NÚMEROS REALES

JORGE A. GUCCIONE AND JUAN J. GUCCIONE

Contents

1 Monoides y grupos conmutativos

Un *monoide conmutativo* es un conjunto A dotado de una operación interna $*$, que es asociativa, conmutativa y tiene neutro. Así se satisface

(1) $(a * b) * c = a * (b * c)$ para todo $a, b, c \in A$,

(2) $a * b = b * a$ para todo $a, b, \in A$,

(3) existe $e \in A$ tal que $e * a = a$ para todo $a \in A$.

El neutro e de A es único, ya que si e' satisface la misma propiedad, entonces $e' = e * e' = e$, donde la primera igualdad se sigue de la propiedad de e y la segunda, de la propiedad de e'.

Por ejemplo el conjunto $\mathbb{N}$ de los números naturales con la operación de producto es un monoide comutativo, mientras que el conjunto $\mathbb{N}_0$ de los números naturales extendidos es un monoide, tanto con la operación de suma como con la de producto.

Un conjunto A puede tener muchas operaciones $*$ distintas que lo convierten en un monoide conmutativo. A pesar de eso muchas veces hablaremos simplemente del monoide conmutativo A cuando sea claro a que operación nos estamos refiriendo. En este caso seguiremos denotando también con A al conjunto subyacente de A.

Un elemento $a \in A$ es *inversible* si existe $b \in A$ tal que $a * b = e$. Este b es único pues si c satisface la misma propiedad, entonces $c = c * e = c * (a * b) = (c * a) * b = e * b = b$. Esto nos autoriza a denotar al inverso de a con a'.

Proposition 1.1. *En cada monoide conmutativo vale lo siguiente:*

(1) *e es inversible y $e' = e$.*

(2) *Si a es inversible a' también lo es y $(a')' = a$.*

(3) *Si a y b son inversible, entonces $a * b$ también lo es y $(a * b)' = a' * b'$.*

Proof. Los items (1) y (2) son triviales. Como

$$(b' * a') * (a * b) = b' * ((a' * a) * b) = b' * (e * b) = b' * b = e,$$

el item (3) también vale. □

Un *morfismo* de un monoide conmutativo A, llamado *dominio*, en otro B, llamado *codominio*, es un terna (A, B, f), donde $f\colon A \to B$, es una función que satisface

$$f(a_1 * a_2) = f(a_1) * f(a_2) \quad \text{para todo } a_1, a_2 \in A \qquad \text{y} \qquad f(e) = e,$$

donde e denota tanto al neutro de A como al de B. Notemos que tanto el dominio como el codominio son parte de la definición de morfismo. Sin embargo, cuando no haya posibilidad de confusión hablaremos simplemente de un morfismo $f\colon A \to B$. Valen las siguiente propiedades

(1) Para cada monoide conmutativo A, la identidad $I_A\colon A \to A$, definida por $I_A(a) \coloneqq a$, es un morfimo de monoides conmutativos.
(2) Si $f\colon A \to B$ y $g\colon B \to C$ son morfismos de monoides conmutativos, entonces también lo es la composición $g \circ f\colon A \to C$.
(3) Si $f\colon A \to B$ es un morfismo biyectivo de monoides conmutativos, entonces $f^{-1}\colon B \to A$ también lo es.

En efecto, la primera de estas propiedades es obvia, mientras que la segunda vale pues

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

Probemos la tercera afirmación. Como evidentemente $f^{-1}(e) = e$ sólo debemos probar que

$$f^{-1}(b_1 * b_2) = f^{-1}(b_1) * f^{-1}(b_2) \quad \text{para todo } b_1, b_2 \in B.$$

lo cual se sigue de que f es inyectivo y de que

$$f(f^{-1}(b_1 * b_2)) = b_1 * b_2 = f(f^{-1}(b_1)) * f(f^{-1}(b_2)) = f(f^{-1}(b_1) * f^{-1}(b_2)).$$

Proposition 1.2. *Si $f\colon A \to B$ es un morfismo de monoides conmutativos y $a \in A$ es inversible, entonces $f(a)$ también lo es y $f(a)' = f(a')$.*

Proof. Pues $f(a') * f(a) = f(a' * a) = f(e) = e$. □

Un *submonoide* de un monoide conmutativo A, es un subconjunto B de A que contiene al neutro e de A y que es cerrado para la operación de A. Claramente B, provisto de operación obtenida restringiendo la operación de A a B, es en si mismo un monoide conmutativo y la inclusión canónica de B en A es un morfismo de monoides conmutativos. Puede ocurrir que un elemento de B sea inversible en A, pero no en B. Por el contrario, si un elemento de B es inversible en B, entonces también lo es en A y con la misma inversa. Esto se sigue de la Proposición 1.2 aplicada a la inclusión canónica de B en A.

Se suelen usar dos notaciones para monoides conmutativos. La *aditiva*, en la que la operación se denota con $+$ y el neutro se denota con 0, y la *multiplicativa*, en la que la operación se denota simplemente con la yuxtaposición y el neutro con 1. En la notación aditiva al inverso de un elemento a se lo llama *opuesto* y se lo denota con $-a$, mientras que, en la notación multiplicativa, se lo denota con a^{-1}.

Un monoide conmutativo es un *grupo* si todos sus elementos son inversibles. Un *morfismo* de grupos conmutativos es un morfismo de monoides cuyo dominio y codominio son grupos conmutativos. Finalmente un subgrupo de un grupo G es un submonoide H de G que en si mismo es un grupo. Como hemos visto arriba, en este caso, la inversa de cada $h \in H$ en H, es también la inversa de h en G. En otras palabras, un subgrupo de un grupo conmutativo G es un submonoide de G, que con cada uno de sus elementos contiene a su inversa. Por ejemplo $\mathbb{Z}$ con la operación de suma es un grupo conmutativo y $\mathbb{N}_0$ es un submonoide (pero no un subgrupo) de $\mathbb{Z}$. El conjunto de los números pares es un subgrupo de $\mathbb{Z}$.

Para cada monoide A, el conjunto $U(A)$ de los elementos inversibles de A es un submonoide de A, que además es un grupo conmutativo, llamado el *grupo de unidades* de A. Por ejemplo $\mathbb{Z}$, con la operación de producto, es un monoide conmutativo cuyo grupo de unidades es $\{1, -1\}$.

2 Anillos conmutativos y cuerpos

Un *anillo conmutativo* es un conjunto provisto de dos operaciones, llamadas suma y producto, y denotadas de manera aditiva y multiplicativa respectivalente, tal que

(1) A con la suma es un grupo conmutativo, llamado el *grupo aditivo* de A.

(2) A con el producto es un monoide conmutativo, llamado el *monoide multiplicativo* de A.

(3) $a(b+c) = ab + ac$ para todo $a, b, c \in A$.

El conjunto $\{0\}$ dotado de la única suma y el único producto posibles es un anillo conmutativo, llamado 0. Otro ejemplo de anillo conmutativo es $\mathbb{Z}$, con la suma y el producto usuales.

Proposition 2.1. *En cada anillo conmutativo vale lo siguiente:*

(1) *Si $a + c = b + c$, entonces $a = b$.*

(2) *$a0 = 0$ para todo $a \in A$.*

(3) *$a(-b) = -ab$ y $(-a)(-b) = ab$ para todo $a, b \in A$.*

Proof. (1) Pues $a = a + 0 = (a + c) + (-c) = (b + c) + (-c) = b + 0 = b$.

(2) Por el item 1) y porque $0 + a0 = a(0 + 0) = a0 + a0$.

(3) Por que, debido al item (2), sabemos que $ab + a(-b) = a(b + (-b)) = a0 = 0$, de lo cual se sigue que $(-a)(-b) = -((-a)b) = -(-(ab)) = ab$. □

Puede ocurrir que en un anillo conmutativo A el 1 coincida con el 0, pero entonces, por el item (2) de la proposición anterior, $a = a1 = a0 = 0$, para todo $a \in A$, de modo que $A = 0$.

Un elemento a de un anillo conmutativo A es *divisor de cero* si existe $b \in A \setminus \{0\}$ tal que $ab = 0$. Es evidente que 1 no es divisor de cero y que 0 es divisor de cero si y sólo si $A \neq 0$. Para cada $a \in A$ son equivalentes:

(1) a no es divisor de cero.

(2) Si $ab = ac$, entonces $b = c$.

En efecto, es evidente que (2) implica (1) pues, en este caso, si $ab = 0$, entonces $ab = a0$ y, por lo tanto, $b = 0$. Supongamos recíprocamente que a no es divisor de cero y que $ab = ac$. Entonces $a(b - c) = 0$, de lo cual se sigue que $b = c$.

Proposition 2.2. *Para cada $a, b \in A$ son equivalentes:*

(1) *a y b no son divisores de cero.*

(2) *ab no es divisor de cero.*

Proof. En efecto, supongamos que (1) vale y que $abc = 0$. Como a no es divisor de cero, se sigue de esto que $bc = 0$. Por lo tanto, dado que b no es divisor de cero, obtenemos que $c = 0$. Esto prueba que ab no es divisor de cero. Supongamos ahora que vale (2) y que $bc = 0$. Entonces $(ab)c = a(bc) = a0 = 0$, de lo cual se sigue que $c = 0$ ya que ab no es divisor de cero. Esto prueba que b no es divisor de cero. Similarmente, a no es divisor de cero. □

Como 1 no es divisor de cero se sigue de la proposición anterior, que el conjunto de no divisores de cero de un anillo conmutativo A, es un submonoide del monoide multiplicativo de A.

Un elemento a de un anillo conmutativo A es *inversible* si lo es como elemento del monoide multiplicativo de A. Como ya vimos el conjunto de elementos inversible de A es un grupo $U(A)$, que llamaremos el *grupo de unidades* de A. Claramente 0 es inversible si y sólo si $1 = 0$. Notemos que si a es inversible, entonces a no es divisor de cero, pues, en este caso, de $ab = 0$, se sigue que $b = a^{-1}(ab) = a^{-1}0 = 0$.

Un anillo conmutativo A distinto de cero, es un *dominio* si no tiene divisores de cero no nulos, y es un *cuerpo* si todos sus elementos no nulos son inversibles. Es evidente un anillo conmutativo $A \neq 0$ es un dominio si y sólo si el conjunto $A \setminus \{0\}$ es cerrado por productos (es decir si y sólo si $A \setminus \{0\}$ es un submonoide del monoide multiplicativo de A), y es un cuerpo si y sólo si $U(A) = A \setminus \{0\}$. Por último, debido a lo que probamos arriba, todo cuerpo es un dominio.

Un *morfismo* de un anillo conmutativo A, llamado *dominio*, en otro B, llamado *codominio*, es un terna (A, B, f), donde $f\colon A \to B$, es una función que es un morfismo de grupos conmutativos para la suma y de monoides conmutativos para el producto. Notemos que tanto el dominio como el codominio son parte de la definición de morfismo de anillos conmuativos. Sin embargo, cuando no haya posibilidad de confusión hablaremos simplemente de un morfismo $f\colon A \to B$. Valen las siguiente propiedades

(1) Para cada anillo conmutativo A, la identidad $I_A\colon A \to A$, definida por $I_A(a) \coloneqq a$, es un morfimo de anillos comutativos.
(2) Si $f\colon A \to B$ y $g\colon B \to C$ son morfismos de anillos conmutativos, entonces también lo es la composición $g \circ f\colon A \to C$.
(3) Si $f\colon A \to B$ es un morfismo biyectivo de anillos conmutativos, entonces $f^{-1}\colon B \to A$ también lo es.

Un *subanillo* de un anillo conmutativo A, es un subconjunto B de A que es tanto un subgrupo del grupo aditivo de A como un submonoide del monoide multiplicativo de A. Claramente B, provisto de las operaciones obtenidas restringiendo las operaciones de A a B, es en si mismo un anillo conmutativo y la inclusión canónica de B en A es un morfismo de anillos conmutativos. Es evidente que un subanillo de un dominio es un dominio.

3 Anillo conmutativos ordenados

Un *anillo conmutativo ordenado* es un anillo conmutativo K provisto de un orden total que satisface:

(1) Si $a < b$, entonces $a + c < b + c$ para todo $c \in K$.
(2) Si $a < b$ y $0 < c$, entonces $ac < bc$.

Al primero de esto axiomas se lo llama *compatibilidad del orden con la suma*, mientras que al segundo se lo llama *compatibilidad del orden con el producto*.

Proposition 3.1. *Para cada $a, b \in K$ vale lo siguiente:*

$$a < b \Leftrightarrow 0 < b - a \Leftrightarrow -b < -a.$$

Proof. Sumando $-a$ a la desigualdad $a < b$, obtenemos que $0 < b - a$. Sumando ahora $-b$ a esta desigualdad, obtenemos que $-b < -a$. Por último, sumando $a + b$ a la desigualdad $-b < -a$, obtenemos que $a < b$. Por lo tanto las tres desigualdades del enunciado son equivalentes. □

Un número a es *positivo* si $0 < a$ y es *negativo* si $a < 0$. Denotemos con P al conjunto de los números positivos y con $-P$ al de los números negativos. De la proposición anterior se sigue en particular que $0 < a \Leftrightarrow -a < 0$, es decir, que $a \in P$ si y sólo si $-a \in -P$. Cada $a \in K \setminus \{0\}$ pertenece necesariamente a P o a $-P$, pero no a ambos. Así $K = P \cup -P \cup \{0\}$ y esta unión es disjunta.

Proposition 3.2. *Si $a < b$ y $c < d$, entonces $a + c < b + d$.*

Proof. Sumando c a la desigualdad $a < b$, obtenemos que $a + c < b + c$, mientras que, sumando b a la desigualdad $c < d$, obtenemos que $b + c < b + d$. Así, por la propiedad transitiva del orden, $a + c < b + d$. □

Corollary 3.3. *El conjunto P es cerrado por sumas.*

Proof. Aplicar la proposición anterior con $a = c = 0$. □

Proposition 3.4. *Si $a < b$ y $c < 0$, entonces $bc < ac$.*

Proof. Como vimos arriba de $c < 0$ se sigue $0 < -c$. Por lo tanto, debido a la compatibilidad del orden con el producto, $-ac < -bc$. Así, de la Proposición 3.1 se sigue que $bc < ac$. □

Proposition 3.5. *Si $0 \leq a < b$ y $0 \leq c < d$, entonces $0 \leq ac < bd$.*

Proof. Multiplicando las desigualdades $0 \leq a < b$ por c, obtenemos que $0 \leq ac \leq bc$, mientras que, multiplicando la desigualdad $c < d$ por b, obtenemos que $bc < bd$. Así, por la propiedad transitiva del orden, $0 \leq ac < bd$. □

Proposition 3.6. *Para cada par a, b, de elementos no nulos de K, vale lo siguiente:*

(1) *Si $a, b \in P$ o $a, b \in -P$, entonces $ab \in P$.*
(2) *Si $a \in P$ y $b \in -P$, entonces $ab \in -P$.*

Proof. (1) Si $0 < a$ y $0 < b$, entonces por la proposición anterior, $0 < ab$. Así, si $a, b \in P$, entonces $ab \in P$. Por otro lado, si $a, b \in -P$, entonces $-a, -b \in P$ y, por lo tanto, $ab = (-a)(-b) \in P$.

(2) Si $a \in P$ y $b \in -P$, entonces $a, -b \in P$ y, por lo tanto, $-ab = a(-b) \in P$. Así, $ab \in -P$. □

Corollary 3.7. *Todo anillo ordenado es un dominio.*

Proof. Si a y b son elementos no nulo de A, entonces los dos están en P, o uno de ellos está en P y el otro en $-P$, o los dos están en $-P$. Por la proposición anterior, en todos los casos el producto ab es distinto de cero. □

Corollary 3.8. *Las sumas de cuadrados de elementos no nulos de K están en P.*

Proof. Por la Proposición 3.6(1) y por el Corolario 3.3. □

En particular $1 = 1^2 \in P$. Es decir que $0 < 1$. Así $a < a + 1$ para todo $a \in A$. Por lo tanto

$$0 < 1 < 2 < 3 < 4 < 5 < \dots.$$

Proposition 3.9. *Tomemos $a \in K$ inversible. Entonces $a \in P$ si y sólo si $a^{-1} \in P$.*

Proof. De la Proposición 3.6 se sigue que si $a \in P$ y $a^{-1} \in -P$, entonces $1 = aa^{-1} \in -P$. Pero como acabamos de ver, esto es falso. Por lo tanto $a \in P$ si y sólo si $a^{-1} \in P$. □

Proposition 3.10. *Para cada par $a, b \in P$ de elementos inversibles vale lo siguiente:*

$$a < b \Leftrightarrow 1 < ba^{-1} \Leftrightarrow b^{-1} < a^{-1}.$$

Proof. Multiplicando por a^{-1} la desigualdad $a < b$, obtenemos que $1 < ba^{-1}$. Multiplicando ahora esta desigualdad por b^{-1}, obtenemos que $b^{-1} < a^{-1}$. Por último, multiplicando la desigualdad $b^{-1} < a^{-1}$ por ab, obtenemos que $a < b$. Por lo tanto las tres desigualdades del enunciado son equivalentes. □

Remark 3.11. Hemos visto que el subconjunto P de los números positivos de un orden total y compatible con la suma y el producto, definido sobre un anillo K, es cerrado por sumas y productos y que además K es la unión disjunta de P, $\{0\}$ y $-P \coloneqq \{x \in K : -x \in P\}$. Recíprocamente, cada subconjunto P de K, cerrado por la suma y el producto, y tal que K es la unión disjunta de P, $\{0\}$ y $-P$, determina un orden total y compatible con la suma y el producto, via $x < y$ si $y - x \in P$. Es fácil ver que estas construcciones son recíprocas una de la otra. Dejamos los detalles al lector.

Un subconjunto A de K es inductivo si $1 \in A$ y $a + 1 \in A$ para todo $a \in A$. Por ejemplo P es un subconjunto inductivo de K. En efecto, ya vimos que $1 \in P$ y del Corolario 3.3 se sigue inmediatamente que $a + 1 \in P$ para todo $a \in P$. Es fácil ver que la intersección de subconjuntos inductivos de K es un subconjunto inductivo de K. Por lo tanto hay un mínimo subconjunto inductivo de K, que es la intersección de todos los subconjuntos inductivos de K, y que denotaremos con $\mathbb{N}$. Como $a < a + 1$ para todo a, ningún subconjunto inductivo de K puede tener máximo.

Theorem 3.12. *Vale lo siguiente:*

(1) $\mathbb{N} \subseteq P$ *y* $1 \leq n$ *para todo* $n \in \mathbb{N}$.

(2) *Si* $m, n \in \mathbb{N}$, *entonces* $m + n \in \mathbb{N}$.

(3) *Si* $m, n \in \mathbb{N}$, *entonces* $mn \in \mathbb{N}$.

(4) *Si* $m, n \in \mathbb{N}$ *y* $m < n$, *entonces* $n - m \in \mathbb{N}$.

(5) *Si* $m, n \in \mathbb{N}$ *y* $m < n \leq m + 1$, *entonces* $n = m + 1$.

Proof. (1) Que $\mathbb{N} \subseteq P$ se sigue inmediatamente de que P es inductivo. Para ver la segunda afirmación basta probar que $\{a \in K : a \geq 1\}$ es un conjunto inductivo, lo que vale ya que si $a \geq 1$, entonces $a + 1 \geq 1$ debido a la Proposition 3.2 y a que $1 \geq 0$.

(2) Será suficiente probar que para cada m el conjunto $A \coloneqq \{n \in \mathbb{N} : m + n \in \mathbb{N}\}$ es inductivo. Veamos que esto es así. Como $m \in \mathbb{N}$ y $\mathbb{N}$ es inductivo, $m + 1 \in \mathbb{N}$. Por lo tanto $1 \in A$. En consecuencia para terminar la demostración sólo debemos ver que si $n \in A$, entonces $n + 1 \in A$. Pero $n \in A$ significa que $m + n \in \mathbb{N}$ y así, como $\mathbb{N}$ es inductivo, $m + n + 1 \in \mathbb{N}$, lo que significa que $n + 1 \in A$.

(3) Será suficiente probar que para cada m el conjunto $A \coloneqq \{n \in \mathbb{N} : mn \in \mathbb{N}\}$ es inductivo. Veamos que esto es así. Como $m1 = m$ e evidente que $1 \in A$. En consecuencia para terminar la demostración sólo debemos ver que si $n \in A$, entonces $n + 1 \in A$. Pero $n \in A$ significa que $mn \in \mathbb{N}$ y así, por el item (1), $m(n + 1) = mn + m \in \mathbb{N}$, lo que significa que $n + 1 \in A$.

(4) Probaremos primero el caso $m = 1$. Para ello bastará ver que el conjunto

$$A \coloneqq \{1\} \cup \{n \in \mathbb{N} : 1 < n \text{ y } n - 1 \in \mathbb{N}\}$$

es inductivo. Como obviamente $1 \in A$ sólo debemos probar que si $n \in A$, entonces $n + 1 \in A$. Pero esto es trivial porque $1 < n + 1$ y $(n + 1) - 1 = n \in A \subseteq \mathbb{N}$. A continuación probaremos el caso en que m es arbitrario. Para ello bastará ver que el conjunto

$$B \coloneqq \{m \in \mathbb{N} : n - m \in \mathbb{N} \text{ para todo } n > m \text{ con } n \in \mathbb{N}\}$$

es inductivo. Por lo que ya hemos probado $1 \in B$. Resta ver que si $m \in B$, entonces $m + 1 \in B$. Supongamos así que $m \in B$ y tomemos $n > m + 1$ en $\mathbb{N}$. Como $n > 1$ se sigue nuevamente de lo que ya hemos probado, que $n - 1 \in \mathbb{N}$. Como además $n - 1 > m$ y $m \in B$, obtenemos que $n - (m + 1) = (n - 1) - m \in \mathbb{N}$ y, en consecuencia, $m + 1 \in B$, como queremos.

(5) Debemos ver que el conjunto

$$A \coloneqq \{m \in \mathbb{N} : \text{si } n \in N \text{ y } m < n \leq m + 1, \text{ entonces } n = m + 1\}$$

es inductivo. Como evidentemente $\{1\} \cup \{a \in K : a \geq 2\}$ es inductivo, ya sabemos que $1 \in A$. Tomemos $m \in A$ y veamos que $m+1 \in A$. Supongamos que $n \in \mathbb{N}$ y que $m+1 < n \leq m+2$. Como $n > 1$ se sigue del item (4) que $n-1 \in \mathbb{N}$. Dado que además $m < n-1 \leq m+1$ y $m \in A$, obtenemos que $n-1 = m+1$ y, por lo tanto, $n = m+2$. Así $m+1 \in A$, como queremos. □

Denotemos con $\mathbb{N}_0$ al conjunto $\mathbb{N} \cup \{0\}$.

Theorem 3.13. *Vale lo siguiente:*

(1) $\mathbb{N} \subseteq P \cup \{0\}$ *y* $0 \leq n$ *para todo* $n \in \mathbb{N}_0$.
(2) *Si* $m, n \in \mathbb{N}_0$, *entonces* $m+n \in \mathbb{N}_0$.
(3) *Si* $m, n \in \mathbb{N}_0$, *entonces* $nm \in \mathbb{N}_0$.
(4) *Si* $m, n \in \mathbb{N}_0$ *y* $m \leq n$, *entonces* $n-m \in \mathbb{N}_0$.
(5) *Si* $m, n \in \mathbb{N}_0$ *y* $m < n \leq m+1$, *entonces* $n = m+1$.

Proof. (1) Por el item (1) del Teorema 3.12 y porque $0 < 1$.
(2) Por el item (2) del Teorema 3.12 y porque $n + 0 = n$ para todo $n \in \mathbb{N}_0$.
(3) Por el item (3) del Teorema 3.12 y porque $n0 = 0$ para todo $n \in \mathbb{N}_0$.
(4) Por el item (4) del Teorema 3.12 y porque $n - 0 = n$ y $n - n = 0$ para todo $n \in \mathbb{N}_0$.
(5) Por el item (5) del Teorema 3.12 y porque $0 < 1$. □

Consideremos un subconjunto Y de un conjunto parcialmente ordenado X. Decimos que un elemento $y \in Y$, es un elemento *minimal* de Y, si Y no tiene ningún elemento menor que y. Cuando X es totalmente ordenado, entonces Y no puede tener más de un elemento minimal, que, en caso de existir, será menor que todos los demás elementos de Y, y que llamaremos *mínimo* o *primer elemento* de Y. Similarmente decimos que un elemento $z \in Y$ es un elemento *maximal* de Y si no existe en Y ningún elemento que sea mayor que z. Analogamente a lo que ocurre con los elementos minimales, cuando X es totalmente ordenado, entonces Y no puede tener más de un elemento maximal, que en este caso de existir, llamaremos *máximo* o último elemento de Y, y que resultará ser mayor que todos los demás elementos de Y. Un conjunto totalmente ordenado X está bien ordenado si cada subconjunto no vacío Y de X tiene primer elemento.

Para cada $n \in \mathbb{N}_0$ denotamos con $\mathbb{I}_n^+$ al conjunto $\{i \in \mathbb{N}_0 : i \leq n\}$. Así $\mathbb{I}_0^+ = \{0\}$, $\mathbb{I}_1^+ = \{0, 1\}$, $\mathbb{I}_2^+ = \{0, 1, 2\}$, etcetera.

Theorem 3.14. *El conjunto* $\mathbb{N}_0$ *está bien ordenado.*

Proof. Tomemos $A \subseteq \mathbb{N}_0$ no vacío y consideremos el subconjunto X de $\mathbb{N}_0$ formado por los $n \in \mathbb{N}_0$ tales que $\mathbb{I}_n^+ \cap A = \emptyset$. Si $0 \in A$, entonces 0 es el primer elemento de A. Así podemos suponer que $0 \notin A$, lo que significa que $0 \in X$. Como $A \neq \emptyset$ existe $n \in A$ y así $n \notin X$. Por lo tanto $X \neq \mathbb{N}_0$ y como $0 \in X$, necesariamente existe $m \in \mathbb{N}_0$ tal que $m \in X$ y $m+1 \notin X$. Pero entonces $\mathbb{I}_m^+ \cap A = \emptyset$ y $\mathbb{I}_{m+1}^+ \cap A \neq \emptyset$, por lo que $m+1$ es el primer elemento de A. □

Theorem 3.15. *Si* $X \subseteq \mathbb{N}_0$ *es tal que* $0 \in X$ *y* $n+1 \in X$ *para cada* $n \in \mathbb{N}_0$ *tal que* $\mathbb{I}_n^+ \subseteq X$, *entonces* $X = \mathbb{N}_0$.

Proof. Debemos probar que $Y := \mathbb{N}_0 \setminus X$ es vacío. En caso contrario existiría un primer elemento $n \in Y$. Dado que $0 \in X$, necesariamente $n \in \mathbb{N}$. Así $\mathbb{I}_{n-1}^+ \subseteq X$ y $n = (n-1) + n \notin X$, lo que se contradice con la hipótesis. □

Denotemos con $\mathbb{Z}$ al conjunto $\mathbb{N}_0 \cup -\mathbb{N}$, donde $-\mathbb{N} := \{-n : n \in \mathbb{N}\}$. Notemos que esta unión es disjunta pues $\mathbb{N}_0 \subseteq P \cup \{0\}$, mientras que $-\mathbb{N} \subseteq -P$.

Theorem 3.16. *El mínimo subanillo de* K *es* $\mathbb{Z}$.

Proof. Supongamos que A es un subanillo de K. Como $0, 1 \in A$ y A es cerrado para la suma, $\mathbb{N}_0 \subseteq A$. Dado que además A es cerrado para la operación de tomar opuestos, también $-\mathbb{N} \subseteq A$ y, por lo tanto, $\mathbb{Z} \subseteq A$. Como $0, 1 \in \mathbb{Z}$ y $\mathbb{Z}$ es cerrado para la operación de tomar opuestos, para terminar la demostración sólo debemos ver que $\mathbb{Z}$ es cerrado para sumas y productos. Veamos primero que $\mathbb{Z}$ es cerrado para el producto. Tomemos $m, n \in \mathbb{Z}$. Ya sabemos que si $m, n \in \mathbb{N}_0$, entonces $mn \in \mathbb{N}_0$. Supongamos ahora que $m \in \mathbb{N}_0$ y $n \in -\mathbb{N}$. Entonces $m, -n \in \mathbb{N}_0$ y así $-mn = m(-n) \in \mathbb{N}_0$, de donde $mn \in \mathbb{Z}$. El caso en que $m \in -\mathbb{N}$ y $n \in \mathbb{N}_0$ se sigue del anterior y de que $mn = nm$. Finalmente si $m, n \in -\mathbb{N}$, entonces $-m, -n \in \mathbb{N}$ y, por lo tanto, $mn = (-m)(-n) \in \mathbb{N}$. Veamos ahora que $\mathbb{Z}$ es cerrado para la suma. Tomemos $m, n \in \mathbb{Z}$. Ya sabemos que si $m, n \in \mathbb{N}_0$, entonces $m + n \in \mathbb{N}_0$; y que si $m \in \mathbb{N}_0$, $n \in -\mathbb{N}$ y $-n \leq m$, entonces $m + n = m - (-n) \in \mathbb{N}_0$. Supongamos ahora que $m \in \mathbb{N}_0$, que $n \in -\mathbb{N}$ y que $m < -n$. Si $m = 0$, entonces evidentemente $m + n \in -\mathbb{N}$. En caso contrario, $-n \in \mathbb{N}$, $-m \in -\mathbb{N}$, $m \leq -n$ y, en consecuencia, por lo que ya hemos visto, $m + n = -((-n) - m) \in -\mathbb{N} \cup \{0\}$. Hemos probado que si $m \in \mathbb{N}_0$ y $n \in \mathbb{Z}$, entonces $m + n \in \mathbb{Z}$. Finalmente, si $m \in -\mathbb{N}$ y $n \in \mathbb{Z}$, entonces $-m \in \mathbb{N}$ y, por lo que acabamos de probar, $m + n = -(-m - n) \in \mathbb{Z}$. □

Remark 3.17. Todo subconjunto no vacío Y de $\mathbb{Z}$ y que está acotado inferiormente en $\mathbb{Z}$ tiene primer elemento. En efecto supongamos que $n_0 \in \mathbb{Z}$ es una cota inferior de Y. Entonces el conjunto $Y' \coloneqq \{n - n_0 : n \in Y\}$ está incluído en $\mathbb{N}_0$ y, por lo tanto, tiene primer elemento n'_0. Entonces $n'_0 + n_0 \in Y$ y es el primer elemento de Y.

Definition 3.18. En cada monoide conmutativo y multiplicativo A, definimos a^n para $a \in A$ y $n \in \mathbb{N}_0$, recursivamente por $a^0 \coloneqq 1$ y $a^{n+1} \coloneqq a^n a$ para todo $n \in \mathbb{N}_0$.

Proposition 3.19. *En cada monoide conmutativo y multiplicativo A vale lo siguiente:*

(1) $a^{m+n} = a^m a^n$ *para todo* $a \in A$ *y todo* $m, n \in \mathbb{N}_0$.
(2) $(a^m)^n = a^{mn}$ *para todo* $a \in A$ *y todo* $m, n \in \mathbb{N}_0$.
(3) $(ab)^m = a^m b^m$ *para todo* $a, b \in A$ *y todo* $m \in \mathbb{N}_0$.
(4) *Si* a *es inversible, entonces* a^m *es inversible y* $(a^m)^{-1} = (a^{-1})^m$ *para todo* $m \in \mathbb{N}_0$.

Proof. (1) Fijemos $m \in \mathbb{N}_0$. Cuando $n = 0$ la igualdad del enunciado es trivial. Veamos que vale para todo $n \in \mathbb{N}$. Para ello es suficiente probar que el conjunto $X \coloneqq \{n \in \mathbb{N} : a^{m+n} = a^m a^n\}$ es inductivo. Es evidente que $1 \in X$. Supongamos que $n \in X$. Entonces

$$a^{m+(n+1)} \coloneqq a^{m+n} a = (a^m a^n) a = a^m (a^n a) = a^m a^{(n+1)},$$

por lo que $n + 1 \in X$.

(2) Fijemos $m \in \mathbb{N}_0$. Cuando $n = 0$ la igualdad del enunciado es trivial. Veamos que vale para todo $n \in \mathbb{N}$. Para ello es suficiente probar que el conjunto $X \coloneqq \{n \in \mathbb{N} : (a^m)^n = a^{mn}\}$ es inductivo. Es evidente que $1 \in X$. Supongamos que $n \in X$. Entonces

$$(a^m)^{n+1} \coloneqq (a^m)^n a^m = a^{mn} a^m = a^{mn+m} = a^{m(n+1)},$$

por lo que $n + 1 \in X$.

(3) Fijemos $n \in \mathbb{N}_0$. Cuando $m = 0$ la igualdad del enunciado es trivial. Veamos que vale para todo $m \in \mathbb{N}$. Para ello es suficiente probar que el conjunto $X \coloneqq \{m \in \mathbb{N} : (ab)^m = a^m b^m\}$ es inductivo. Es evidente que $1 \in X$. Supongamos que $m \in X$. Entonces

$$(ab)^{m+1} \coloneqq (ab)^m ab = a^m b^m ab = a^m a b^m b = a^{m+1} b^{m+1},$$

por lo que $m + 1 \in X$.

(4) Pues, por el item (3), tenemos $a^m (a^{-1})^m = (a a^{-1})^m = 1^m = 1$. □

Definition 3.20. En cada grupo conmutativo y multiplicativo A, definimos a^{-n} para $a \in A$ y $n \in \mathbb{N}$, por $a^{-n} \coloneqq (a^n)^{-1}$.

Proposition 3.21. *En cada grupo conmutativo y multiplicativo A vale lo siguiente:*

(1) $a^{m+n} = a^m a^n$ *para todo* $a \in A$ *y todo* $m, n \in \mathbb{Z}$.

(2) $(a^m)^n = a^{mn}$ *para todo* $a \in A$ *y todo* $m, n \in \mathbb{Z}$.

(3) $(ab)^m = a^m b^m$ *para todo* $a, b \in A$ *y todo* $m \in \mathbb{Z}$.

(4) $(a^m)^{-1} = (a^{-1})^m$ *para todo* $m \in \mathbb{Z}$.

Proof. (1) El caso en $m, n \in \mathbb{N}_0$ ya fue probado antes. Supongamos que $m \in \mathbb{N}_0$, $n \in -\mathbb{N}$ y $m + n \in \mathbb{N}_0$. Entonces $a^{m+n}a^{-n} = a^m$, por lo que $a^{m+n} = a^m a^n$. Supongamos ahora que $m \in \mathbb{N}_0$, $n \in -\mathbb{N}$ y $m + n \in -\mathbb{N}$. Entonces $a^{-n} = a^m a^{-(m+n)}$, de donde $a^{m+n} = a^m a^n$. Finalmente si $m, n \in -\mathbb{N}$, entonces $a^{-n}a^{-m} = a^{-(m+n)}$, lo cual implica que $a^{m+n} = a^m a^n$.

(2) El caso en $m, n \in \mathbb{N}_0$ ya fue probado antes. Supongamos que $m \in \mathbb{N}_0$ y $n \in -\mathbb{N}$. Entonces $(a^m)^{-n} = a^{-mn}$, de donde tomando inversos, obtenemos que $(a^m)^n = a^{mn}$. Supongamos ahora que $m \in -\mathbb{N}$ y $n \in \mathbb{N}_0$. Entonces $(a^{-m})^n = a^{-mn}$, de donde por el item (4) de la Proposition 3.19, tomando inversos obtenemos que $a^{mn} = ((a^{-m})^{-1})^n = (a^m)^n$. Finalmente, si $m, n \in -\mathbb{N}$, entonces $(a^{-m})^{-n} = a^{(-m)(-n)} = a^{mn}$, lo que, nuevamente por el item (4) de la Proposition 3.19, implica que $a^{mn} = ((a^{-m})^{-1})^n = (a^m)^n$.

(3) El caso en $m \in \mathbb{N}_0$ fue considerado en la Proposition 3.19(3). Supongamos que $m \in -\mathbb{N}$. Entonces $(ab)^{-m} = a^{-m}b^{-m}$, por lo que, tomando inversos obtenemos que $(ab)^m = a^m b^m$.

(4) Pues, por el item (3), tenemos $a^m(a^{-1})^m = (aa^{-1})^m = 1^m = 1$. □

Una función $f\colon A \to B$ entre conjunto ordenado A y B es *estrictamente creciente* si de $a < a'$ se sigue que $f(a) < f(a')$.

Proposition 3.22. *Consideremos un anillo conmutativo ordenado K y denotemos con P al conjunto de sus números positivos. Para cada $n \in \mathbb{N}$ la función $f_n\colon P \cup \{0\} \to P \cup \{0\}$, definida por $f_n(a) \coloneqq a^n$, es estrictamente creciente.*

Proof. Será suficiente ver que $X \coloneqq \{n \in \mathbb{N} : a^n < b^n$ para todo $a < b$ en $P_0\}$ es inductivo. Es obvio que $1 \in X$. Supongamos que $n \in X$. Entonces $0 \leq a^n < b^n$ para cada $a < b$ en P y, así, se sigue de la Proposición 3.5, que $0 \leq a^{n+1} < b^{n+1}$, por lo que $n + 1 \in X$, como queremos. □

Remark 3.23. Consideremos un anillo conmutativo ordenado K y tomemos $a > 0$ en K.

- Si $a < 1$, entonces $a^{n+1} < a^n$ para todo $n \in \mathbb{N}$.
- Si $a > 1$, entonces $a^{n+1} > a^n$ para todo $n \in \mathbb{N}$.

En efecto, la primera afirmación se sigue multiplicando la desigualdad $a < 1$ por a^n y la segunda es similar.

Proposition 3.24 (Desigualdad de Bernoulli)**.** *Si $x \geq -1$ y $n \in \mathbb{N}_0$, entonces $(1+x)^n \geq 1+nx$.*

Proof. Procedemos por inducción sobre n. Los casos $n = 0$ y $n = 1$ son triviales. Supongamos por hipótesis inductiva que $(1+x)^n \geq 1+nx$. Dado que $1+x \geq 0$, se sigue de la compatibilidad del orden con el producto que

$$(1+x)^{n+1} = (1+x)^n(1+x) \geq (1+nx)(1+x) = 1 + nx + x + nx^2 \geq 1 + (n+1)x,$$

como queremos. □

Definition 3.25. Definimos el valor absoluto $|x|$ de un elemento $x \in K$, por $|x| = \max\{x, -x\}$. Por lo tanto $|x| = x$ si $x \in P \cup \{0\}$ y $|x| = -x$ si $x \in -P$.

Tomemos $a, b, x \in K$. Claramente

$$a - b \leq x \leq a + b \Leftrightarrow -b \leq x - a \leq b \Leftrightarrow |x - a| \leq b,$$

y lo mismo vale con $\leq$ reemplazado por $<$.

Theorem 3.26. *Vale lo siguiente:*

(1) $|x + y| \leq |x| + |y|$.
(2) $|xy| = |x||y|$.
(3) $||x| - |y|| \leq |x - y|$.

Proof. (1) Como $-|x| \leq x \leq |x|$ y $-|y| \leq y \leq |y|$ se sigue de la Proposition 3.2, que

$$-|x| - |y| \leq x + y \leq |x| + |y|.$$

Así $|x + y| \leq |x| + |y|$.
(2) Si $x, y \in P \cup \{0\}$, entonces $|x||y| = xy = |xy|$, donde la última igualdad se sigue de la Proposición 3.6(1). Si $x \in P \cup \{0\}$ e $y \in -P$, entonces $|x||y| = x(-y) = -(xy) = |xy|$, donde la última igualdad se sigue de la Proposición 3.6(2). El caso en que $x \in -P$ e $y \in P \cup \{0\}$ se sigue del caso anterior y de que $|x||y| = |y||x|$ y $|xy| = |yx|$. Finalmente, si $x, y \in -P$, entonces $|x||y| = (-x)(-y) = |xy|$, donde la última igualdad se sigue nuevamente de la Proposición 3.6(1).
(3) Del item (1) se sigue que $|x| \leq |x - y| + |y|$ e $|y| \leq |y - x| + |x|$. Así $|x| - |y| \leq |x - y|$ y $|y| - |x| \leq |y - x|$. Como $|y - x| = |x - y|$, se sigue de esto que $||x| - |y|| \leq |x - y|$. □

4 Cuerpos ordenados

Un cuerpo ordenado es un anillo conmutativo ordenado que es un cuerpo. Dado un cuerpo ordenado K consideremos el subconjunto $\mathbb{Q}$ de K definido por $\mathbb{Q} := \{pq^{-1} : p \in \mathbb{Z} \text{ y } q \in \mathbb{N}\}$.

Theorem 4.1. *Consideremos un cuerpo ordenado K. El mínimo subcuerpo de K es $\mathbb{Q}$.*

Proof. Supongamos que A es un subcuerpo de K. Como $\mathbb{Z}$ es el mínimo subanillo de K, claramente $\mathbb{Z} \subseteq A$. Pero entonces, como A es un cuerpo $q^{-1} \in A$, para todo $q \in \mathbb{N}$ y, en consecuencia, $pq^{-1} \in A$ para todo $p \in \mathbb{Z}$ y todo $q \in \mathbb{N}$. Por lo tanto $\mathbb{Q} \subseteq K$. Para terminar la demostración debemos probar que $\mathbb{Q}$ es cerrado por sumas y productos y que cada elemento no nulo de $\mathbb{Q}$ tiene inverso en $\mathbb{Q}$. Que $\mathbb{Q}$ es cerrado por suma y producto se sigue de que

$$pq^{-1} + rs^{-1} = psq^{-1}s^{-1} + qrq^{-1}s^{-1} = (ps + qr)(qs)^{-1} \quad \text{y} \quad pq^{-1}rs^{-1} = (pr)(qs)^{-1}.$$

Veamos finalmente que que cada elemento no nulo de $\mathbb{Q}$ es inversible en $\mathbb{Q}$. Para ello tomemos $p \in \mathbb{Z}$ y $q \in \mathbb{N}$ tales que $pq^{-1} \neq 0$. Entonces $p \neq 0$, y si $p \in P$, entonces $qp^{-1} \in \mathbb{Q}$ es la inversa de pq^{-1}; mientras que si $p \in -P$, entonces $(-q)(-p)^{-1} \in \mathbb{Q}$ es la inversa de pq^{-1}. En efecto, esto se sigue de que, en el primer caso, $pq^{-1}qp^{-1} = pp^{-1} = 1$; mientras que, en el segundo caso, $pq^{-1}(-q)(-p)^{-1} = pq^{-1}(-1)q(-1)^{-1}p^{-1} = pq^{-1}qp^{-1} = 1$. □

Remark 4.2. Para cada par $x < y$, de elementos de $\mathbb{Q}$, tenemos $x < (x + y)/2 < y$. En efecto sumando x a la desigualdad $x < y$ obtenemos $2x < x + y$ y similarmente sumando y a la desigualdad $x < y$ obtenemos $x + y < 2y$. En consecuencia $2x < x + y < 2y$. Multiplicando por $1/2$ esta desigualdad y usando que $0 < 1/2$, obtenemos que $x < (x + y)/2 < y$. En particular, entre dos números racionales siempre hay otro número racional. Notemos que $z := (x + y)/2$ es el punto medio de x e y (es decir que $y - z = z - x$).

Un subconjunto Y de un conjunto totalmente ordenado X está *acotado superiormente* si existe $z \in X$ tal que $y \leq z$ para todo $y \in Y$. A este elemento z se lo denomina una *cota superior* de Y.

Una cota superior de Y se llama *supremo* de Y si es una cota superior mínima. Obviamente un supremo si existe es único. Notemos que para z en Y son equivalentes

(1) z es el máximo de Y,

(2) z es el supremo de Y,

(3) z es una cota superior de Y.

Similarmente decimos que Y está *acotado inferiormente* si existe $z \in X$ tal que $z \leq y$ para todo $y \in Y$. A este elemento z se lo denomina una *cota inferior* de Y. Una cota inferior de Y se llama *ínfimo* de Y si es una cota inferior máxima. Obviamente un ínfimo si existe es único. Notemos que para z en Y son equivalentes

(1) z es el mínimo de Y,

(2) z es el ínfimo de Y,

(3) z es una cota inferior de Y.

Theorem 4.3. *Para cada cuerpo ordenado las siguientes afirmaciones son equivalentes:*

(1) $\mathbb{N}$ *no está acotado superiormente.*

(2) *Para cada par de elementos* $y, z \in K$ *con* $y > 0$ *existe* $n \in \mathbb{N}$ *tal que* $z < ny$.

(3) *Para cada* $y > 0$ *en* K *existe* $n \in \mathbb{N}$ *tal que* $\frac{1}{n} < y$.

Proof. (1) $\Rightarrow$ (2) Como $\mathbb{N}$ no está acotado superiormente existe $n \in \mathbb{N}$ tal que $\frac{z}{y} < n$. Dado que $y > 0$ se sigue de esto que $z < ny$.

(2) $\Rightarrow$ (3) Por hipótesis existe $n \in \mathbb{N}$ tal que $ny > 1$. Por lo tanto $\frac{1}{n} < y$.

(3) $\Rightarrow$ (1) Por hipótesis para cada $y > 0$ existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < \frac{1}{y}$. Por lo tanto $n > y$. Esto muestra que ningún número positivo de K es una cota superior de $\mathbb{N}$. Es obvio que de esto se sigue que el item (1) vale. □

Un cuerpo ordenado es arquimediano si satisface las propiedades equivalentes del teorema anterior.

Existen cuerpos K que no son arquimedianos, es decir cuerpos en los que el conjunto $\mathbb{N}$, de los números naturales, está acotado. Uno de ellos es el cuerpo de funciones racionales $\mathbb{Q}(X)$, con el orden obtenido definiendo el conjunto P de las fracciones positivas por: $\frac{p(x)}{q(x)} \in P$ si el coeficiente principal de $p(x)q(x)$ es positivo. Es obvio que $n < x$ para todo $n \in \mathbb{N}$. Si bien el conjunto de los números naturales puede estar acotado en K, lo que no puede ocurrir es que tenga supremo. Porque si s es el supremo de $\mathbb{N}$ en K, entonces existe $n \in \mathbb{N}$ tal que $s - 1 < n$ (porque $s - 1 < s$) y, así $s < n + 1$, lo que se contradice con el hecho de que s es cota superior de $\mathbb{N}$.

Definition 4.4. Un subconjunto A de un cuerpo ordenado es *denso* en K si para todo $x < y$ en K existe $z \in A$ tal que $x < z < y$.

Theorem 4.5. *Si* K *es un cuerpo ordenado arquimediano, entonces* $\mathbb{Q}$ *es denso en* K.

Proof. Debemos ver que para cada $x < y$ en K, existe $z \in \mathbb{Q}$ tal que $x < z < y$. Dado que K es arquimediano existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < y - x$. Consideremos el conjunto $Y \coloneqq \{m \in \mathbb{Z} : yn \leq m\}$. Por la Nota 3.17 el conjunto Y tiene un primer elemento m_0. Como $m_0 - 1 < m_0$, necesariamente $m_0 - 1 < yn$. Afirmamos que $xn < m_0 - 1$. En efecto, en caso contrario, $m_0 - 1 \leq xn < yn \leq m_0$, lo que es imposible pues $1 < (y - x)n$. En consecuencia, $x < \frac{m_0 - 1}{n} < y$, como queremos. □

5 Cuerpos ordenados completos

Theorem 5.1. *Para cada conjunto totalmente ordenado X las siguientes afirmaciones son equivalentes:*

(1) *Todo subconjunto no vacío y acotado superiormente de X tiene supremo.*

(2) *Todo subconjunto no vacío y acotado inferiormente de X tiene ínfimo.*

Proof. (1) $\Rightarrow$ (2) Supongamos que Y es un subconjunto no vacío y acotado inferiormente de X. Denotemos con Z al conjunto de las cotas inferiores de Y. Por hipótesis $Z \neq \emptyset$ y además todos los elementos de Y son cotas superiores de Z. Nuevamente por hipótesis Z tiene supremo w. Así, por un lado $w \leq y$ para todo $y \in Y$ (pues estos y son cotas superiores de Z y w es el supremos de Z), de manera que z es una cota inferior de Y; mientras que, por otro lado, si z es una cota inferior de Y, entonces $z \in Z$ y, por lo tanto, $z \leq w$, lo que muestra que w es el ínfimo de Y.
(2) $\Rightarrow$ (1) Es similar a la prueba de que (1) $\Rightarrow$ (2). □

Un conjunto totalmente ordenado es *completo* si satisface las propiedades equivalentes del teorema anterior. Un cuerpo ordenado es *completo* si lo es como conjunto ordenado. Por el comentario al final de la subsección anterior, todo cuerpo ordenado completo es arquimediano.

A continuación vamos a probar que en todo cuerpo ordenado completo los núneros positivos tiene raíces cuadradas.

Theorem 5.2. *Supongamos que K es un cuerpo ordenado completo. Entonces, para cada $a > 0$ en K existe un único $b > 0$ en K, tal que $b^2 = a$.*

Proof. Por la Proposition 3.22 existe a lo sumo un único $b \in P$ tal que $b^2 = a$. Veamos ahora que efectivamente existe un tal b. Escribamos $X_a := \{x \geq 0 : x^2 < a\}$ e $Y_a := \{x \geq 0 : x^2 > a\}$. Estos conjunto no son vacíos pues $0 \in X_a$ y $a + 1 \in Y_a$ (si $a \leq 1$, entonces $(a+1)^2 > 1^2 > a$ y si $a > 1$, entonces $(1+a)^2 > a^2 > a$). Además si $x \in X_a$ e $y \in Y_a$ entonces $x < y$ (pues si $y < x$, entonces $y^2 < x^2$, lo que se contradice con que $x^2 < a$ e $y^2 > a$). En particular X_a está acotado superiormente. Denotemos con b al supremo de X_a. Afirmamos que $b^2 = a$. Haremos esto por el absurdo. Supongamos primero que $b^2 < a$ (en otras palabras que $b \in X_a$). Vamos a ver que entonces existe $\epsilon > 0$ en $\mathbb{Q}$ tal que $b + \epsilon \in X_a$ (lo que es imposible pues se contradice con el hecho de que b es el supremo de X_a). Debemos ver así que podemos elegir $\epsilon > 0$ en $\mathbb{Q}$ tal que $(b+\epsilon)^2 < a$. Tomemos $0 < \epsilon < \min(1, (a - b^2)/(2b + 1))$. Entonces

$$(b+\epsilon)^2 = b^2 + 2\epsilon b + \epsilon^2 < b^2 + 2\epsilon b + \epsilon = b^2 + \epsilon(2b+1) < b^2 + a - b^2 = a,$$

como queremos. En consecuencia necesariamente $b^2 \geq a$. Así para terminar la demostración sólo debemos ver que $b^2 > a$ es imposible. Vamos a ver que entonces existe $\epsilon > 0$ en $\mathbb{Q}$ tal que $b - \epsilon \in Y_a$ (lo que es imposible pues como los elementos de Y_a son cotas superiores de X_a con esto se contradice que b es el supremo de X_a). Debemos ver así que podemos elegir $\epsilon > 0$ en $\mathbb{Q}$ tal que $(b-\epsilon)^2 > a$. Tomemos $0 < \epsilon < (b^2 - a)/2b$. Entonces

$$(b-\epsilon)^2 = b^2 - 2\epsilon b + \epsilon^2 > b^2 - 2\epsilon b > b^2 - (b^2 - a) = a,$$

nuevamente como queremos. □

Nuestro próximo objetivo es probar que dos cuerpos ordenados completos K y K' son canónicamente isomorfos (concretamente vamos a ver que hay un único morfismo de K en K', y que además este morfismo es un isomorfismo que respeta el orden). Notemos para empezar que si K y K' son cuerpos ordenados, K es completo y $f\colon K \to K'$ es un morfismo de cuerpos, entonces f respeta el orden. En efecto si $a < b \in K$, entonces existe $c \in P$ tal que $b - a = c^2$. Por lo tanto $f(b) - f(a) = f(c)^2 > 0$ y, en consecuencia, $f(a) < f(b)$. Así sólo debemos probar que si K y K' son cuerpos ordenados completos, entonces hay un único morfismo de K en K' de cuerpos

ordenados, y que además este morfismo es un isomorfismo. Comenzaremos con los siguientes resultados.

Proposition 5.3. *Consideremos dos cuerpos ordenado K y K' y denotemos con $\mathbb{Q}$ al mínimo subanillo de K. Supongamos que K es arquimediano y que $f\colon \mathbb{Q} \to K'$ es una función creciente. Entonces vale lo siguiente:*

(1) *Si K' es completo, entonces existe una función creciente $\overline{f}\colon K \to K'$ que extiende a f.*
(2) *Si $\overline{f}\colon K \to K'$ extiende a f y f es estrictamente creciente, entonces $\overline{f}$ también lo es.*
(3) *Si $f(\mathbb{Q})$ es denso en K', entonces existe a lo sumo una función creciente de K en K' que extiende a f.*

Proof. (1) Para cada $a \in K$ escribamos con

$$D_a \coloneqq \{q \in \mathbb{Q} : q \leq a\} \qquad \text{y} \qquad f(D_a) \coloneqq \{f(q) : q \in \mathbb{Q} \text{ y } q \leq a\}.$$

Es evidente que $f(D_a)$ no es vacío. Afirmamos que $f(D_a)$ está acotado superiormente. En efecto, si $q' \in \mathbb{Q}$ es tal que $a \leq q'$, entonces $f(q) \leq f(q')$ para cada $q \in D_a$ y, por lo tanto, $f(q')$ es una cota superior de $f(D_a)$. En consecuencia, dado que K' es completo, $f(D_a)$ tiene supremo. Definimos la función $\overline{f}$ por $\overline{f}(a) \coloneqq \sup f(D_a)$. Notemos ahora que, como f es creciente,

$$\overline{f}(q') = \sup f(D_{q'}) = \sup\{f(q) : q \in \mathbb{Q} \text{ y } q \leq q'\} = f(q') \quad \text{para todo } q' \in \mathbb{Q}.$$

Además es evidente que si $a < a'$, entonces

$$\overline{f}(a) = \sup f(D_a) \leq \sup f(D_{a'}) = \overline{f}(a'),$$

ya que $D_a \subseteq D_{a'}$.

(2) Tomemos $a < a'$ en K. Por hipótesis existen $q < q'$ en $\mathbb{Q}$ tales que $a \leq q < q' \leq a'$. En consecuencia

$$\overline{f}(a) \leq \overline{f}(q) = f(q) < f(q') = \overline{f}(q') \leq \overline{f}(a'),$$

por lo que $\overline{f}$ es estrictamente creciente.

(3) Supongamos que $\overline{f}\colon K \to K'$ es una función creciente que extiende a f. Para cada $a \in K$ escribamos

$$f(D_a) \coloneqq \{f(q) : q \in \mathbb{Q} \text{ y } q \leq a\} \quad \text{y} \quad D_a^f \coloneqq \{f(q) : q \in \mathbb{Q} \text{ y } f(q) \leq \overline{f}(a)\}.$$

Es evidente que $f(D_a) \subseteq D_a^f$ ya que si $q \in D_a$, entonces $f(q) = \overline{f}(q) \leq \overline{f}(a)$. Por lo tanto

$$\sup f(D_a) \leq \sup D_a^f = \overline{f}(a),$$

donde la última igualdad se sigue de $f(\mathbb{Q})$ es denso en K'. En consecuencia, para terminar la demostración bastará ver que $\sup f(D_a) = \sup D_a^f$ (porque esto mostrará que $\overline{f}$ está determinada por f). Supongamos que $\sup f(D_a) < \overline{f}(a)$. Dado que $f(\mathbb{Q})$ es denso en K' existe $q \in \mathbb{Q}$ tal que $\sup f(D_a) < f(q) < \overline{f}(a)$. Entonces, por la definición de $f(D_a)$, necesariamente $a < q$. Así, como $\overline{f}$ es creciente, $\overline{f}(a) \leq \overline{f}(q) = f(q)$, lo que es una contradicción. □

Para cada par de subconjuntos A y B de un anillo K, escribimos

$$A + B \coloneqq \{a + b : a \in A \text{ y } b \in B\} \qquad \text{y} \qquad AB \coloneqq \{ab : a \in A \text{ y } b \in B\}.$$

Lemma 5.4. *Consideremos un cuerpo ordenado completo K.*

- *Para cada $a \in K$ escribamos $D_a \coloneqq \{q \in \mathbb{Q} : q \leq a\}$.*
- *Para cada $a \in P$ escribamos $D_a^+ \coloneqq \{q \in \mathbb{Q} : 0 < q \leq a\}$.*

Se satisfacen las siguientes afirmaciones:

(1) *$a + b = \sup(D_a + D_b)$ para todo $a, b \in K$.*
(2) *$ab = \sup(D_a^+ D_b^+)$ para todo $a, b \in P$.*

Proof. (1) Claramente $a+b$ es una cota superior de $D_a + D_b$. Para terminar la demostración debemos ver que si c es una cota superior de $D_a + D_b$, entonces $a+b \leq c$. Tomemos $n \in \mathbb{N}$. Como $\mathbb{Q}$ es denso en K existen $x \in D_a$ e $y \in D_b$ tales que $a - 1/2n < x$ y $b - 1/2n < y$. Por lo tanto $a + b - 1/n < x + y$ y así $a + b - 1/n < c$, lo que implica que $a + b \leq c$ (si $c < a + b$, entonces existen $u < v$ en $\mathbb{Q}$ tales que $c \leq u < v \leq a + b$ y así, si $n \in \mathbb{N}$ es tal que $1/n < v - u$, entonces $c < a + b - 1/n$).

(2) Claramente ab es una cota superior de $D_a^+ D_b^+$. Para terminar la demostración debemos ver que si c es una cota superior de $D_a^+ D_b^+$, entonces $ab \leq c$. Tomemos $n \in \mathbb{N}$ arbitrario. Afirmamos que existen $x \in D_a^+$ e $y \in D_b^+$ tales que $ab - 1/n < xy$. En efecto, dado que $\mathbb{Q}$ es denso en K, cualquiera sea $m \in \mathbb{N}$, existen $x \in D_a^+$ e $y \in D_b^+$ tales que $a - 1/m < x$ y $b - 1/m < y$ y, en consecuencia, para verificar que vale lo afirmado, bastará ver que se puede elejir m de modo que $ab - 1/n < (a - 1/m)(b - 1/m)$. Pero esto es así, pues

$$ab - \frac{1}{n} < \Big(a - \frac{1}{m}\Big)\Big(b - \frac{1}{m}\Big) \Leftrightarrow -\frac{1}{n} < -\frac{a+b}{m} + \frac{1}{m^2} \Leftrightarrow \frac{a+b}{m} < \frac{1}{n} + \frac{1}{m^2},$$

y, por lo tanto, basta tomar $m > (a+b)n$. Notemos ahora que de la existencia de $x \in D_a^+$ e $y \in D_b^+$ tales que $ab - 1/n < xy$ se sigue que $ab - 1/n < c$ y, que como n es arbitrario, de esto se sigue a su vez que $ab \leq c$. □

En la siguiente nota establecemos el resultado de unicidad prometido.

Remark 5.5. Consideremos dos cuerpos ordenados completos K y K' y denotemos con $\mathbb{Q}$ y $\mathbb{Q}'$ a los mínimos subanillos de K y K' respectivamente. Es fácil ver que hay un único morfismo de cuerpos $f\colon \mathbb{Q} \to \mathbb{Q}'$ y que este morfismo es un isomorfismo de cuerpos ordenados. Denotemos con $g\colon \mathbb{Q}' \to \mathbb{Q}$ a la inversa de f. Por la Proposition 5.3 los isomorfismos f y g se extienden de manera única a funciones estrictamente crecientes $\overline{f}\colon K \to K'$ y $\overline{g}\colon K' \to K$. Como $\overline{g} \circ \overline{f}\colon K \to K$ extiende a la identidad de $\mathbb{Q}$ necesariamente $\overline{g} \circ \overline{f} = \mathrm{id}_K$ (porque la identidad de K es la única función estrictamente creciente de K en si mismo que extiende a la identidad de $\mathbb{Q}$). Similarmente $\overline{f} \circ \overline{g} = \mathrm{id}_{K'}$. Afirmamos que $\overline{f}$ es un isomorfismo de cuerpos. Para cada $a \in K$ y cada $a' \in K'$ escribamos

$$D_a \coloneqq \{q \in \mathbb{Q} : q \leq a\} \qquad \text{y} \qquad E_{a'} \coloneqq \{q \in \mathbb{Q}' : q \leq a'\}.$$

Como $\overline{f}$ es un isomorfismo de órdenes es evidente que $f(D_a) = E_{\overline{f}(a)}$ para todo $a \in K$. Por lo tanto, debido al item (1) del lema anterior,

$$\overline{f}(a+b) = \overline{f}(\sup(D_a + D_b)) = \sup f(D_a + D_b) = \sup(f(D_a) + f(D_b)) = \overline{f}(a) + \overline{f}(b),$$

para todo $a, b \in K$. En particular $\overline{f}(-a) = -\overline{f}(a)$ para todo $a \in K$. En consecuencia para terminar la demostración bastará ver que $\overline{f}(ab) = \overline{f}(a)\overline{f}(b)$ para todo $a, b \in P$. Nuevamente como en el lema anterior para cada $a > 0$ en K y cada $a' > 0$ en K' escribamos

$$D_a^+ \coloneqq \{q \in \mathbb{Q} : 0 < q \leq a\} \qquad \text{y} \qquad E_{a'}^+ \coloneqq \{q \in \mathbb{Q}' : 0 < q \leq a'\}.$$

Como $\overline{f}$ es un isomorfismo de órdenes es evidente que $f(D_a^+) = E_{\overline{f}(a)}^+$ para todo $a \in K$. Por lo tanto, debido al item (2) del lema anterior,

$$\overline{f}(ab) = \overline{f}(\sup(D_a^+ D_b^+)) = \sup f(D_a^+ D_b^+) = \sup(f(D_a^+) f(D_b^+)) = \sup(E_{\overline{f}(a)}^+ E_{\overline{f}(b)}^+) = \overline{f}(a)\overline{f}(b),$$

para todo $a, b \in P$.

Así, salvo isomorfismos canónicos hay a lo sumo un único cuerpo ordenado completo. Se puede probar que efectivamente hay un cuerpo ordenado completo al que llamaremos cuerpo de los números reales y al que denotaremos con $\mathbb{R}$.

A continuación generalizamos el Teorema 5.2 mostrando que en $\mathbb{R}$ los números positivos tiene raíces n-ésimas, para $n \in \mathbb{N}$ arbitrario. Necesitaremos el siguiente lemma.

Lemma 5.6. *Para cada $b > 0$ y cada $n \in \mathbb{N}$ existe $A_n > 0$ tal que $(b+\epsilon)^n \leq b^n + A_n\epsilon$ para todo $0 < \epsilon < 1$.*

Proof. Por inducción en n. El caso $n = 1$ es trivial. Supongamos que el resultado vale para n. Entonces

$$(b+\epsilon)^{n+1} \leq (b^n + A_n\epsilon)(b+\epsilon) = b^{n+1} + (A_n b + b^n + A_n\epsilon)\epsilon \leq b^{n+1} + (A_n b + b^n + A_n)\epsilon,$$

de modo que podemos tomar $A_{n+1} \coloneqq A_n b + b^n + A_n$. □

Theorem 5.7. *Supongamos que K es un cuerpo ordenado completo. Entonces, para cada $a > 0$ en K y cada $n \in \mathbb{N}$ existe un único $b > 0$ en K, tal que $b^n = a$.*

Proof. Por la Proposition 3.22 existe a lo sumo un único $b \in P$ tal que $b^n = a$. Veamos ahora que efectivamente existe un tal b. Escribamos $X_a \coloneqq \{x \geq 0 : x^n < a\}$ e $Y_a \coloneqq \{x \geq 0 : x^n > a\}$. Estos conjunto no son vacíos pues $0 \in X_a$ y $a + 1 \in Y_a$ (si $a \leq 1$, entonces $(a+1)^n > 1^n > a$ y si $a > 1$, entonces $(a+1)^n > a^n > a$). Además si $x \in X_a$ e $y \in Y_a$ entonces $x < y$ (pues si $y < x$, entonces $y^n < x^n$, lo que se contradice con que $x^n < a$ e $y^n > a$). En particular X_a está acotado superiormente. Denotemos con b al supremo de X_a. Afirmamos que $b^n = a$. Haremos esto por el absurdo. Supongamos primero que $b^n < a$ (en otras palabras que $b \in X_a$). Vamos a ver que entonces existe $\epsilon > 0$ en $\mathbb{Q}$ tal que $b + \epsilon \in X_a$ (lo que es imposible pues se contradice con el hecho de que b es el supremo de X_a). Debemos ver así que podemos elegir $\epsilon > 0$ en $\mathbb{Q}$ tal que $(b+\epsilon)^n < a$. Tomemos $0 < \epsilon < \min(1, (a - b^n)/A_n)$, donde A_n es como en el lema anterior. Entonces

$$(b+\epsilon)^n < b^n + A_n\epsilon < b^n + A_n\frac{a-b^n}{A_n} = b^n + a - b^n = a,$$

como queremos. En consecuencia necesariamente $b^n \geq a$. Así para terminar la demostración sólo debemos ver que $b^n > a$ es imposible. Vamos a ver que entonces existe $\epsilon > 0$ en $\mathbb{Q}$ tal que $b - \epsilon \in Y_a$ (lo que es imposible pues como los elementos de Y_a son cotas superiores de X_a con esto se contradice que b es el supremo de X_a). Debemos ver así que podemos elegir $\epsilon > 0$ en $\mathbb{Q}$ tal que $(b-\epsilon)^n > a$. Tomemos $0 < \epsilon < \min(b, (b^n - a)/nb^{n-1})$. Entonces, por la desigualdad de Bernoulli,

$$(b-\epsilon)^n = b^n\Big(1 - \frac{\epsilon}{b}\Big)^n \geq b^n\Big(1 - n\frac{\epsilon}{b}\Big) = b^n - nb^{n-1}\epsilon > b^n - nb^{n-1}\frac{b^n - a}{nb^{n-1}} = b^n - b^n + a = a,$$

nuevamente como queremos. □

Remark 5.8. Al elemento b obtenido en el teorema anterior se lo denomina raíz n-ésima de a y se lo denota $\sqrt[n]{a}$ o $a^{1/n}$. También definimos $\sqrt[n]{0}$ como 0. Claramente $(\sqrt[n]{a})^n = \sqrt[n]{a^n} = a$ para cada $a \geq 0$ y cada $n \in \mathbb{N}$.

Proposition 5.9. *Tomemos $q, s \in \mathbb{N}$, $p, r \in \mathbb{Z}$ y $a \geq 0$ en $\mathbb{R}$. Si $\frac{p}{q} = \frac{r}{s}$, entonces $\sqrt[q]{a^p} = \sqrt[s]{a^r}$.*

Proof. En efecto,

$$\big(\sqrt[q]{a^p}\big)^{qs} = (a^p)^s = a^{ps} = a^{rq} = (a^r)^q = \big(\sqrt[s]{a^r}\big)^{qs},$$

de donde $\sqrt[q]{a^p} = \sqrt[s]{a^r}$. □

Definition 5.10. Para cada $a \geq 0$ y cada número racional $\frac{m}{n}$ se define $a^{\frac{m}{n}}$ por $\sqrt[n]{a^m}$ (por la proposición anterior esta definición es correcta).

Proposition 5.11. *Se satisfacen las siguientes igualdades:*

(1) $a^{\frac{m}{n}+\frac{m'}{n'}} = a^{\frac{m}{n}} a^{\frac{m'}{n'}}$,
(2) $(a^{\frac{m}{n}})^{\frac{m'}{n'}} = a^{\frac{m}{n}\frac{m'}{n'}}$,
(3) $(ab)^{\frac{m}{n}} = a^{\frac{m}{n}} b^{\frac{m}{n}}$,

(4) *Si* $a \neq 0$, *entonces* $a^{\frac{m}{n}} \neq 0$ *y* $\left(a^{\frac{m}{n}}\right)^{-1} = (a^{-1})^{\frac{m}{n}}$,

(5) *Si* $0 \leq a < b$, *entonces* $0 \leq a^{\frac{m}{n}} < b^{\frac{m}{n}}$ *para todo* $\frac{m}{n} > 0$ *en* $\mathbb{Q}$.

(6) *Si* $0 < a < 1$ *y* $\frac{m}{n} < \frac{m'}{n'}$, *entonces* $a^{\frac{m}{n}} > a^{\frac{m'}{n'}}$.

(7) *Si* $1 < a$ *y* $\frac{m}{n} < \frac{m'}{n'}$, *entonces* $a^{\frac{m}{n}} < a^{\frac{m'}{n'}}$.

Proof. (1) En efecto,

$$\left(a^{\frac{m}{n}+\frac{m'}{n'}}\right)^{nn'} = a^{mn'+m'n} = a^{mn'}a^{m'n} = \left(a^{\frac{m}{n}}\right)^{nn'}\left(a^{\frac{m'}{n'}}\right)^{nn'} = \left(a^{\frac{m}{n}}a^{\frac{m'}{n'}}\right)^{nn'},$$

de donde $a^{\frac{m}{n}+\frac{m'}{n'}} = a^{\frac{m}{n}}a^{\frac{m'}{n'}}$.

(2) En efecto,

$$\left((a^{\frac{m}{n}})^{\frac{m'}{n'}}\right)^{nn'} = (a^{\frac{m}{n}})^{m'n} = a^{mm'} = \left(a^{\frac{mm'}{nn'}}\right)^{nn'},$$

de donde $(a^{\frac{m}{n}})^{\frac{m'}{n'}} = a^{\frac{m}{n}\frac{m'}{n'}}$.

(3) En efecto,

$$\left((ab)^{\frac{m}{n}}\right)^{n} = (ab)^{m} = a^m b^m = \left(a^{\frac{m}{n}}\right)^{n}\left(b^{\frac{m}{n}}\right)^{n} = \left(a^{\frac{m}{n}}b^{\frac{m}{n}}\right)^{n},$$

de donde $(ab)^{\frac{m}{n}} = a^{\frac{m}{n}}b^{\frac{m}{n}}$.

(4) En efecto, por el item 3) tenemos $a^{\frac{m}{n}}(a^{-1})^{\frac{m}{n}} = (aa^{-1})^{\frac{m}{n}} = 1^{\frac{m}{n}} = 1$.

(5) Supongamos que $b^{\frac{m}{n}} \leq a^{\frac{m}{n}}$. Por la Proposición 3.22,

$$b^m = \left(b^{\frac{m}{n}}\right)^n \leq \left(a^{\frac{m}{n}}\right)^n = a^m,$$

lo que se contradice con la Proposición 3.22.

(6) Como $mn' < m'n$ se sigue del primer item del Remark 3.23 que

$$\left(a^{\frac{m}{n}}\right)^{nn'} = a^{mn'} > a^{m'n} = \left(a^{\frac{m'}{n'}}\right)^{nn'}$$

Así $a^{\frac{m}{n}} > a^{\frac{m'}{n'}}$.

(7) Como $mn' < m'n$ se sigue del segundo item del Remark 3.23 que

$$\left(a^{\frac{m}{n}}\right)^{nn'} = a^{mn'} < a^{m'n} = \left(a^{\frac{m'}{n'}}\right)^{nn'}$$

Así $a^{\frac{m}{n}} < a^{\frac{m'}{n'}}$. □

Para cada $a < b$ en un conjunto totalmente ordenado K se definen el

- *intervalo abierto y acotado* (a, b), por $(a, b) \coloneqq \{x \in K : a < x < b\}$.
- *intervalo abierto a izquierda, cerrado a derecha y acotado* $(a, b]$, por $(a, b] \coloneqq (a, b) \cup \{b\}$.
- *intervalo cerrado a izquierda, abierto a derecha y acotado* $[a, b)$, por $[a, b) \coloneqq (a, b) \cup \{a\}$.
- *intervalo cerrado y acotado* $[a, b]$, por $[a, b] \coloneqq (a, b) \cup \{a, b\}$.

También definimos el *intervalo cerrado y acotado* $[a, a]$, por $[a, a] \coloneqq \{a\}$. Finalmente para cada $a \in K$ defnimos la

- *semirecta a derecha abierta* $(-\infty, a)$, por $(-\infty, a) \coloneqq \{x \in K : x < a\}$.
- *semirecta a derecha cerrada* $(-\infty, a]$, por $(-\infty, a] \coloneqq (-\infty, a) \cup \{a\}$.
- *semirecta a izquierda abierta* (a, ∞), por $(a, \infty) \coloneqq \{x \in K : a < x\}$.
- *semirecta a izquierda cerrada* $([a, \infty)$, por $[a, \infty) \coloneqq (a, \infty) \cup \{a\}$.

Theorem 5.12 (principio de intervalos encajados)**.** *Si* $J_1 \supseteq J_2 \supseteq J_3 \supseteq J_4 \supseteq \ldots$ *es una sucesión decreciente de intervalos cerrados y acotados* $J_n \coloneqq [a_n, b_n]$ *de* $\mathbb{R}$, *entonces* $\bigcap_{n\in\mathbb{N}} J_n = [a, b]$, *donde* $a \coloneqq \sup\{a_n : n \in \mathbb{N}\}$ *y* $b \coloneqq \inf\{b_n : n \in \mathbb{N}\}$ *(en particular* $\bigcap J_n \neq \emptyset$*).*

Proof. Es evidente que

$$a_1 \leq a_2 \leq \cdots \leq a_n \leq \cdots \leq b_n \leq \cdots \leq b_2 \leq b_1.$$

En particular $\{a_n : n \in \mathbb{N}\}$ está acotado superiormente y, así, existe $a \coloneqq \sup\{a_n : n \in \mathbb{N}\}$. Como cada b_n es una cota superior de $\{a_n : n \in \mathbb{N}\}$, sabemos que $a \leq b_n$ para todo $n \in \mathbb{N}$. Por lo tanto, existe $b \coloneqq \inf\{b_n : n \in \mathbb{N}\}$ y $a \leq b$. Es obvio que $[a, b] = \bigcap_{n\in\mathbb{N}}[a_n, b_n]$, pues $x \in J_n$ para todo n equivale a que $a_n \leq x \leq b_n$ para todo n, lo que significa que $a \leq x \leq b$. □

Es obvio que dado un intervalo cerrado y acotado $[a, b]$ con $a < b$ en $\mathbb{R}$ y un $x \in [a, b]$ existe otro intervalo cerrado $[c, d]$ con $a \leq c < d \leq b$, tal que $x \notin [c, d]$. Vamos a usar esto y el teorema anterior para probar el siguiente teorema.

Theorem 5.13. *Para cada $a < b$ en $\mathbb{R}$ el conjunto $[a, b]$ no es numerable.*

Proof. Supongamos que $\{x_1, x_2, x_3, \dots\} \subseteq [a, b]$. Vamos a ver que esta inclusión necesariamente es propia. Afirmamos que existen

$$a = a_0 \leq a_1 \leq a_2 \leq \cdots \leq a_n \leq \cdots \leq b_n \leq \cdots \leq b_2 \leq b_1 \leq b_0 = b,$$

en $\mathbb{R}$ tales que $\{x_1, \dots, x_n\} \cap [a_n, b_n] = \emptyset$. En efecto, una vez elejidos $a_n < b_n$ que satisfacen esta condición, se sigue inmediatamente de la observación anterior que existen $a_n \leq a_{n+1} < b_{n+1} \leq b_n$ tales que $x_{n+1} \notin [a_{n+1}, b_{n+1}]$ y, por lo tanto, $\{x_1, \dots, x_{n+1}\} \cap [a_{n+1}, b_{n+1}] = \emptyset$. Es obvio así que

$$\{x_1, x_2, x_3, \dots\} \cap \bigcap_{n\in\mathbb{N}} [a_n, b_n] = \emptyset.$$

Dado que por el teorema anterior $\bigcap_{n\in\mathbb{N}}[a_n, b_n] \neq \emptyset$, el conjunto $\{x_1, x_2, x_3, \dots\}$ está propiamente contenido en $[a, b]$. □