. Los sistemas formales son el marco dentro del cual se lleva a cabo la teoría de demostraciones.

Finalmente, es conveniente incluir notación para referirse a aquellas fórmulas de un sistema formal que no hacen parte de su conjunto de teoremas.

#### Nota 0.12

Para  $F$  un sistema formal y  $\phi$  una fórmula de  $F$ , la expresión

$$\not\models_F \phi$$

se usa para denotar que  $\phi$  *no* es teorema de  $F$ .

Unas palabras de precaución sobre el significado asociado a la relación  $\not\models_F$  para cualquier sistema formal  $F$ . Para poder afirmar que una fórmula  $\phi$  no es teorema de  $F$  (i.e., para afirmar  $\not\models_F \phi$ ) hay que justificar que *no* existe demostración alguna de  $\phi$  en  $F$ . En particular, no es suficiente con desfallecer en el intento de encontrar una demostración para  $\phi$ , sino que es necesario “demostrar” que no existe tal demostración. Para este propósito se requieren, generalmente, técnicas de razonamiento externas al sistema formal, es decir, técnicas para razonar acerca del sistema formal como objeto de estudio (e.g., metateoremas del sistema formal).

Por ejemplo y de acuerdo con la interpretación intuitiva de lo que representa el sistema formal ADD, sería deseable que la fórmula  $\| + \| = \| \|= \|$  no sea uno de sus teoremas. En el Ejemplo 0.7 de la siguiente sección se establece un metateorema garantizando que la cantidad de palotes a la izquierda y a la derecha de ‘=’ coincide en cualquier teorema de ADD. Gracias a dicho metateorema, se puede concluir que  $\not\models_{ADD} \| + \| = \| \|= \|$  porque la cantidad de palotes a la izquierda y a la derecha de ‘=’ no coincide: son 4 y 3, respectivamente. La técnica utilizada en el Ejemplo 0.7 es la inducción matemática sobre fórmulas de un sistema formal, la cual se explica a continuación.

**0.3.1. Inducción sobre teoremas.** A veces es necesario demostrar que el conjunto de teoremas de un sistema formal  $F$  satisface una propiedad  $Q$ . Esta sección estudia la inducción sobre la longitud de una demostración, un principio de inducción derivado del *principio de inducción matemática* (Metateorema 0.5), sumamente útil para demostrar propiedades sobre teoremas de un sistema formal y extensivamente empleado a lo largo de este texto para tal fin.

Suponga que  $\vdash_F \phi$ , en donde  $\phi$  es una fórmula de  $F$ . Entonces, por la definición de teorema, necesariamente existe al menos una demostración de  $\phi$  con  $n \geq 1$  renglones (aquí,  $n$  es una variable sobre los números naturales). Dicha demostración puede verse de

la siguiente forma:

$$\begin{array}{ll}
 0. & \phi_0 & (\dots) \\
 1. & \phi_1 & (\dots) \\
 \dots & & \\
 n-1. & \phi_{n-1} & (\dots)
 \end{array}$$

en la cual cada expresión  $\phi_i$  ( $0 \leq i \leq n-1$ ) es una fórmula de  $\mathsf{F}$  y la última fórmula  $\phi_{n-1}$  es en realidad  $\phi$  (de lo contrario la secuencia de fórmulas no sería una demostración de  $\phi$ ).

#### Nota 0.13

Fíjese que la fórmula  $\phi$  que se usa como objeto de la demostración, aparte de ser un teorema, es cualquier fórmula del sistema formal. Ninguna otra suposición se ha hecho sobre la forma o estructura interna de  $\phi$ . Lo mismo sucede con los  $\phi_i$ . Entonces, en caso tal de lograr el objetivo de demostrar que  $\phi$  tiene la propiedad  $Q$ , necesariamente se logra demostrar que *cualquier* teorema de  $\mathsf{F}$  tiene la propiedad  $Q$ . Este tipo de comportamiento se conoce comúnmente como el *principio de universalidad*.

Por un momento suponga que la propiedad  $Q$  satisface las siguientes dos condiciones:

1. cada axioma de  $\mathsf{F}$  tiene la propiedad  $Q$ ,
2. cada regla de inferencia de  $\mathsf{F}$  es tal que si sus premisas tienen la propiedad  $Q$ , entonces necesariamente su conclusión tiene la propiedad  $Q$ .

Bajo estas dos suposiciones, el objetivo es demostrar  $Q(\phi)$  (i.e., que el teorema  $\phi$  tiene la propiedad  $Q$ ). Al analizar la demostración  $\phi_0, \dots, \phi_{n-1}$  de  $\phi$  bajo estos dos supuestos, se tiene que la fórmula  $\phi_0$  es necesariamente un axioma de  $\mathsf{F}$  dado que aparece en la primera línea de la demostración. Por la suposición (1), entonces se concluye que  $\phi_0$  tiene la propiedad  $Q$ . Ahora considere la segunda fórmula  $\phi_1$ . Si esta fórmula es también un axioma, entonces tiene la propiedad  $Q$  por la suposición (1). De lo contrario,  $\phi_1$  es la conclusión de una regla de inferencia cuya única premisa puede ser  $\phi_0$ . Ya se conoce que la fórmula  $\phi_0$  tiene la propiedad  $Q$ . Entonces, por la suposición (2), se concluye que  $\phi_1$  también tiene la propiedad  $Q$ . Al continuar de esta forma, se llegará a la conclusión de que la fórmula  $\phi_{n-1}$  (la misma  $\phi$ ) tiene la propiedad  $Q$ , i.e.,  $Q(\phi)$ .

El párrafo anterior hace un recuento informal de una técnica de demostración importante llamada *inducción sobre teoremas* o *inducción sobre la longitud de una demostración*. A continuación, en el Metateorema 0.14, se presenta una demostración formal (i.e., rigurosa) de este resultado.

#### Metateorema 0.14

Sea  $\mathsf{F}$  un sistema formal y  $Q$  una propiedad sobre las fórmulas de  $\mathsf{F}$ .

Para demostrar que todo teorema de  $\mathsf{F}$  tiene la propiedad  $Q$ , basta con:

1. demostrar que cada axioma de  $\mathcal{F}$  tiene la propiedad  $Q$
2. demostrar que cada regla de inferencia de  $\mathcal{F}$  es tal que si cada una de sus premisas tiene la propiedad  $Q$ , entonces su conclusión tiene la propiedad  $Q$ .

**Demostración.** Para  $n \in \mathbb{N}$ , sea  $S(n)$  la propiedad “todo teorema de  $\mathcal{F}$  con una demostración de máximo  $n$  renglones tiene la propiedad  $Q$ ”. El objetivo es entonces demostrar que todo  $n \geq 1$  tiene la propiedad  $S$ . De este modo, se habrá demostrado que todo teorema de  $\mathcal{F}$  tiene la propiedad  $Q$  (¿por qué?). La demostración procede por inducción matemática sobre  $n$ , suponiendo que (1) y (2) son ciertos.

**Caso base:** En este caso  $n = 1$  y el objetivo es demostrar que todo teorema de  $\mathcal{F}$  con una demostración de máximo un renglón tiene la propiedad  $Q$ . Dado que hay un solo renglón en la demostración, necesariamente dicho teorema es un axioma (porque aparece en el primer renglón de la demostración); por la suposición (1), se concluye que el teorema tiene la propiedad  $Q$ .

**Caso inductivo:** Suponga que  $n \geq 1$  tiene la propiedad  $S$ ; el objetivo es demostrar que  $n + 1$  tiene la propiedad  $S$ . Sea  $\phi$  un teorema de  $\mathcal{F}$  con una demostración de  $n + 1$  pasos; algo de la forma  $\phi_0, \phi_1, \dots, \phi_{n-1}, \phi$ , en donde cada  $\phi_i$  es una fórmula de  $\mathcal{F}$ . Hay dos casos sobre  $\phi$ . Si  $\phi$  es un axioma, entonces por la suposición (1),  $\phi$  tiene la propiedad  $Q$ . Si no,  $\phi$  es la conclusión de una regla de inferencia con premisas en  $\phi_0, \phi_1, \dots, \phi_{n-1}$ . Note que cualquier premisa tiene una demostración de máximo  $n$  líneas (la misma demostración de  $\phi$  sirve como testigo). Entonces, por la hipótesis inductiva se obtiene que cada premisa tiene la propiedad  $Q$ . Por la suposición (2), dado que  $\phi$  es la conclusión de una regla de inferencia cuyas premisas todas tienen la propiedad  $Q$ , necesariamente  $\phi$  tiene la propiedad  $Q$ . En cualquiera de los dos casos,  $\phi$  tiene la propiedad  $Q$  y consecuentemente  $n + 1$  tiene la propiedad  $S$ . Es decir,  $S(n)$  implica  $S(n + 1)$ .

Por el principio de inducción matemática todo  $n \geq 1$  tiene la propiedad  $S(n)$ . Es decir, todo teorema de  $\mathcal{F}$  tiene la propiedad  $Q$ .  $\square$

No debe ser una sorpresa “descubrir” que la inducción sobre teoremas comúnmente recibe el nombre de “demostración por inducción sobre el número de pasos de una demostración”. Su uso se ilustra con el siguiente ejemplo.

#### Ejemplo 0.7

Considere el sistema ADD. Una fórmula  $x + y = z$  de ADD se llama *balanceada* si y solo si el número de ocurrencias de ‘|’ en  $x$  e  $y$  es igual al número de ocurrencias de ‘|’ en  $z$ . Por ejemplo,  $|| + ||| = ||||$  es balanceada pero  $|| + | = |$  no lo es. El objetivo es demostrar que todo

teorema de ADD es una fórmula balanceada (o, alternativamente, que si  $\phi$  es un teorema de ADD, entonces  $\phi$  es balanceada).

Para este fin, sea usa el principio de inducción sobre teoremas (Metateorema 0.14). En este ejemplo,  $Q$  es la propiedad de que una fórmula sea balanceada. El único axioma de ADD es  $| + | = ||$ ; esta fórmula es balanceada dado que la cantidad de ‘|’ a la izquierda y a la derecha de ‘=’ es 2. Hay dos reglas de inferencia. En este ejemplo se razona sobre  $R1$  y se deja al lector completar la demostración para  $R2$ . La premisa de  $R1$  es  $x + y = z$ ; sean  $i, j, k \in \mathbb{N}$  la cantidad de ocurrencias de ‘|’ en  $x$ ,  $y$  y  $z$ , respectivamente. Como hipótesis se tiene que  $i + j = k$ . En la conclusión de  $R1$ , el número de ocurrencias de ‘|’ en  $x|$  es  $i + 1$  y en  $z|$  es  $k + 1$ . Entonces  $(i + 1) + j = (k + 1)$  y la conclusión  $x| + y = z|$  es balanceada, como se esperaba.

En el Ejemplo 0.7 se demuestra (usando el principio de inducción sobre teoremas) que si  $\phi$  es un teorema de ADD, entonces  $\phi$  es balanceada. Como se justificará en el desarrollo de este texto, esta conclusión es equivalente a la siguiente afirmación: si una fórmula de ADD no es balanceada, entonces no es uno de sus teoremas. Esto permite concluir directamente, por ejemplo, que la fórmula  $|| + || = |||$  no es teorema de ADD.

#### Nota 0.15

Cuando se deseé demostrar que una fórmula  $\phi$  no hace parte del conjunto de teoremas de un sistema formal, posiblemente sea útil encontrar una propiedad que cumplen todos los teoremas de dicho sistema formal, pero que no cumple  $\phi$ . Con base en esta propiedad universal de todos los teoremas, se puede justificar que  $\phi$  no es uno de ellos.

Hay una forma alternativa para presentar la demostración del Ejemplo 0.7, usando como principio subyacente el mismo de la inducción sobre teoremas. El objetivo es contar con una demostración más algebraica, en la cual la manipulación simbólica permita ahorrar en prosa y, a su vez, haga los pasos deductivos posiblemente más claros para algunos lectores. Con este propósito, se enriquecerá el lenguaje con el que hasta ahora se cuenta.

#### Ejemplo 0.8

Considere el sistema ADD. Se propone la función  $P$ , definida para cualquier expresión  $\phi$  de ADD, de la siguiente manera:

$P(\phi)$ : cantidad de palotes en  $\phi$ .

Por ejemplo,  $P(\| + |) = 4$ ,  $P(| + | = \|) = 5$ ,  $P(=) = 0$  y  $P(+) = 0$ . Note que para cualquier fórmula  $x + y = z$  de ADD se tiene que

$$P(x + y = z) = P(x) + P(y) + P(z).$$

#### Nota 0.16

Es importante resaltar que en el Ejemplo 0.8 los símbolos  $+$  y  $=$  aparecen con dos significados distintos. Por una parte, estos símbolos hacen parte del sistema formal ADD y no tienen nada que ver con la suma e igualdad de números, respectivamente. Por otra parte, los símbolos  $+$  y  $=$  en la definición de  $P$  si corresponden a la suma e igualdad de números naturales, respectivamente. En particular, la expresión que aparece al final del Ejemplo 0.8 puede ser escrita, con más precisión y evitando ambigüedades, anotando cada operador con un sufijo que indique el sistema formal al cual pertenece; por ejemplo:

$$P(x +_{\text{ADD}} y =_{\text{ADD}} z) =_{\mathbb{N}} P(x) +_{\mathbb{N}} P(y) +_{\mathbb{N}} P(z).$$

En general, este nivel de detalle se evita en la escritura de expresiones para facilitar su lectura. Sin embargo, en algunas partes del texto se apelará a este tipo de detalles dado que evitan posibles confusiones al lector.

Con base en la meta-notación introducida en el Ejemplo 0.8 (i.e.,  $P$  no hace parte del sistema formal), a continuación se presenta una demostración alternativa a la del Ejemplo 0.7.

#### Ejemplo 0.9

Considere el sistema ADD. Una fórmula  $x + y = z$  de ADD se llama *balanceada* si y solo si  $P(x) + P(y) = P(z)$ . El objetivo es demostrar que todo teorema de ADD es una fórmula balanceada.

Para este fin, sea usado el principio de inducción sobre teoremas (Metateorema 0.14). En este ejemplo,  $Q$  es la propiedad definida para cualquier fórmula  $x + y = z$  de la siguiente manera:

$$Q(x + y = z) : P(x) + P(y) = P(z).$$

El único axioma de ADD es  $| + | = \|$ ; esta fórmula es balanceada dado que:

$$P(|) + P(|) = 1 + 1 = 2 = P(\|).$$

Hay dos reglas de inferencia. En este ejemplo se razona sobre  $R1$  y se deja al lector completar la demostración para  $R2$ . La premisa de  $R1$  es  $x + y = z$  y entonces la hipótesis es

$P(x) + P(y) = P(z)$ . Como  $x| + y = z|$  es la conclusión de  $R1$ , el objetivo es demostrar que esta fórmula tiene la propiedad  $Q$ :

$$\begin{aligned} P(x|) + P(y) &= P(x) + 1 + P(y) && \text{(definición de } P\text{)} \\ &= (P(x) + P(y)) + 1 && \text{(aritmética)} \\ &= P(z) + 1 && \text{(suposición: } P(x) + P(y) = P(z)\text{)} \\ &= P(z|) && \text{(definición de } P\text{).} \end{aligned}$$

Es decir, si  $x + y = z$  es balanceada, también lo es  $x| + y = z|$ .

Al final, la diferencia primordial entre las demostraciones de los ejemplos 0.7 y 0.9 radica en la forma en la cual se presentan las argumentaciones. La del Ejemplo 0.7 sigue una tradición más cercana a lo comúnmente usado en matemáticas, mientras que la del Ejemplo 0.9 está más alineada con lo propuesto y preferido en este texto: es muchas ocasiones, en aras de la claridad, es posible y deseable ‘calcular’ una demostración.

## Ejercicios

1. Complete el Ejemplo 0.7 con el caso para la regla  $R2$  de ADD.

2. Complete el Ejemplo 0.9 con el caso para la regla  $R2$  de ADD.

3. Liste todos los teoremas del siguiente sistema formal:

**Lenguaje:** hay tres símbolos ‘ $a$ ’, ‘ $b$ ’ y ‘ $c$ ’; toda expresión es una fórmula.

**Axiomas:**  $cabcba$ .

**Reglas de inferencia:** hay tres reglas de inferencia:

- a) si la fórmula comienza con  $a$ , agregue  $cac$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante;
- b) si la fórmula comienza con  $b$ , agregue  $bab$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante;
- c) si la fórmula comienza con  $c$ , agregue  $ca$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante.

4. Liste todos los teoremas del siguiente sistema formal:

**Lenguaje:** hay tres símbolos ‘ $a$ ’, ‘ $b$ ’ y ‘ $c$ ’; toda expresión es una fórmula.

**Axiomas:**  $abccba$ .

**Reglas de inferencia:** hay tres reglas de inferencia:

- a) si la fórmula comienza con  $a$ , agregue  $bab$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante;
- b) si la fórmula comienza con  $b$ , agregue  $abba$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante;
- c) si la fórmula comienza con  $c$ , agregue  $ca$  a la derecha y luego elimine los primeros tres símbolos de la expresión resultante.

5. Justifique por qué las siguientes fórmulas no son teoremas de ADD:

- a)  $| + | = |$   
 b)  $\| + \| = \|\|$   
 c)  $| + \| = \|\|$
6. En el Ejemplo 0.7 se demuestra que si una fórmula es teorema de ADD, entonces dicha fórmula es balanceada. Demuestre la otra dirección de esta afirmación: si una fórmula de ADD es balanceada, entonces dicha fórmula es teorema de ADD.
7. Proponga un sistema formal MULT que sea similar a ADD pero cuyos teoremas sean ecuaciones ciertas de la multiplicación de los números naturales positivos. Demuestre que la fórmula  $\| \times \| = \|\|\|$  es un teorema de MULT.
8. Considere el sistema formal PR cuyas fórmulas son cadenas (i.e., secuencias) de paréntesis. El lenguaje tiene dos símbolos: ‘(’ y ‘)’. Cualquier expresión es una fórmula. El único axioma es  $()$ . Sean  $\phi$  y  $\psi$  dos fórmulas de PR; hay tres reglas de inferencia:
- $$\frac{\phi}{(\phi)} \text{ ADD} \qquad \frac{\phi}{\phi\phi} \text{ DOUBLE} \qquad \frac{\phi(\psi)}{\phi\psi} \text{ OMIT.}$$
- a) Demuestre que las siguientes fórmulas son teoremas de PR:
- 1)  $((())()$
  - 2)  $(0)(0)(0)$
  - 3)  $0((0))0$
- b) Demuestre que todo teorema de PR tiene la propiedad de que la cantidad de paréntesis izquierdos es igual a la cantidad de paréntesis derechos.
9. Considere el sistema formal PR' cuyas fórmulas, al igual que en el sistema PR (Ejercicio 8), son cadenas de paréntesis bien formadas. De hecho, en PR', el lenguaje, el conjunto de fórmulas y el conjunto de axiomas son los mismos de PR. Las reglas de inferencia de PR' son las siguientes:
- $$\frac{\phi}{(\phi)} \text{ ADD}' \qquad \frac{\phi \quad \psi}{\phi\psi} \text{ JOIN.}$$
- a) Demuestre que cada una de las fórmulas en el Ejercicio 8a son teoremas de PR'.
- b) ¿Son todos los teoremas de PR teoremas de PR'? Justifique su respuesta.
- c) ¿Son todos los teoremas de PR' teoremas de PR? Justifique su respuesta.
10. Sea F un sistema formal. Considere una función  $f$  que asigna a cada fórmula de F un valor en el conjunto  $\{0, 1\}$  y que satisface las siguientes condiciones:
- a) Si  $\phi$  es un axioma de F, entonces  $f(\phi) = 0$ .
  - b) Si  $\phi_0, \dots, \phi_n$  son las premisas de una regla de inferencia de F con conclusión  $\phi$  y  $f(\phi_0) = f(\phi_1) = \dots = f(\phi_n) = 0$ , entonces  $f(\phi) = 0$ .
- Demuestre que si  $\vdash_F \psi$ , entonces  $f(\psi) = 0$ .
11. Investigue acerca de las siguientes expresiones y explique brevemente su significado. Ilustre cada una de ellas con un ejemplo.
- a) Problema de decisión.
  - b) Algoritmo/procedimiento de decisión.
  - c) Problema decidable.
  - d) Problema indecidible.
12. Considere el sistema formal EVEN cuyos teoremas representan números naturales pares distintos a cero. El único símbolo del sistema formal es ‘|’, cualquier expresión es

una fórmula y el único axioma es  $\parallel$ . Hay una regla de inferencia:

$$\frac{\phi}{\phi \parallel} \text{PILE.}$$

- a) Demuestre que cualquier teorema de EVEN tiene una cantidad par de palotes.
  - b) Demuestre que cualquier fórmula con una cantidad par de palotes es un teorema de EVEN.
  - c) Demuestre que EVEN es decidible.
  - d) Cambie el axioma de EVEN por uno nuevo, resultando en un sistema formal ODD, de tal manera que los teoremas de ODD representen exactamente los números naturales impares.
13. Consideré el sistema formal 2POW descrito a continuación: hay dos símbolos ‘a’ y ‘b’, cualquier expresión es una fórmula, el único axioma es  $ab$  y hay una regla de inferencia:
- $$\frac{\phi}{a\phi b} \text{EXTEND.}$$
- a) Demuestre para  $n \geq 1$ ,  $a^n b^n$  es un teorema de 2POW ( $a^n$  denota la cadena de  $n$  apariciones de  $a$ ).
  - b) Sea  $\phi$  un teorema de 2POW. Demuestre que hay un  $n \geq 1$  tal que  $\phi$  es  $a^n b^n$ .
  - c) Demuestre que 2POW es decidible.
14. A continuación se describe el sistema formal PAL cuyos teoremas son todas los palíndromes sobre 3 letras. El lenguaje tiene tres símbolos ‘a’, ‘b’ y ‘c’, cualquier expresión es una fórmula y hay seis axiomas:  $a, b, c, aa, bb$  y  $cc$ . El sistema cuenta con tres reglas de inferencia en las cuales  $\phi$  denota cualquier expresión de PAL:
- $$\frac{\phi}{a\phi a} \text{ADD } a \quad \frac{\phi}{b\phi b} \text{ADD } b \quad \frac{\phi}{c\phi c} \text{ADD } c.$$
- a) Demuestre que las siguientes fórmulas son teoremas de PAL:
    - 1)  $abcccba$
    - 2)  $abcccba$
  - b) Demuestre que todo teorema de PAL es palíndrome.
  - c) Demuestre que todo palíndrome sobre los símbolos ‘a’, ‘b’ y ‘c’ es teorema de PAL.
15. A continuación se describe el sistema formal MIU el cual aparece en el libro *Gödel, Escher, Bach* de D. Hofstadter (1973). Hay tres símbolos ‘M’, ‘I’ y ‘U’, cualquier expresión es una fórmula y hay un único axioma  $MI$ . El sistema tiene 4 reglas de inferencia, que se presentan a continuación. En ellas,  $\phi$  y  $\psi$  representan cualquier expresión (i.e., secuencia finita de símbolos, posiblemente vacía):

$$\frac{\phi I}{\phi IU} \text{R1} \quad \frac{M\phi}{M\phi\phi} \text{R2} \quad \frac{\phi III\psi}{\phi U\psi} \text{R3} \quad \frac{\phi UU\psi}{\phi\psi} \text{R4.}$$

- a) Demuestre que las siguientes fórmulas son teoremas de MIU:
  - 1)  $MIU$
  - 2)  $MIUIUIUIU$
  - 3)  $MUIIIIU$

- b) Demuestre que la cantidad de apariciones de  $I$  en un teorema de MIU nunca es múltiplo de 3.
- c) ¿Es MU un teorema de MIU?
16. Considere el sistema formal COFFEE en el cual hay dos símbolos, ‘◦’ y ‘•’. Cualquier expresión es una fórmula y hay un único axioma ◦. El sistema tiene 4 reglas de inferencia, las cuales se presentan a continuación. En ellas,  $\phi$  y  $\psi$  representan cualquier expresión (i.e., secuencia finita de símbolos, posiblemente vacía):
- $$\frac{\phi \bullet \psi}{\phi \bullet \circ \psi} \text{ R1} \quad \frac{\phi \bullet \psi}{\phi \circ \bullet \psi} \text{ R2} \quad \frac{\phi \circ \psi}{\phi \circ \circ \psi} \text{ R3} \quad \frac{\phi \circ \psi}{\phi \bullet \bullet \psi} \text{ R4.}$$
- a) Demuestre que las siguientes fórmulas son teoremas de COFFEE:
- 1) ◦◦◦
  - 2) ◦◦•◦◦
  - 3) ◦◦◦•◦◦◦◦◦
- b) Demuestre que la cantidad de apariciones de • en un teorema de COFFEE es par.
17. Considere el sistema formal C•FFEE que resulta de COFFEE cambiando el axioma ◦ por •. La reglas de inferencia de C•FFEE son las mismas que en COFFEE. Demuestre o refute:
- a) La cantidad de apariciones de • en un teorema de C•FFEE es par.
  - b) La cantidad de apariciones de • en un teorema de C•FFEE es impar.
  - c) La cantidad de apariciones de ◦ en un teorema de C•FFEE es impar.
  - d) La cantidad de apariciones de ◦ en un teorema de C•FFEE es par.
18. Considere el sistema formal MCOFFEE en el cual hay dos símbolos, ‘◦’ y ‘•’. Cualquier expresión es una fórmula y hay un único axioma ◦. El sistema tiene 4 reglas de inferencia, las cuales se presentan a continuación. En ellas,  $\phi$  y  $\psi$  representan cualquier expresión (i.e., secuencia finita de símbolos, posiblemente vacía):
- $$\frac{\phi \circ \circ \circ \bullet \psi}{\phi \bullet \circ \psi} \text{ R1} \quad \frac{\phi \bullet \psi}{\phi \circ \bullet \psi} \text{ R2} \quad \frac{\phi \circ \circ \circ \circ \psi}{\phi \bullet \bullet \psi} \text{ R3} \quad \frac{\phi \circ \psi}{\phi \circ \circ \psi} \text{ R4.}$$
- a) Demuestre que las siguientes fórmulas son teoremas de MCOFFEE:
- 1) ◦◦◦••
  - 2) ◦•◦◦
  - 3) ◦◦◦•◦◦◦◦◦◦
- b) Demuestre que la cantidad de apariciones de • en un teorema de MCOFFEE es par.
-