ANA MESTRE

LÒGICA A LA INFORMÀTICA.

Notas de Clase para IL

0. Preliminares

Marta Arias, Rafel Farré, Guillem Godoy, Robert Nieuwenhuis,
Pilar Nivela, Albert Oliveras, Enric Rodríguez

3 de septiembre de 2009

1. Conjuntos

Un *conjunto* $\mathcal{A}$ es una colección de elementos distintos. Si un elemento x pertenece al conjunto $\mathcal{A}$ escribiremos $x \in \mathcal{A}$ y si x no pertenece al conjunto $\mathcal{A}$ escribiremos $x \notin \mathcal{A}$.

Hay conjuntos finitos e infinitos. El *cardinal* de un conjunto finito $\mathcal{A}$, denotado por $|\mathcal{A}|$, es el número de elementos que pertenecen a $\mathcal{A}$. Al conjunto de cero elementos, denotado por $\emptyset$, se le llama *conjunto vacío*.

Podemos, por ejemplo, considerar el conjunto $\mathcal{B}$ formado por los elementos a, b y c que se escribe de la forma $\mathcal{B} = \{ a, b, c \}$.

En los conjuntos no hay noción de orden entre sus elementos; así, al escribir $\{a, b, c\}$ estamos representando el mismo conjunto que escribiendo $\{ b, a, c \}$. Si, por el contrario, queremos considerar algunos elementos de un conjunto en un cierto orden, escribiremos por ejemplo $\langle a, b, c \rangle$ o $\langle b, a, c \rangle$, que son *secuencias* (listas ordenadas) distintas de elementos de $\{ a, b, c \}$.

Otro ejemplo de conjunto podría ser el conjunto $\mathcal{F}$ de todos los estudiantes de la FIB. Si Juan es un estudiante de la FIB escribiremos $Juan \in \mathcal{F}$. El conjunto $\mathcal{I}$ de todos los estudiantes e de la FIB que están matriculados en IL se puede expresar de la forma

$$\mathcal{I} = \{ e \mid e \in \mathcal{F} \text{ y } e \text{ matriculado en } IL \}$$

donde la barra vertical | se lee "tal que".

Ejemplos de conjuntos infinitos frecuentemente utilizados son el conjunto de los números naturales $\mathbb{N} = \{ 0, 1, 2, \ldots \}$, el de los números enteros $\mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2, \ldots \}$, el de los racionales

$$\mathbb{Q} = \{ \frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0 \}$$

y el de los números reales $\mathbb{R}$, como 2,3, $-27{,}82$ o $1/3$, posiblemente con un número infinito de decimales. Los naturales, los enteros y los racionales son números reales. También lo son los llamados números irracionales (no hay períodos en sus decimales) como por ejemplo $\pi = 3{,}141592653589\ldots$ y $\sqrt{2} = 1{,}414213562373\ldots$

Inclusión e igualdad de conjuntos

Se dice que el conjunto $\mathcal{A}$ está *incluído* en un conjunto $\mathcal{B}$, o que $\mathcal{A}$ es un *subconjunto* de $\mathcal{B}$, denotado por $\mathcal{A} \subseteq \mathcal{B}$, si todo elemento que pertenece a $\mathcal{A}$ también pertenece a $\mathcal{B}$. Por lo tanto, para todo conjunto $\mathcal{A}$ se cumple $\emptyset \subseteq \mathcal{A}$ y $\mathcal{A} \subseteq \mathcal{A}$. Por ejemplo, $\{ e, b \} \subseteq \{ a, b, c, d, e \}$.

Si $\mathcal{A} \subseteq \mathcal{B}$ y existe un elemento de $\mathcal{B}$ que no pertenece a $\mathcal{A}$ se dice que $\mathcal{A}$ es un *subconjunto propio* de $\mathcal{B}$ y se escribe $\mathcal{A} \subset \mathcal{B}$.

Dos conjuntos $\mathcal{A}$ y $\mathcal{B}$ se dice que son *iguales*, denotado $A = B$, si un elemento pertenece a A si y sólo si pertenece a B. Nótese que esto es equivalente a decir que $\mathcal{A} \subseteq \mathcal{B}$ y $\mathcal{B} \subseteq \mathcal{A}$.

Operaciones sobre conjuntos

Dados dos conjuntos $\mathcal{A}$ y $\mathcal{B}$, el *complementario* de $\mathcal{B}$ en $\mathcal{A}$, denotado por $\mathcal{A} - \mathcal{B}$, es el conjunto de los elementos que pertenecen a $\mathcal{A}$ y no pertenecen a $\mathcal{B}$, esto es

$$\mathcal{A} - \mathcal{B} = \{\, x \mid x \in \mathcal{A} \ y \ x \notin \mathcal{B} \,\}$$

La *unión* de dos conjuntos $\mathcal{A}$ y $\mathcal{B}$, denotado por $\mathcal{A} \cup \mathcal{B}$, es el conjunto de los elementos que pertenecen a $\mathcal{A}$, a $\mathcal{B}$ o a los dos, esto es

$$\mathcal{A} \cup \mathcal{B} = \{\, x \mid x \in \mathcal{A} \ o \ x \in \mathcal{B} \,\}$$

La *intersección* de dos conjuntos $\mathcal{A}$ y $\mathcal{B}$, denotado por $\mathcal{A} \cap \mathcal{B}$, es el conjunto de los elementos que pertenecen a la vez a $\mathcal{A}$ y a $\mathcal{B}$, esto es

$$\mathcal{A} \cap \mathcal{B} = \{\, x \mid x \in \mathcal{A} \ y \ x \in \mathcal{B} \,\}$$

Dos conjuntos $\mathcal{A}$ y $\mathcal{B}$ son *disjuntos* si $\mathcal{A} \cap \mathcal{B} = \emptyset$. Si dado un natural $n > 0$ tenemos n conjuntos $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n$, decimos que son *disjuntos dos a dos* si para todos los i, j con $1 \leq i < j \leq n$ se cumple $\mathcal{B}_i \cap \mathcal{B}_j = \emptyset$.

Dado un natural $n > 0$, y n conjuntos $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_n$, la unión de estos n conjuntos la denotamos por

$$\bigcup_{i=1}^{n} \mathcal{A}_i$$

y está definida de la forma

$$\bigcup_{i=1}^{n} \mathcal{A}_i = \{\, x \mid \textit{existe } i \in \{1, \ldots n\} \textit{ tal que } x \in \mathcal{A}_i \,\}$$

Del mismo modo la intersección de n conjuntos $\mathcal{A}_1, \mathcal{A}_2, \ldots \mathcal{A}_n$, es

$$\bigcap_{i=1}^{n} \mathcal{A}_i = \{\, x \mid x \in \mathcal{A}_i \textit{ para todo } i \in \{1, \ldots n\} \,\}$$

Dado un conjunto $\mathcal{A}$, se dice que los n conjuntos disjuntos dos a dos $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_n$ son una *partición* de $\mathcal{A}$ si

$$\mathcal{A} = \bigcup_{i=1}^{n} \mathcal{B}_i$$

El *producto cartesiano* de $\mathcal{A}$ por $\mathcal{B}$, denotado por $\mathcal{A} \times \mathcal{B}$, es el conjunto de todos los pares ordenados (a, b) donde a pertenece a $\mathcal{A}$ y b pertenece a $\mathcal{B}$:

$$\mathcal{A} \times \mathcal{B} = \{\, (a, b) \mid a \in \mathcal{A} \ y \ b \in \mathcal{B} \,\}$$

Propiedades de las operaciones sobre conjuntos

$\mathcal{A} \cup \mathcal{A} = \mathcal{A}$	idempotencia de $\cup$
$\mathcal{A} \cap \mathcal{A} = \mathcal{A}$	idempotencia de $\cap$
$\mathcal{A} \cup \mathcal{B} = \mathcal{B} \cup \mathcal{A}$	conmutatividad de $\cup$
$\mathcal{A} \cap \mathcal{B} = \mathcal{B} \cap \mathcal{A}$	conmutatividad de $\cap$
$(\mathcal{A} \cup \mathcal{B}) \cup C = \mathcal{A} \cup (\mathcal{B} \cup C)$	asociatividad de $\cup$
$(\mathcal{A} \cap \mathcal{B}) \cap C = \mathcal{A} \cap (\mathcal{B} \cap C)$	asociatividad de $\cap$
$\mathcal{A} \cup (\mathcal{B} \cap C) = (\mathcal{A} \cup \mathcal{B}) \cap (\mathcal{A} \cup C)$	distributividad de $\cup$ respecto de $\cap$
$\mathcal{A} \cap (\mathcal{B} \cup C) = (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap C)$	distributividad de $\cap$ respecto de $\cup$
$C - (\mathcal{A} \cup \mathcal{B}) = (C - \mathcal{A}) \cap (C - \mathcal{B})$	
$C - (\mathcal{A} \cap \mathcal{B}) = (C - \mathcal{A}) \cup (C - \mathcal{B})$	

Partes de un conjunto

Dado un conjunto $\mathcal{A}$, el conjunto de todos los subconjuntos de $\mathcal{A}$, denotado por $\mathcal{P}(\mathcal{A})$, recibe el nombre de *partes* de $\mathcal{A}$:

$$\mathcal{P}(\mathcal{A}) = \{ \mathcal{B} \mid \mathcal{B} \subseteq \mathcal{A} \}$$

Por ejemplo, si $\mathcal{A} = \{ a, b \}$ entonces $\mathcal{P}(\mathcal{A}) = \{ \emptyset, \{a\}, \{b\}, \{a, b\} \}$

Si $\mathcal{A}$ es un conjunto finito entonces $|\mathcal{P}(\mathcal{A})| = 2^{|\mathcal{A}|}$.

Cadenas sobre un conjunto

Dado $\mathcal{A}$, el conjunto de las *cadenas* sobre $\mathcal{A}$, denotado por $\mathcal{A}^*$ está definido por:

1. λ es una cadena sobre $\mathcal{A}$, llamada *cadena vacía* (λ es la letra griega "lambda").
2. si ω es una cadena sobre $\mathcal{A}$ y $a \in \mathcal{A}$ entonces ωa es una cadena sobre $\mathcal{A}$ (ω es la letra griega "omega").
3. nada más es una cadena sobre $\mathcal{A}$.

Al conjunto $\mathcal{A}^*$ se le llama también *palabras* sobre el *alfabeto* $\mathcal{A}$.

Por ejemplo si $\mathcal{A} = \{a, b\}$ entonces $\mathcal{A}^* = \{ \lambda, a, b, aa, ab, ba, bb, aaa, aab, \ldots \}$.

La *longitud* de una cadena $\omega = a_1\ a_2\ \ldots a_k$, denotada por $|\omega|$, es el número de elementos de ω, esto es, $|\omega| = k$.

Operaciones típicas sobre cadenas son la *concatenación* y la *inversión*. La *concatenación* de las cadenas ω_1 y ω_2 es la cadena $\omega_1\omega_2$. La *inversión* de una cadena $\omega = a_1\ a_2\ \ldots a_k$, denotada por ω^{inv}, es la cadena $\omega^{inv} = a_k\ a_{k-1}\ \ldots a_1$. Una cadena es capicúa, también llamada palíndromo, si $\omega = \omega^{inv}$.

Dadas dos cadenas ω_1 y ω_2, se dice que ω_1 es un *prefijo* de la cadena $\omega_1\omega_2$, y que ω_2 es un *sufijo* de $\omega_1\omega_2$.

2. Relaciones y funciones

Sean $\mathcal{A}$ y $\mathcal{B}$ dos conjuntos. Una *relación binaria* R entre $\mathcal{A}$ y $\mathcal{B}$ es un subconjunto del producto cartesiano $\mathcal{A} \times \mathcal{B}$. Si $(a, b) \in R$ se dice que a y b *están relacionados por* R. Si $\mathcal{A} = \mathcal{B}$ se dice que R es una *relación binaria en* $\mathcal{A}$.

En muchas ocasiones, en lugar de escribir $(a, b) \in R$ se escribe $a\ R\ b$. Esta notación se llama *infija* y se usa en relaciones frecuentemente utilizadas como $=$, $>$, $\geq$, etc., escribiéndose $a = b$, $a > b$, $a \geq b$, etc.

Por ejemplo, la relación $\mathcal{B} \subseteq C$ entre subconjuntos $\mathcal{B}$ y C de un conjunto $\mathcal{A}$ es una relación binaria en $\mathcal{P}(\mathcal{A})$.

En el conjunto $\mathbb{Z}$ podemos definir la relación en la que dos números enteros n y m están relacionados si ambos tienen el mismo resto al hacer la división entera por 3. A esta relación se la llama *congruencia módulo* 3 y la denotaremos de la forma $n =_{mod\ 3} m$. En general, dado un natural $p > 0$, se hablará de la relación *congruencia módulo* p.

Una relación $\sim$ en $\mathcal{A}$ es

- *reflexiva* si $a \sim a$, para todo $a \in \mathcal{A}$
- *simétrica* si para todos los $a \in A$, $b \in A$ con $a \sim b$ se cumple $b \sim a$
- *antisimétrica* si para todos los $a \in A$, $b \in A$ con $a \sim b$ y $b \sim a$ se cumple $a = b$
- *transitiva* si para todos los $a \in A$, $b \in A$, $c \in A$, con $a \sim b$ y $b \sim c$ se cumple $a \sim c$.
- *de equivalencia* si es reflexiva, simétrica y transitiva.

Por ejemplo, la relación de igualdad $=$ en un conjunto $\mathcal{A}$, donde cada elemento sólo está relacionado consigo mismo, también es una relación de equivalencia. La relación *congruencia módulo* p es de equivalencia en $\mathbb{Z}$.

Escribimos $f: \mathcal{A} \to \mathcal{B}$ para indicar que f es una relación binaria entre $\mathcal{A}$ y $\mathcal{B}$ en la que cada elemento de $\mathcal{A}$ está relacionado con un único elemento de $\mathcal{B}$. En este caso a f se le llama una *función* de $\mathcal{A}$ en $\mathcal{B}$, y en lugar de escribir $(a, b) \in f$, o de escribir $a\ f\ b$, se escribe $f(a) = b$.

Por ejemplo, la función $f: \mathcal{A} \to \mathcal{A}$ definida por $f(a) = a$ se llama la *identidad* sobre $\mathcal{A}$. También podemos considerar la función $suc: \mathbb{N} \to \mathbb{N}$ que a cada natural n le hace corresponder su sucesor, esto es, $suc(n) = n + 1$ para todo $n \in \mathbb{N}$.

Una función $f: \mathcal{A} \to \mathcal{B}$ es:

- *inyectiva* si para todos los $a_1, a_2 \in \mathcal{A}$ tales que $f(a_1) = f(a_2)$ se cumple que $a_1 = a_2$.
- *exhaustiva* si para todo $b \in \mathcal{B}$ existe $a \in \mathcal{A}$ tal que $f(a) = b$.
- *biyectiva* si es inyectiva y exhaustiva.

2.1. Relación de equivalencia y conjunto cociente

Si R es una relación de equivalencia en $\mathcal{A}$, se llama *clase de equivalencia* de a *módulo* R, denotada por $[a]_R$, al subconjunto de $\mathcal{A}$ de todos los elementos x relacionados con a:

$$[a]_R = \{\, x \in A \mid a\, R\, x \,\}$$

El conjunto de todas las clases de equivalencia $[a]_R$ es una partición de $\mathcal{A}$ llamada *conjunto cociente de* $\mathcal{A}$ *módulo* R y denotada por $A/_R$:

$$A/_R = \{\, [a]_R \mid a \in A \,\}$$

Cuando el contexto deja claro a qué relación nos estamos refiriendo, a veces escribimos simplemente $[a]$ en lugar de $[a]_R$.

Por ejemplo, si consideramos en $\mathbb{Z}$ la relación de equivalencia *módulo* 3 el conjunto de las clases de equivalencia, denotado por $\mathbb{Z}/=_{mod\ 3}$, es $\{\, [0], [1], [2] \,\}$. Aquí $[0]$ es la clase $\{\, \ldots, -6, -3, 0, 3, 6, \ldots \,\}$ de todos los múltiplos de 3, es decir, la de los enteros cuyo resto de la división entera por 3 es 0. La clase del 1 está formada por todos los enteros cuyo resto módulo 3 es 1, esto es $[1] = \{\, \ldots, -7, -4, 0, 4, 7, \ldots \,\}$ y la clase del 2 es $[2] = \{\, \ldots, -8, -5, 0, 5, 8, \ldots \,\}$.

2.2. Relaciones de orden

Una relación en un conjunto $\mathcal{A}$ es un *orden* si es reflexiva, antisimétrica y transitiva. Una relación de orden suele denotarse por $\leq$.

Por ejemplo, en $\mathbb{N}$ la relación menor o igual $\leq$ de los naturales es una relación de orden. En $\mathcal{P}(\mathcal{A})$ la relación $\subseteq$ es una relación de orden.

Se define la relación $<$ de la forma $a < b$ si $a \leq b$ y $a \neq b$ y se llama relación de *orden estricto* en $\mathcal{A}$.

Una relación de orden $\leq$ en $\mathcal{A}$ es *total* si para todos los elementos $a_1, a_2 \in A$ se cumple $a \leq b$ o bien $b \leq a$, es decir, si todo par de elementos están relacionados por $\leq$.

3. Combinatoria

Dado un natural $n > 0$, definimos el *factorial de* n, denotado $n!$, como el producto $1 \cdot 2 \cdots n$. Equivalentemente podríamos haber definido recursivamente que $1!$ es 1 y que si $n > 1$ entonces $n!$ es $(n-1)! \cdot n$.

El número de subconjuntos de m elementos de un conjunto $\mathcal{A}$ de n elementos, llamado también *combinaciones* de n elementos tomados de m en m, es

$$\binom{n}{m} = n!\ /\ (n-m)!m!$$

Una *permutación* de un conjunto $\mathcal{A}$ es una secuencia con todos los elementos de $\mathcal{A}$. Por ejemplo, las permutaciones del conjunto $\{a, b, c\}$ son $\langle a, b, c\rangle$, $\langle a, c, b\rangle$, $\langle b, a, c\rangle$,

$\langle b, c, a\rangle$, $\langle c, a, b\rangle$ y $\langle c, b, a\rangle$. Más formalmente, también se puede decir que una permutación de $\mathcal{A}$ es una función biyectiva de $\mathcal{A}$ en $\mathcal{A}$. Si $|\mathcal{A}| = n$, entonces el número de permutaciones de $\mathcal{A}$ es $n!$.

4. Demostración de propiedades

Antes hemos mencionado que un conjunto $\{a_1, \ldots, a_n\}$ tiene 2^n subconjuntos distintos (las partes del conjunto). Supongamos que una determinada persona no está convencida de esta propiedad y queremos escribir una justificación que le convenza.

Por ejemplo, podríamos argumentar lo siguiente. Si S es un subconjunto de un conjunto $\{a_1, \ldots, a_n\}$, por cada uno de los n elementos tenemos 2 posibilidades: que pertenezca a S o no. Así, tenemos 2 posibilidades para a_1, y por cada una de ellas, 2 posibilidades para a_2, lo cual da $2 \cdot 2$ posibilidades para a_1 y a_2. Por cada una de estas $2 \cdot 2$ posibilidades, tenemos 2 posibilidades para a_3, lo cual da $2 \cdot 2 \cdot 2$, que son 2^3 posibilidades para los tres primeros elementos, y así sucesivamente hasta alcanzar las 2^n posibilidades para los n elementos.

Es posible que con esto hayamos convencido a nuestro interlocutor. Si es así, para él esta justificación es una *demostración*. Sin embargo, lo que para una persona es demostración suficiente puede no serlo para otra, por ejemplo, porque no tiene los conocimientos necesarios para aceptar sin explicaciones algunos pasos intermedios. El grado de detalle en una demostración también depende del contexto. Por ejemplo, si se trata de demostrar la corrección de un programa para una aplicación crítica en seguridad, como el control de una central nuclear, está claro que se debe ser muy minucioso, sin dar nada por hecho. En esta asignatura se estudiarán demostraciones a distintos niveles: primero sólo a partir de las definiciones, y después utilizando propiedades ya demostradas previamente.

A continuación veremos algunos métodos de demostración.

4.1. Inducción

En su forma más sencilla el método de demostración por *inducción* dice que, para demostrar una propiedad para todos los números naturales, basta con demostrar que *a*) es cierta para 0, y *b*) para toda $i > 0$, si la propiedad es cierta para $i - 1$ entonces lo es para i.

Volviendo a nuestro ejemplo previo, la propiedad a demostrar es que, para todo natural n, todos los conjuntos con n elementos tienen 2^n subconjuntos distintos:

- El apartado *a*), llamado *caso base* de la inducción, se cumple, ya que $2^0 = 1$, y efectivamente $\emptyset$ tiene un único subconjunto, que es $\emptyset$.
- Veamos el apartado *b*), el llamado *caso de inducción*. Consideramos un conjunto $\{a_1, \ldots, a_i\}$. Podemos suponer que la propiedad se cumple para $i - 1$, esto es, el conjunto $\{a_1, \ldots, a_{i-1}\}$, que tiene $i - 1$ elementos, tiene 2^{i-1} subconjuntos; esta suposición es la llamada *hipótesis de inducción*. Por cada uno de estos 2^{i-1}

subconjuntos existen dos subconjuntos de $\{a_1, \ldots, a_i\}$, uno con a_i y otro sin él. Esto nos da un total de $2 \cdot 2^{i-1} = 2^i$ subconjuntos de $\{a_1, \ldots, a_i\}$, que es lo que queríamos demostrar en este apartado *b*).

Con los dos apartados concluídos, nuestra demostración por inducción está terminada.

Para entender por qué el caso base junto con el caso de inducción realmente implican la propiedad para todos los naturales, podemos pensar en lo que ocurre en una cadena de fichas de dominó colocadas verticalmente a poca distancia entre sí: si sabemos que si cae una ficha cae la siguiente (caso de inducción), basta con tirar la primera ficha (caso base) para que caigan todas.

También se pueden usar otras variantes de la inducción, como por ejemplo donde la propiedad se demuestra para los naturales a partir de un caso base mayor que 0, o por ejemplo donde en la hipótesis de inducción se supone que la propiedad se cumple para todo natural menor estrictamente que i.

4.2. Contrarrecíproco

El método de demostración por el *contrarrecíproco* sirve para propiedades de la forma "A implica B", es decir, para demostrar que si es cierta la propiedad A entonces también lo será la propiedad B. Para ello se demuestra "no B implica no A", es decir, que si B es falsa, entonces A también.

Veamos un ejemplo. Demostremos que si el cuadrado de un número natural n es par, entonces n es par. El contrarrecíproco dice que si n es impar, su cuadrado es impar. Como n es impar, es de la forma $2k+1$ para un cierto natural k. Luego $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$, y por lo tanto n^2 es impar.

4.3. Reducción al absurdo

Otro método de demostración es el de la *reducción al absurdo*: suponemos que la propiedad a demostrar es falsa y de allí deducimos un *absurdo* o *contradicción*, es decir, una situación imposible. Por lo tanto la propiedad no puede ser falsa.

Veamos un ejemplo. Queremos demostrar que $\sqrt{2}$ no es un número racional, es decir, que no existen naturales n y m tales que $\sqrt{2} = \frac{n}{m}$.

Supongamos que la propiedad a demostrar es falsa, es decir, que *sí* existen naturales n y m tales que $\sqrt{2} = \frac{n}{m}$. Si n y m son números pares, dividimos ambos números por 2. El resultado será otra fracción igual a $\sqrt{2}$. Repetimos esto hasta que al menos uno de los dos sea impar. Por eso, *sin pérdida de generalidad* podemos asumir que existen naturales n y m tales que $\sqrt{2} = \frac{n}{m}$, donde n es impar o m es impar.

Si $\sqrt{2} = \frac{n}{m}$, entonces elevando al cuadrado ambos lados de la igualdad obtenemos $2 = (\frac{n}{m})^2 = \frac{n^2}{m^2}$. Por lo tanto $n^2 = 2m^2$. Esto implica que n es par, ya que su cuadrado es par, como vimos antes por el contrarrecíproco.

Por otro lado, como n es par, tenemos $n = 2k$ para algún natural k. Entonces $n^2 = (2k)^2 = 4k^2$. Como también tenemos $n^2 = 2m^2$, tenemos $2m^2 = 4k^2$, es decir, $m^2 = 2k^2$. Como antes, m debe ser par porque su cuadrado es par.

Esto es una contradicción: por un lado habíamos visto que n es impar o m es impar, y por otro que los dos son pares. Hemos llegado a esta situación absurda mediante razonamientos correctos a partir de la suposición de que $\sqrt{2}$ es racional. Por lo tanto esa suposición debe ser falsa: $\sqrt{2}$ no es racional, como queríamos demostrar.