UN POCO DE MATEMÁTICA CONSTRUCTIVA

EDUARDO J. DUBUC, MARINA FRAGALÁ, MARINA VALDORA

1. Introducción

La matemática dejó de ser constructiva cuando se incorporó la utilización de la teoría de conjuntos, y en particular el axioma de elección en demostraciones de existencia. Simultáneamente comenzó a utilizarse el tercero excluido como método de demostración. *Recordar que el tercero excluido es el hecho que le da validez a las demostraciones por el absurdo en lógica clásica.* Al principio estas técnicas despertaron mucha desconfianza, y lo que hoy se acepta sin la menor objeción fue altamente cuestionado por la escuela intuicionista. Pitágoras ya sabía que la diagonal del cuadrado no es conmensurable con el lado, es decir, que $\sqrt{2}$ es un número irracional. Veamos el siguiente ejemplo de demostración no constructiva:

1.1. *Existen números α, β irracionales tales que α^β es un número racional.*

Demostración. Consideremos el número $\sqrt{2}^{\sqrt{2}}$. Si es racional, ponemos $\alpha = \beta = \sqrt{2}$ y listo. Si es irracional, ponemos $\alpha = \sqrt{2}^{\sqrt{2}}$, $\beta = \sqrt{2}$. Entonces $\alpha^\beta = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}.\sqrt{2}} = (\sqrt{2})^{(\sqrt{2})^2} = (\sqrt{2})^2 = 2$ y listo. □

No parece una demostración muy convincente. Podemos dudar si hemos demostrado que realmente existen dos números irracionales α, β tales que la exponencial α^β es racional. El problema es que tenemos dos posibilidades, pero no sabemos cuál de las dos da la respuesta. No estamos en condición de exibir un α y un β y afirmar con seguridad que para ese α y ese β la exponencial α^β es racional.

Lo que si está claro, es que nunca podremos demostrar que *la exponencial entre dos números irracionales es irracional.* Esta última conclusión es precisamente lo que la escuela intuicionista afirma que queda demostrado por el argumento en 1.1 arriba. Una demostración de la proposición 1.1 aceptable para la escuela intuicionista debe permitir exibir un α y un β, junto con una demostración que para ese α y ese β la exponencial α^β es racional.

Muchas demostraciones igualmente basadas en el tercero excluido son aceptadas sin ninguna objeción por la matemática moderna, como por ejemplo el teorema de Gauss:

Teorema 1.2 (Teorema de Gauss)**.** *Todo polinomio $f(x)$ con coeficientes en un cuerpo $\mathbb{K}$ se descompone como producto de polinomios irreducibles.*

Demostración. Si $f(x)$ es irreducible, ya está. Si no, se escribe $f(x) = g(x)h(x)$ con los grados de $g(x)$ y de $h(x)$ estrictamente menores que el grado de $f(x)$. Como los grados no pueden bajar indefinidamente, se llega necesariamente a los factores irreducibles. □

En 1931 aparece el primer libro de álgebra moderna *Moderne Algebra*, escrito por B. L. Van Der Waerden, matemático de la Universidad de Amsterdam, colaborador y colega de dos de los principales creadores de esta álgebra, E. Artin y E. Noether. A pesar de establecer resultados no constructivos, la preocupación por los aspectos

constructivos, especialmente en la teoría de cuerpos, está ampliamente presente en el libro de Van der Waerden (lo que ya no ocurre en textos posteriores), que aún hoy en día puede usarse perfectamente como libro de texto en cursos de álgebra.

Van Der Waerden dice ([2] preface to the second edition) "I have tried to avoid as much as possible any questionable set-theoretical reasoning in algebra. Unfortunately, a completely finite presentation of algebra, avoiding all non constructive proofs, is not possible without great sacrifices. On the other hand, it was possible at least to compile the building stones for a constructive foundation of algebra in so far as they exists at this time. In the theory of fields I did so by presenting the field theoretical operations in a finite number of steps in such a fashion that the intuitionistic foundations of the theory, in so far as it is possible today, can be seen readily. The theory of factorization is likewise presented in a more finite manner. I completely omitted those parts of the theory of fields which rest on the axiom of choice."

En este artículo pretendemos explicar e ilustrar en qué consiste esta problemática constructiva e intuicionista en el contexto del teorema de Gauss, contexto que históricamente fue encarado en forma especialmente constructiva por el matemático Kronecker, basándonos exclusivamente en el hermoso texto de Van der Waerden. Además, ligado a ello, presentar una construcción debida al matemático A. Joyal [1] que permite obtener intuicionisticamente la clausura pitagórica (todo elemento positivo tiene una raíz cuadrada positiva) de un cuerpo totalmente ordenado sin tener que decidir si un dado elemento ya tiene o no una raíz cuadrada. Los métodos y razonamientos que utilizamos en este artículo sirven también para ilustrar técnicas básicas de la teoría de categorías, que es una teoría particularmente bien adaptada a la matemática constructiva. Finalmente, se mostrará como una matemática constructiva al estilo del siglo diecinueve tiene una vigencia actual debido a la utilización de computadoras en el álgebra.

2. El teorema de Gauss constructivo y el problema de adjuntar raíces cuadradas

Kronecker, que siempre practicó una matemática constructiva, demuestra el teorema de Gauss para el cuerpo $\mathbb{Q}$ de los racionales de la siguiente manera:

Teorema 2.1 (Teorema de Gauss constructivo)**.** *Se tiene un procedimiento eficiente (algoritmo) que dado un polinomio $f(x)$ con coeficientes en un cuerpo $\mathbb{K}$, lo descompone en un producto de factores irreducibles en un número finito de pasos.*

Nota: *Este enunciado no es válido en general. Por ejemplo, resulta falso para el cuerpo $\mathbb{R}$ de los números reales.*

Demostración. Para $\mathbb{K} = \mathbb{Q}$. Observar primero que multiplicando por el mínimo común múltiplo de los denominadores podemos asumir que los coeficientes son enteros, y (dividiendo por el factor adecuado) sin ningún divisor común. Además, recordar que no es difícil demostrar que si un polinomio con coeficientes enteros es irreducible en $\mathbb{Z}[X]$ entonces también lo es en $\mathbb{Q}[X]$ (ver [2], sección 23). De acuerdo a esto, podemos asumir que la factorización se realiza en $\mathbb{Z}[X]$.

Sea $f(x) \in \mathbb{Z}[X]$ de grado n. Si no es irreducible, uno de los factores debe ser de grado $\leq n/2$, entonces debemos investigar si $f(x)$ tiene un factor $g(x)$ de grado $\leq s$, donde s es el mayor entero $\leq n/2$.

Calculamos los números $f(a_0),\ f(a_1),\ \ldots\ f(a_s)$ en $s+1$ enteros a_i (por ejemplo, $0,\ \pm 1,\ \pm 2,\ \ldots$). Si $g(x)$ divide a $f(x)$, entonces $g(a_0)$ divide a $f(a_0)$, $g(a_1)$ divide a $f(a_1)$, etc. Pero cada $f(a_i)$ tiene un número finito de factores; por lo tanto hay sólo un número finito de posibles valores $g(a_i)$. Para cada posible combinación de valores

$g(a_0),\ g(a_1),\ \ldots\ g(a_s)$, hay un único polinomio $g(x)$ de grado $\leq s$ (construido por ejemplo con la fórmula de Lagrange). De esta manera se encuentra un número finito de polinomios entre los cuales deben encontrarse todos los factores de $f(x)$ de grado $\leq s$. Con el algoritmo de división chequeamos, uno por uno, si alguno de ellos (que será necesariamente de grado ≥ 1) divide realmente a $f(x)$. Si ninguno lo hace, entonces $f(x)$ es irreducible, en caso contrario, se encuentran dos factores. Luego se procede a aplicar el mismo procedimiento a cada factor, y de esta manera se llega a los factores irreducibles. □

La construcción fundamental de la teoría de extensiones de cuerpos consiste en agregar raíces de polinomios irreducibles al cuerpo.

Veamos, como ejemplo, en qué consiste agregarle a $\mathbb{Q}$ una raíz cuadrada de 2. Para ello definimos el anillo

$$\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\} \subset \mathbb{R}$$

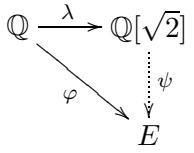
con el producto

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (bc + ad)\sqrt{2}$$

Se observa que $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/_{(x^2-2)}$ y que vale la siguiente propiedad:

i) Existe un morfismo de cuerpos $\mathbb{Q} \xrightarrow{\lambda} \mathbb{Q}[\sqrt{2}]$ tal que $(\sqrt{2})^2 = \lambda(2)$.

ii) Para todo otro par $(E,\ e)$, $e \in E$, donde E es un cuerpo munido de un morfismo de cuerpos $\varphi : \mathbb{Q} \to E$ tal que $e^2 = \varphi(2)$, existe un único morfismo de cuerpos $\psi : \mathbb{Q}[\sqrt{2}] \to E$ tal que $\psi(\sqrt{2}) = e$ y que hace conmutar el siguiente diagrama



$\mathbb{Q}[\sqrt{2}]$ resulta un cuerpo porque $\sqrt{2}$ es irracional (o sea sabemos que $\sqrt{2}$ no existe en $\mathbb{Q}$, es decir que el polinomio $x^2 - 2$ es irreducible).

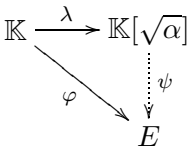
Consideremos ahora el caso general del problema ilustrado con este ejemplo. Se tiene un cuerpo $\mathbb{K}$ y se le quiere agregar una raíz cuadrada de un elemento α, y obtener de nuevo un cuerpo. Más precisamente queremos construir:

$$\mathbb{K} \xrightarrow{\lambda} \mathbb{K}[\sqrt{\alpha}]$$

donde

i) $\mathbb{K}[\sqrt{\alpha}]$ es un cuerpo con un elemento distinguido $\theta \in \mathbb{K}[\sqrt{\alpha}]$ tal que $\lambda(\alpha) = \theta^2$

ii) Para todo otro par $(E,\ e)$, $e \in E$, donde E es un cuerpo munido de un morfismo de cuerpos $\varphi : \mathbb{K} \to E$ tal que $e^2 = \varphi(\alpha)$, existe un único morfismo de cuerpos $\psi : \mathbb{K}[\sqrt{\alpha}] \to E$ tal que $\psi(\theta) = e$ y que hace conmutar el siguiente diagrama



Si un tal cuerpo existe, queda caracterizado completamente (salvo isomorfismo único) por esta propiedad, llamada *propiedad universal*.

Para obtener un tal cuerpo se procede como sigue:

Si α no tiene raiz cuadrada en $\mathbb{K}$, se construye el anillo cociente $\mathbb{K}[x]/_{(x^2-\alpha)}$, que resulta ser un cuerpo porque el polinomio $x^2-\alpha$ es irreducible. Por el algoritmo de división este cociente resulta isomorfo al conjunto $\mathbb{K}\times\mathbb{K}$ con las operaciones:

$$(a,\ b)+(c,\ d)=(a+c,\ b+d),\quad (a,\ b)(c,\ d)=(ac+\alpha\ bd,\ bc+ad).$$

Se toma $\theta=(0,\ 1)$. El lector puede verificar fácilmente la validez de la propiedad universal.

Si $\alpha\in\mathbb{K}$ ya tiene raíz cuadrada en $\mathbb{K}$, tendríamos que quedarnos con el propio cuerpo $\mathbb{K}$ y señalar una raíz de α, θ, $\theta^2=\alpha$. Pero $-\theta$ es también una raíz cuadrada de α, y no hay ningun criterio para distinguir entre θ y $-\theta$. En este caso es fácil demostrar que un tal cuerpo no existe. Debería ser el propio $\mathbb{K}$ junto con una raiz distinguida. La presencia de la otra raíz contradice la propiedad universal.

Resulta necesario poder distinguir entre las dos raíces cuadradas de α, para luego elegir una. Una manera de hacer esto es suponer que $\mathbb{K}$ está munido de un orden total, y entonces debe tener la raíz positiva y la raíz negativa. En este caso, se decide que la raíz positiva es la distinguida.

Vamos a considerar cuerpos totalmente ordenados y morfismos que preservan el orden, y el problema de agregar raíces cuadradas sólo a los elementos positivos.

Si $\alpha>0$ no tiene raíz en $\mathbb{K}$, puede verse que la construcción anterior está munida de un orden total, y resuelve el problema también en este contexto. Es instructivo analizar cuando $a+b\sqrt{2}>0$ en el ejemplo $\mathbb{Q}[\sqrt{2}]$, y obtener las condiciones en a, b que se utilizan para *definir* $a+b\,\theta>0$ en $\mathbb{K}[x]/_{(x^2-\alpha)}$ (relacionado con esto ver 4.4).

Si α ya tiene raíz cuadrada en $\mathbb{K}$, ponemos $\mathbb{K}[\sqrt{\alpha}]=\mathbb{K}$, con la raíz positiva como elemento distinguido. Es immediato verificar la propiedad universal (tener en cuenta que los morfismos deben preservar el orden).

En conclusión, en el contexto de los cuerpos totalmente ordenados, hemos demostrado que el cuerpo $\mathbb{K}[\sqrt{\alpha}]$ con la propiedad universal que lo caracteriza siempre existe. Tenemos:

$$(*)\qquad \mathbb{K}[\sqrt{\alpha}]=\mathbb{K}[x]/_{(x^2-\alpha)}\quad o\quad \mathbb{K}[\sqrt{\alpha}]=\mathbb{K}.$$

Pero no sabemos cuál de las dos igualdades vale si no se cuenta con un procedimiento efectivo que permita decidir si $x^2-\alpha$ es irreducible o no. No estamos en condición de exibir un cuerpo y afirmar con seguridad que ese cuerpo es $\mathbb{K}[\sqrt{\alpha}]$. Esta demostración de la existencia de tal cuerpo es inaceptable para el intuicionismo, y sólo será aceptable si se cuenta con una demostración del teorema de Gauss constructivo para $\mathbb{K}$ (como es el caso cuando $\mathbb{K}=\mathbb{Q}$), ya que en ese caso la disjunción (*) es decidible. El teorema de Gauss constructivo no es válido para un cuerpo arbritrario, y el problema que se presenta es:

Como desarrollar la teoría de cuerpos sin el teorema de Gauss ?

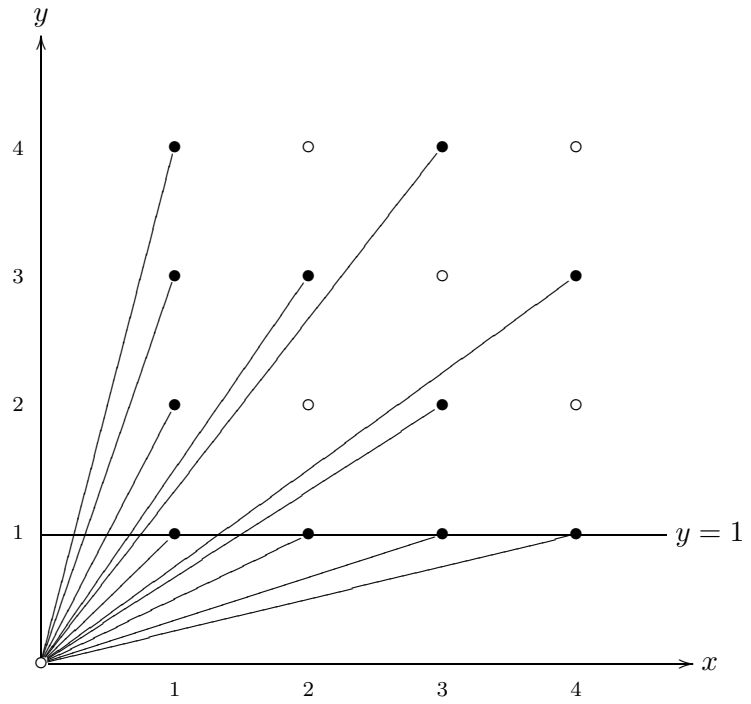
3. Algunas precisiones sobre la matemática intuicionista

Para el intuicionismo no todos los conjuntos son *"discretos"* como es el caso en la teoría de conjuntos clásica.

Definición 3.1. *Un conjunto X es discreto si la relación de igualdad es decidible, en el sentido que se tiene un procedimiento (algoritmo) que, dados x, $y\in X$, en un número finito de pasos decide si $x=y$ o $x\neq y$.*

Notar que demostraciones por el absurdo de enunciados que afirman la igualdad entre elementos de X son entonces válidas intuicionísticamente.

Los enteros $\mathbb{Z}$ son un conjunto discreto y los racionales también. Hablando informalmente, los números racionales se pueden "despegar" y en consecuencia forman un conjunto discreto (aún cuando su topología usual del orden no sea discreta, sino densa). Esto lo podemos ilustrar como sigue (donde se consideran solo los racionales positivos):



Los números racionales corresponden a los puntos visibles desde el origen (coordenadas relativamente primas), que es un conjunto claramente discreto. Las intersecciones de la recta por el origen determinada por estos puntos con la recta horizontal $y = 1$ forma el conjunto de los números racionales con el orden usual.

Formalmente, $\mathbb{Q}$ resulta discreto según la definición 3.1 porque $\mathbb{Z}$ es discreto:

$$x,\ y \in \mathbb{Q},\ x = a/b,\ y = c/d,\ a,\ b,\ c,\ d \in \mathbb{Z},\ \ entonces\ \ x = y \iff ad = cb$$

En la ilustración de arriba el conjunto $\mathbb{R}$ de números reales es toda la recta $y = 1$, y sus puntos corresponden al conjunto de todas las direcciones. Los números reales no siempre se pueden "despegar", en particular no siempre se pueden despegar del 0. Esto es así aún cuando se consideren solamente números reales definidos por un algoritmo que permite conocerlos con precisión arbitraria. Una demostración formal de este hecho es la siguiente.

Adoptemos por ejemplo la construcción de $\mathbb{R}$ por medio de sucesiones de Cauchy:

$$C = \{x = (a_n)_{n\in\mathbb{N}},\ a_n \in \mathbb{Q}\ /\ es\ de\ Cauchy\},$$

$$I \subset C,\quad (a_n)_{n\in\mathbb{N}} \in I \iff \forall \epsilon \in \mathbb{Q},\ \epsilon > 0,\ \exists n_0\ /\ \forall n > n_0\ |a_n| < \epsilon$$

Los números reales se definen como el conjunto cociente $\mathbb{R} = C/I$. La relación de igualdad en $\mathbb{R}$ es la relación de equivalencia módulo I en C:

$$x \equiv y\ mod(I) \iff x - y\ \in\ I$$

Que $\mathbb{R}$ sea decidible significa que esta relación es decidible en el sentido que se tiene un procedimiento (algoritmo) que, dados $x,\ y \in C$, en un número finito de pasos

decide si $x - y \in I$ o $x - y \notin I$. Puede verse que esta relación no es decidible argumentando como sigue.

Los números primos $s \in \mathbb{N}$ de la forma $s = 2^{2^k} + 1$ se llaman primos de Fermat (resultan primos para $k = 0,\ 1,\ 2,\ 3,\ 4,\ 5$, y no se conoce ningún otro primo de Fermat). Definamos la función $\chi : \mathbb{N} \to \{0,\ 1\}$:

$$\chi(s) = 1 \ \textit{ si } s \textit{ es un primo de Fermat con } k > 5, \ \ \chi(s) = 0 \ \textit{ si no.}$$

La función χ es calculable para cada $s \in \mathbb{N}$ en un número finito de pasos, y se sigue que las sumas parciales $a_n = \sum_{s \leq n} \chi(s)/2^s$ definen una sucesión de Cauchy $x = (a_n)_{n \in \mathbb{N}}$. Este elemento $x \in C$ determina un número real ξ que es la suma de la serie $\xi = \sum_s \chi(s)/2^s$ (que se puede calcular con presición arbritraria).

Es immediato comprobar que decidir en este caso $\xi = 0$ o $\xi \neq 0$, es decir, $x \in I$ o $x \notin I$, significa resolver el problema

$$\exists\, k > 5 \mid s = 2^{2^k} + 1 \textit{ es primo} \quad o \quad \forall\, k > 5,\ s = 2^{2^k} + 1 \textit{ no es primo.}$$

Similarmente puede verse que si $\mathbb{R}$ fuese decidible se tendría un procedimiento (algoritmo) que resuelve simultáneamente todo problema de este tipo en un número finito de pasos. Pero la solución de las ecuaciones Diofánticas es indecidible con un procedimiento uniforme recursivo ($10^{\underline{o}}$ problema de Hilbert).

Un cuerpo será llamado intuicionista si su conjunto subyacente es discreto y posee algoritmos para las operaciones. Estos cuerpos se dicen *"dados explícitamente"* ("given explicitly") en [2], seccion 42.

Definición 3.2. *Un cuerpo $\mathbb{K}$ es intuicionista si dados elementos $\alpha,\ \beta \in \mathbb{K}$:*

i) se tiene un algoritmos que decide en un número finito de pasos si $\alpha = \beta$.

ii) se tienen algoritmos que computan en un número finito de pasos las operaciones: $\alpha + \beta$, $\alpha - \beta$, $\alpha \times \beta$ y $\alpha \div \beta$.

Notar que la definición anterior es equivalente a tener algoritmos para las operaciones y un algoritmo para poder comparar cualquier elemento con 0, pues $\alpha = \beta \Leftrightarrow \alpha - \beta = 0$.

Si $\mathbb{K}$ es un cuerpo intuicionista, también lo será cualquier extensión algebraica simple $\mathbb{K}[\theta]$, con ecuación dada $f(\theta) = 0$, $\mathbb{K}[\theta] = \mathbb{K}[x]/(f(x))$. Esto se sigue del algoritmo de división para polinomios. $\mathbb{K}[\theta]$ resulta isomorfo a un producto finito de copias de $\mathbb{K}$ (por lo tanto discreto) y esta claro que los algoritmos para las operaciones de $\mathbb{K}$ permiten definir algoritmos para las operaciones de $\mathbb{K}[\theta]$.

Como mostró Kronecker, el teorema de Gauss constructivo es cierto para $\mathbb{Q}$, y resulta que en los ejemplos concretos de cuerpos intuicionistas siempre resulta posible demostrarlo. Por ejemplo, $\mathbb{Q}$ (los racionales), $\mathbb{Q}[i]$ (cuerpo de los números de Gauss), $\mathbb{Q}(X)$ (cuerpo de funciones racionales con coeficientes racionales), $F_p = \mathbb{Z}/p\mathbb{Z}$ (cuerpo de enteros módulo un número primo), etc, etc ([2] sección 42). Kronecker también demostró que si el teorema es cierto para un cuerpo intuicionista $\mathbb{K}$, entonces también lo es para cualquier extensión algebraica simple separable $\mathbb{K}[\theta]$, con ecuación dada $f(\theta) = 0$. Pero aún en este caso, como podría ser $\mathbb{Q}[\theta]$ por ejemplo, Van Der Waerden dice que si bien es teóricamente posible encontrar los factores irreducibles de un polinomio dado, en la práctica se presentan dificultades aritméticas casi insuperables aún en los casos más simples ([2] sección 42). Podemos pensar que desarrollar un software (basado en estas demostraciones del teorema de Gauss constructivo) que permita decidir si un polinomio arbritrario es irreducible o no, es imposible en la práctica.

Por otro lado, además, no se conoce una demostración general del teorema de Gauss constructivo para un cuerpo intuicionista arbritrario. Es decir, dado un

cuerpo intuicionista $\mathbb{K}$, no se cuenta en general con un algoritmo que permita decidir si un polinomio en $\mathbb{K}[X]$ es irreducible o no.

En consecuencia, el problema con que se enfrenta el álgebra constructiva es que hay que ser capaz de desarrollar la teoría de extensiones de cuerpos sin el teorema de Gauss.

Esto quedo ilustrado más arriba cuando vimos que la construcción clásica de $\mathbb{K}[\sqrt{\alpha}]$, que depende del teorema de Gauss, resulta inaceptable para el intuicionismo

¿Cómo hacer entonces para obtener un construcción unificada de $\mathbb{K}[\sqrt{\alpha}]$ sin tener que decidir si $x^2 - \alpha$ es reducible o no? De esto se trata la siguiente sección.

4. Construcción de $\mathbb{K}[\sqrt{\alpha}]$ para un cuerpo totalmente ordenado

Sea $\mathbb{K}$ un cuerpo totalmente ordenado, y $\alpha > 0$ un elemento de $\mathbb{K}$. Nuestro objetivo es describir una construcción unificada del cuerpo $\mathbb{K}[\sqrt{\alpha}]$ que solucione el problema de agregarle a $\mathbb{K}$ una raíz cuadrada de α, sin tener que decidir si α ya tiene o no raíz en $\mathbb{K}$.

Definición 4.1. *Un cuerpo totalmente ordenado $\mathbb{K}$ es intuicionista si dados elementos α y $\beta \in \mathbb{K}$:*

i) se tiene un algoritmo que decide en un número finito de pasos si

$$\alpha > \beta \ \ o \ \ \alpha < \beta \ \ o \ \ \alpha = \beta.$$

ii) se tienen algoritmos que computan en un número finito de pasos las operaciones:

$$\alpha + \beta, \ \ \alpha - \beta, \ \ \alpha \times \beta, \ \ \alpha \div \beta.$$

Notar que la definición anterior es equivalente a tener algoritmos para las operaciones y un algoritmo para poder comparar cualquier elemento con 0, pues $\alpha > \beta \Leftrightarrow \alpha - \beta > 0$ y $\alpha = \beta \Leftrightarrow \alpha - \beta = 0$.

Sea entonces $\mathbb{K}$ un cuerpo totalmente ordenado intuicionista, y α un elemento positivo de $\mathbb{K}$. Construimos el anillo $\mathbb{K}[\theta] = \mathbb{K}[x]/_{(x^2-\alpha)}$, que por el algoritmo de división resulta isomorfo al conjunto $\mathbb{K} \times \mathbb{K}$, con $\theta = (0,\ 1)$, y con las operaciones:

$$(a,\ b) + (c,\ d) = (a + c,\ b + d), \quad (a,\ b)(c,\ d) = (ac + \alpha bd,\ bc + ad).$$

Esta claro que los algoritmos para las operaciones de $\mathbb{K}$ permiten definir algoritmos para las operaciones de $\mathbb{K}[\theta]$. Adoptamos ahora la notación tradicional

$$\mathbb{K}[\theta] \cong \{a + b\,\theta : a, b \in \mathbb{K}, \ \ \theta^2 = \alpha\}$$

con las operaciones

$$(a + b\,\theta) + (c + d\,\theta) = (a + c) + (b + d)\,\theta, \ \ (a + b\,\theta)(c + d\,\theta) = ac + \alpha bd + (bc + ad)\,\theta$$

Es obvio que $\theta^2 = \alpha$. El problema que se presenta ahora es que si α ya tiene una raíz cuadrada en $\mathbb{K}$, $\mathbb{K}[\theta]$ no es un cuerpo. El matemático Andre Joyal, de la Universidad de Quebec en Montreal, tuvo la idea de definir un ideal I tal que el cociente $\mathbb{K}[\theta]/I$ resulta siempre un cuerpo, independientemente de si α tiene raíz en $\mathbb{K}$ o no [1].

Consideremos el siguiente subconjunto de $\mathbb{K}[\theta]$

$$I = \{a + b\,\theta \in \mathbb{K}[\theta] \ / \ a = 0 \ y \ b = 0 \ \ o \quad b \neq 0 \ \ y \ \ -\frac{a}{b} > 0 \ \ y \ \ (-\frac{a}{b})^2 = \alpha\}$$

La relación de pertenencia a I es perfectamente decidible, y por lo tanto si I es un ideal, el conjunto cociente resultará discreto. Observar que $I = \{0\}$ si α no tiene raíz cuadrada en $\mathbb{K}$. Sin embargo podremos demostrar que I es un ideal sin saber si $I = \{0\}$ o no.

Proposición 4.2. *I es un ideal.*

Demostración. Sean $(a+b\,\theta)\ ,\ (a'+b'\,\theta)\in I$ y $(c+d\,\theta)\in\mathbb{K}[\theta]$. Debemos ver

$i)\ (a+b\,\theta)\ +\ (a'+b'\,\theta)\ \in I$
$ii)(a+b\,\theta)\ .\ (c\ +d\ \theta)\ \in I$

Los casos $a=b=0$ ó $a'=b'=0$ son ambos triviales. Por lo tanto sólo consideraremos:

$b\neq 0,\ \ -\frac{a}{b}>0\ \ y\ \ (-\frac{a}{b})^2=\alpha$ y
$b'\neq 0,\ \ -\frac{a'}{b'}>0\ \ y\ (-\frac{a'}{b'})^2=\alpha$

$i)\ \ (a+b\,\theta)\ +\ (a'+b'\,\theta)=(a+a')+(b+b')\,\theta$

Caso 1: $b+b'=0$.
Debemos ver que $a+a'=0$. Pero

$$\frac{a^2}{b^2}=\alpha=\frac{a'^2}{b'^2}\ \Rightarrow\ a^2=\alpha b^2,\ \ a'^2=\alpha b'^2\ \Rightarrow\ a^2=a'^2\ \Rightarrow\ (a-a')(a+a')=0$$

Supongamos que $a=a'$. Como $b=-b'$ entonces $\frac{a}{b}=-\frac{a'}{b'}>0$. Esto es absurdo pues $\frac{a}{b}<0$. Por lo tanto $a\neq a'$ y $a+a'=0$.

Caso 2: $b+b'\neq 0$.
Veamos que $-\frac{a+a'}{b+b'}>0$ y $(-\frac{a+a'}{b+b'})^2=\alpha$.

$$(-\frac{a+a'}{b+b'})^2=\frac{a^2+2aa'+a'^2}{b^2+2bb'+b'^2}=\frac{\alpha b^2+2aa'+\alpha b'^2}{b^2+2bb'+b'^2}=\alpha(\frac{\alpha b^2+2aa'+\alpha b'^2}{\alpha b^2+2\alpha bb'+\alpha b'^2})=\alpha$$

pues como $(aa')^2=(\alpha bb')^2$ entonces $(aa'-\alpha bb')(aa'+\alpha bb')=0$. Pero si $(aa'+\alpha bb')=0$ entonces $\frac{aa'}{bb'}=-\alpha$ y no es posible pues el primer miembro es positivo y el segundo es negativo. Luego resulta que $aa'=\alpha bb'$ y con esto queda demostrada la igualdad.

Nos queda ver $-\frac{a+a'}{b+b'}>0$:
Como $(\frac{a}{b})^2=\alpha=(\frac{a'}{b'})^2\ \Leftrightarrow\ (\frac{a}{b}-\frac{a'}{b'})(\frac{a}{b}+\frac{a'}{b'})=0$ y $\frac{a}{b}+\frac{a'}{b'}<0$, se sigue que $\frac{a}{b}-\frac{a'}{b'}=0$.
Luego $a+a'=a+\frac{ab'}{b}=a(1+\frac{b'}{b})=a(\frac{b+b'}{b})$. Se concluye que $\frac{a+a'}{b+b'}=\frac{a}{b}<0$.

En ambos casos se obtuvo $(a+b\,\theta)\ +\ (a'+b'\,\theta)\ \in I$.

$ii)\ (a+b\,\theta).(c+d\,\theta)=ac+\alpha bd+(ad+bc)\,\theta$

Tenemos dos casos nuevamente.

Caso 1: $ad+bc=0$.
Veamos que $ac+\alpha bd=0$: $ac+\alpha bd=a(-\frac{ad}{b})+\frac{a^2}{b^2}bd=-\frac{a^2d}{b}+\frac{a^2d}{b}=0$.

Caso 2: $ad+bc\neq 0$

Debemos ver $-\frac{ac+\alpha bd}{ad+bc}>0$: $-\frac{ac+\alpha bd}{ad+bc}=-\frac{ac+\frac{a^2}{b^2}bd}{ad+bc}=-\frac{a}{b}\frac{cb+ad}{ad+bc}=-\frac{a}{b}>0$.

y $(-\frac{ac+\alpha bd}{ad+bc})^2=\alpha$: $(-\frac{ac+\alpha bd}{ad+bc})^2=(-\frac{a}{b})^2=\alpha$ □

El orden total es necesario para que I sea un ideal. Es fácil ver, por ejemplo, que sin la condición $-\frac{a}{b}>0$, I no resulta cerrado para la suma.

Proposición 4.3. *$\mathbb{K}[\theta]/I$ es un cuerpo totalmente ordenado intuicionista, y se tiene $[\theta]>0$ con $[\theta]^2=\alpha$.*

Demostración. Está claro que $[\theta]^2=\alpha$. Por otro lado ya observamos que la relación de pertenencia a I es decidible. Los algoritmos para las operaciones en $\mathbb{K}[\theta]$

definen respectivos algoritmos en el cociente $\mathbb{K}[\theta]/I$. Para ver que es un cuerpo sólo queda encontrar el inverso multiplicativo de los elementos distintos de cero.

Sea $[a+b\,\theta] \in \mathbb{K}[\theta]/I$ un elemento no nulo (o sea $a+b\,\theta \notin I$). Le buscamos el inverso multiplicativo. Hay tres casos:

Caso 1: $b=0$

Como $a+b\,\theta \ \notin I$, entonces $a \neq 0$. Luego $[a+b\,\theta]^{-1} = \frac{1}{a}$.

Caso 2: $b \neq 0$ y $(-\frac{a}{b})^2 \neq \alpha$

O sea $\ a^2 - \alpha b^2 \neq 0$ y por lo tanto $[a+b\,\theta]^{-1} = \frac{a-b\,\theta}{a^2-\alpha b^2}$.

Caso 3: $b \neq 0,\ \ (-\frac{a}{b})^2 = \alpha \ \text{ y } \ \frac{a}{b} > 0$.

Para ello notar que $\frac{a}{b} - \theta \in I$, es decir $[\frac{a}{b}] = [\theta]$. Luego $[a+b\,\theta] = [a+b\,\frac{a}{b}] = [2a]$. Se tiene que $[a+b\,\theta]^{-1} = [\frac{1}{2a}]$.

Resta definir una relación de orden total y ver que se tiene un algoritmo que permite comparar elementos. Definimos

$$[a+b\,\theta] > [a'+b'\,\theta] \Longleftrightarrow [(a-a')+(b-b')\,\theta] > 0. \tag{4.4}$$

Luego bastaría comparar con 0, lo que hacemos a continuación:

$$i)\ [a+b\,\theta] = 0 \iff \begin{cases} a=0 \quad y \quad b=0 \\ b\neq 0 \quad y \quad -\frac{a}{b} > 0 \quad y \quad \alpha = (-\frac{a}{b})^2 \end{cases}$$

$$ii)\ [a+b\,\theta] > 0 \Longleftrightarrow \begin{cases} a>0 \quad y \quad b=0 \\ a\geq 0 \quad y \quad b>0 \\ a<0 \quad y \quad b>0 \quad y \quad \alpha > (-\frac{a}{b})^2 \\ a>0 \quad y \quad b<0 \quad y \quad \alpha < (-\frac{a}{b})^2 \end{cases}$$

$$iii)\ [a+b\,\theta] < 0 \Longleftrightarrow \begin{cases} a<0 \quad y \quad b=0 \\ a\leq 0 \quad y \quad b<0 \\ a<0 \quad y \quad b>0 \quad y \quad \alpha < (-\frac{a}{b})^2 \\ a>0 \quad y \quad b<0 \quad y \quad \alpha > (-\frac{a}{b})^2 \end{cases}$$

Observemos que $[\theta] > 0$ y que la condición de ser igual a cero es la de pertenencia a I.

Veamos que la relación está bien definida, es decir si $[a+b\ \theta] = [a'+b'\ \theta]$ y $[a+b\,\theta] > 0$ entonces $[a'+b'\,\theta] > 0$.

$[a+b\,\theta] = [a'+b'\,\theta]$ significa que $a=a'$ y $b=b'$ o bien

$$b-b' \neq 0\ ,\ -\frac{a-a'}{b-b'} > 0 \quad y \quad \alpha = (-\frac{a-a'}{b-b'})^2 \tag{4.5}$$

En el primer caso se verifica trivialmente que $[a'+b'\,\theta] > 0$. En el segundo tenemos que considerar varias posibilidades. Analicemos sólo uno de ellas:

$$a<0\ ,\ b>0 \quad y \quad \alpha > (\frac{a}{b})^2 \tag{4.6}$$

De 4.5 y 4.6 se deduce que $(\frac{a-a'}{b-b'})^2 > (\frac{a}{b})^2$ y como ambas bases son negativas entonces $\frac{a-a'}{b-b'} < \frac{a}{b}$ (como en 4.2). De esto se sigue que $\frac{ab'-ba'}{b(b-b')} < 0$ o lo que es lo mismo $\frac{ab'}{b-b'} < \frac{ba'}{b-b'}$ pues $b>0$. Considerando todas las posibles combinaciones de signos de a', b' y $b-b'$ se llega a que $[a'+b'\,\theta] > 0$. Por ejemplo, supongamos $b-b' > 0$, $b' < 0$ y $a' > 0$ y veamos que $\alpha < (\frac{a'}{b'})^2$. Como

$$b-b' > 0 \Longrightarrow ab' < ba' \Longrightarrow (a-a')b' < a'(b-b') \Longrightarrow 0 > \frac{a-a'}{b-b'} > \frac{a'}{b'}$$

entonces $\alpha = (\frac{a-a'}{b-b'})^2 < (\frac{a'}{b'})^2$. Por lo tanto $[a' + b'\,\theta] > 0$.

Para ver que esta relación define un orden total debemos verificar los axiomas de tricotomía, transitividad, monotonía de la suma y del producto. El primero de ellos se satisface por definición: dados dos elementos cualesquiera siempre son comparables. La monotonía de la suma, o sea:

$$[a + b\,\theta] > [a' + b'\,\theta] \implies [a + b\,\theta] + [c + d\,\theta] > [a' + b'\,\theta] + [c + d\,\theta]$$

también es inmediata a partir de la definición. Con respecto a la monotonía del producto, es decir

$$[a + b\,\theta] > [a' + b'\,\theta] \quad y \quad [c + d\,\theta] > 0 \implies [a + b\,\theta].[c + d\,\theta] > [a' + b'\,\theta].[c + d\,\theta]$$

bastaría ver

$$([a + b\,\theta] - [a' + b'\,\theta]).[c + d\,\theta] > 0$$

y esto se reduce a probar que el producto de dos elementos positivos es positivo. Supongamos entonces que $[a + b\,\theta] > 0$ y $[a' + b'\,\theta] > 0$ y veamos que

$$[a + b\,\theta].[a' + b'\,\theta] = [(aa' + \alpha bb') + (ba' + ab')\,\theta] > 0.$$

De nuevo deberíamos considerar varios casos. Estudiemos uno de ellos:

$$a < 0,\ \ b > 0,\ \ \alpha > (-\frac{a}{b})^2, \quad y \quad a' < 0,\ \ b' > 0,\ \ \alpha > (-\frac{a'}{b'})^2$$

Se verifica $aa' + \alpha bb' > 0$ y $ba' + ab' < 0$, por lo cual debemos probar que $\alpha < (\frac{aa'+\alpha bb'}{ba'+ab'})^2$ que es equivalente a

$$0 < \ b^2b'^2\alpha^2 - (a'^2b^2 + a^2b'^2)\alpha + a^2a'^2 \ = \ b^2b'^2(\alpha - (\frac{a}{b})^2)(\alpha - (\frac{a'}{b'})^2)$$

Pero si $\alpha > (\frac{a}{b})^2$ y $\alpha > (\frac{a'}{b'})^2$ la desigualdad anterior se verifica. Los otros casos son similares.

Algo parecido sucede con la transitividad:

$$[a + b\,\theta] > [a' + b'\,\theta]\ \ y\ \ [a' + b'\,\theta] > [a'' + b''\,\theta] \Longrightarrow [a + b\,\theta] > [a'' + b''\,\theta]$$

es decir

$$[a + b\,\theta] - [a' + b'\,\theta] > 0\ \ y\ \ [a' + b'\,\theta] - [a'' + b''\,\theta] > 0 \Longrightarrow [a + b\,\theta] - [a'' + b''\,\theta] > 0$$

y para esto podríamos ver que si se suman dos elementos positivos el resultado es positivo. Supongamos entonces que $[a + b\,\theta] > 0$ y $[a' + b'\,\theta] > 0$ y veamos que $[(a + a') + (b + b')\,\theta] > 0$. De nuevo hay que considerar varias posibilidades, por ejemplo:

$$a < 0\ ,\ b > 0\ ,\ \alpha > (\frac{a}{b})^2 \quad y \quad a' > 0\ ,\ b' < 0\ ,\ \alpha < (\frac{a'}{b'})^2.$$

En este caso se tiene que $(\frac{a}{b})^2 < \alpha < (\frac{a'}{b'})^2$ y por lo tanto $\frac{a}{b} > \frac{a'}{b'}$, es decir $ab' < a'b$. Sumando ab se obtiene

$$a(b + b') < b(a + a') \tag{4.7}$$

En cambio si sumamos $a'b'$ se obtiene

$$b'(a + a') < a'(b + b') \tag{4.8}$$

Hay cuatro casos a considerar que corresponden a todas las distintas combinaciones de signos de $a + a'$ y $b + b'$ (el caso $b + b' = 0$ es trivial). Si $b + b' > 0$ se usa la desigualdad 4.7 y si $b + b' < 0$ se usa la desigualdad 4.8. Consideremos, por ejemplo, el caso $b + b' < 0$ y $a + a' > 0$. De 4.8 se sigue que $\frac{a+a'}{b+b'} < \frac{a'}{b'} < 0$ y por lo tanto $\alpha < (\frac{a'}{b'})^2 < (\frac{a+a'}{b+b'})^2$ lo cual demuestra $[(a + a') + (b + b')\,\theta] > 0$. Queda a cargo del lector chequear las otras opciones. □

Resta ahora verificar que el cuerpo $\mathbb{K}[\theta]/I$ satisface la propiedad universal que define a $\mathbb{K}[\sqrt{\alpha}]$. Es decir, es el menor cuerpo totalmente ordenado intuicionista que contiene a $\mathbb{K}$ como subcuerpo, y a las raíces cuadradas de α, con la raíz positiva explícitamente indicada.

Corolario 4.9. *Denotemos* $\mathbb{K}[\sqrt{\alpha}] = \mathbb{K}[\theta]/I$ *y* $\sqrt{\alpha} = [\theta]$. *Dados elementos* $a, a' \in \mathbb{K}$: $[a] = [a'] \Leftrightarrow a = a'$, *por lo que podemos escribir a los elementos de* $\mathbb{K}[\sqrt{\alpha}]$ *de la forma* $a + b\sqrt{\alpha}$. *Se tiene:*

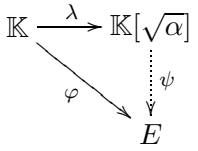
i) un morfismo de cuerpos totalmente ordenados:

$$\mathbb{K} \xrightarrow{\lambda} \mathbb{K}[\sqrt{\alpha}], \quad \sqrt{\alpha} \in \mathbb{K}[\sqrt{\alpha}], \quad (\sqrt{\alpha})^2 = \alpha, \quad \sqrt{\alpha} > 0.$$

ii) Para todo cuerpo intuicionista totalmente ordenado E, *y morfismo de cuerpos totalmente ordenados*

$$\mathbb{K} \xrightarrow{\varphi} E, \quad e \in E, \quad e^2 = \varphi(\alpha), \quad e > 0,$$

existe un único morfismos de cuerpos totalmente ordenados $\psi : \mathbb{K}[\sqrt{\alpha}] \to E$ *tal que* $\psi(\sqrt{\alpha}) = e$, *y que hace conmutar el siguiente diagrama*



Demostración. Definimos ψ de la única forma posible para que el diagrama conmute, o sea $\psi(a + b\sqrt{\alpha}) = \varphi(a) + \varphi(b)\, e$. Veamos que está bien definido y que es morfismo de cuerpos ordenados.

a) Buena definición.

Sea $a + b\sqrt{\alpha} = a' + b'\sqrt{\alpha}$, es decir $(a - a') + (b - b')\,\theta \in I$. Queremos ver

$$\varphi(a) + \varphi(b)\, e = \varphi(a') + \varphi(b')\, e$$

Es trivial si $b - b' = 0$ debido a que $a - a' = 0$. Analicemos el caso

$$b - b' \neq 0,\ -\frac{a - a'}{b - b'} > 0 \ \ y \ \ (-\frac{a - a'}{b - b'})^2 = \alpha.$$

Como $(\frac{a-a'}{b-b'})^2 = \alpha$, $\varphi((\frac{a-a'}{b-b'})^2) = \varphi(\alpha) = e^2$. Pero $\frac{a-a'}{b-b'} < 0$ y φ es un morfismo de cuerpos ordenados, entonces

$$\varphi(\frac{a - a'}{b - b'}) = -e, \quad \varphi(a - a') + \varphi(b - b')e = 0, \quad \varphi(a) - \varphi(a') + (\varphi(b) - \varphi(b'))\, e = 0,$$

$$\varphi(a) + \varphi(b)\, e = \varphi(a') + \varphi(b')\, e.$$

b) ψ es morfismo.

Chequeemos únicamente un caso y lo demás quedará a cargo del lector:

$$\psi(a + b\sqrt{\alpha})\psi(a' + b'\sqrt{\alpha}) = \psi((a + b\sqrt{\alpha})(a' + b'\sqrt{\alpha})) \ :$$

$\psi(a + b\sqrt{\alpha})\psi(a' + b'\sqrt{\alpha}) = (\varphi(a) + \varphi(b)\, e)(\varphi(a') + \varphi(b')\, e) =$

$= \varphi(a)\varphi(a') + \varphi(b)\varphi(b')\, e^2 + (\varphi(b)\varphi(a') + \varphi(a)\varphi(b'))\, e$. Pero $e^2 = \varphi(\alpha)$, entonces:

$= \varphi(aa' + \alpha\, bb') + \varphi(ba' + ab')\, e = \psi(aa' + \alpha\ bb' + (ba' + ab')\sqrt{\alpha}) =$

$= \psi((a + b\sqrt{\alpha})(a' + b'\sqrt{\alpha}))$

c) ψ preserva el orden (o sea es morfismo de cuerpos ordenados)

Bastaría estudiar el caso $a + b\sqrt{\alpha} > 0$ (análogamente para $a + b\sqrt{\alpha} < 0$).Veamos

$$\psi(a + b\sqrt{\alpha}) = \varphi(a) + \varphi(b)\ e > 0$$

Recordemos que $a + b\sqrt{\alpha} > 0 \iff \begin{cases} a > 0 & y & b = 0 \\ a \geq 0 & y & b > 0 \\ a < 0 & y & b > 0 & y & \alpha > (-\frac{a}{b})^2 \\ a > 0 & y & b < 0 & y & \alpha < (-\frac{a}{b})^2 \end{cases}$

Caso 1: $a > 0$ y $b = 0$.
Luego $\varphi(a) > 0$ pues φ es morfismo de cuerpos ordenados.

Caso 2: $a \geq 0$ y $b > 0$.
Se deduce que $\varphi(\frac{a}{b}) \geq 0 > -e$, luego $\varphi(a) + \varphi(b)\, e > 0$.

Caso 3: $a < 0$ y $b > 0$ y $\alpha > (-\frac{a}{b})^2$.
Como $e^2 = \varphi(\alpha) > \varphi(-\frac{a}{b})^2$ entonces $e^2 - \varphi(-\frac{a}{b})^2 > 0$, o sea $(e - \varphi(-\frac{a}{b}))(e + \varphi(-\frac{a}{b})) > 0$. Pero como $e + \varphi(-\frac{a}{b}) > 0$ luego $e - \varphi(-\frac{a}{b}) > 0$, con lo cual $\varphi(a) + \varphi(b)\, e > 0$.

Caso 4: $a > 0$ y $b < 0$ y $\alpha < (-\frac{a}{b})^2$.
Similar al caso anterior.

□

Observar que para construir $\mathbb{K}[\sqrt{\alpha}]$ no tuvimos que decidir si α ya tiene raíz cuadrada en $\mathbb{K}$ o no. En síntesis, hemos logrado sumergir mediante un proceso unificado a $\mathbb{K}$ en el menor cuerpo (salvo isomorfismos) que contiene las raíces cuadradas de α.

5. LA CLAUSURA PITAGÓRICA CONSTRUCTIVA

Nos interesa ahora sumergir a $\mathbb{K}$ en un cuerpo pitagórico. Es decir, tal que todo elemento positivo tenga raíz cuadrada (en particular, se tendrán raíces cuadradas para todos los elementos positivos de $\mathbb{K}$).

Podemos repetir el proceso de la sección anterior con un segundo elemento positivo β de $\mathbb{K}$ y conseguir así

$$\mathbb{K} \longrightarrow \mathbb{K}[\sqrt{\alpha}] \longrightarrow \mathbb{K}[\sqrt{\alpha}][\sqrt{\beta}] = \mathbb{K}[\sqrt{\alpha}, \sqrt{\beta}]$$

un cuerpo totalmente ordenado e intuicionista que contiene las raíces cuadradas de dos elementos positivos de $\mathbb{K}$.

Esto se puede repetir una cantidad finita de veces obteniendo

$$\mathbb{K} \longrightarrow \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$$

Este proceso admite sólo finitas repeticiones ¿Cómo hacer entonces para construir un cuerpo $\mathbb{K}_1$ que contenga a $\mathbb{K}$ y a todas sus raíces cuadradas? Éste es nuestro objetivo immediato. Advertimos que este cuerpo no será todavía pitagórico, es decir, si bien contiene todas las raíces cuadradas de los elementos positivos de $\mathbb{K}$, todavía le faltarán las raíces cuadradas de sus propios elementos que no estén en $\mathbb{K}$. Recién en una segunda etapa podremos sumergir a $\mathbb{K}$ en su clausura pitagórica.

Resulta claro que cada vez que agregamos la raíz cuadrada de un elemento, por iteración de la propiedad universalse tiene:

5.1. *Propiedad universal de* $\mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$

i) Se tiene un cuerpo totalmente ordenado intuicionista $\mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$ *y un morfismo de cuerpos ordenados*

$$\mathbb{K} \xrightarrow{\lambda} \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}], \quad \lambda(\alpha_i) = \sqrt{\alpha_i}^2, \quad \sqrt{\alpha_i} > 0, \quad 1 \leq i \leq n.$$

ii) Para todo cuerpo intuicionista totalmente ordenado E y morfismo de cuerpos ordenados

$$\varphi : \mathbb{K} \to E, \quad e_i \in E, \quad \varphi(\alpha_i) = e_i^2, \quad e_i > 0, \quad 1 \leq i \leq n,$$

existe un único morfismo de cuerpos totalmente ordenados $\psi : \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}] \to E$ *tal que* $\psi(\sqrt{\alpha_i}) = e_i$ *y que hace conmutar el siguiente diagrama.*

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{\lambda} & \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}] \\ & \searrow^{\varphi} & \vdots \, \psi \\ & & \downarrow \\ & & E \end{array}$$

En particular si $I = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq J = \{\beta_1, \beta_2, ..., \beta_m\}$ existe un único morfismo de cuerpos ordenados, que denotamos $\psi_{I,J}$, que hace conmutar el siguiente diagrama

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}] \\ & \searrow & \vdots \, \psi_{I,J} \\ & & \downarrow \\ & & \mathbb{K}[\sqrt{\beta_1}, \sqrt{\beta_2}, ..., \sqrt{\beta_m}] \end{array}$$

y tal que $\psi_{I,J}(\sqrt{\alpha_i}) = \sqrt{\beta_j}$ cuando $\alpha_i = \beta_j$.

Observemos que esto es sólo una manera precisa de decir que si $I \subset J$, $\mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$ es un subcuerpo de $\mathbb{K}[\sqrt{\beta_1}, \sqrt{\beta_2}, ..., \sqrt{\beta_m}]$. Tenemos esta familia de cuerpos indexada por los subconjuntos finitos de $\mathbb{K}$, y lo que se quiere hacer es tomar la "unión" de todos estos cuerpos (alli tendremos raíces cuadradas para todos los elementos positivos de $\mathbb{K}$). Si tuviésemos la clausura algebraica real de $\mathbb{K}$, todos estos cuerpos resultan subcuerpos de ella, y podemos entonces tomar la unión dentro de esta clausura. El problema es que en esta etapa, no se puede asumir la existencia constructiva de esta clausura. Para construir la "unión" de estos cuerpos, sin utilizar que son todos subcuerpos de un cuerpo más grande, se utiliza la técnica categórica del *colímite filtrante*.

De la unicidad se siguen claramente las siguientes ecuaciones:

$$I = J, \;\; \psi_{I,I} = id, \;\; y \; si \; I \subset J \subset K, \;\; \psi_{I,K} = \psi_{J,K} \circ \psi_{I,J} \tag{5.2}$$

Consideremos ahora la unión disjunta sobre las partes finitas de $\mathbb{K}$ de todos los $\mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$. Es decir

$$\widetilde{\mathbb{K}} = \coprod_{\{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq \mathbb{K}} \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$$

cuyos elementos son los pares (x, I) donde $I = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subseteq \mathbb{K}$ y $x \in \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}]$.

Definimos a continuación una relación de equivalencia en la unión disjunta:

$$(x, I) \sim (y, J) \iff \exists K \supset I, \; K \supset J, \; \psi_{I,K}(x) = \psi_{J,K}(y). \tag{5.3}$$

Observar que resulta equivalente suponer que $K = I \cup J$, y que de las ecuaciones 5.2 se sigue que la relación resulta reflexiva y transitiva. Además, es claramente decidible puesto que así lo es la igualdad en el cuerpo $\mathbb{K}[\sqrt{\gamma_1}, \sqrt{\gamma_2}, ..., \sqrt{\gamma_s}]$, con $K = I \cup J$. Tenemos:

Proposición 5.4. *La relación definida en 5.3 es una relación de equivalencia decidible(es decir, se tienen algoritmos que en un número finito de pasos permiten decidir si dos elementos están relacionados o no, lo que significa que el conjunto cociente es discreto en el sentido intuicionista).*

Ya estamos entonces en condiciones de proponer

$$\mathbb{K}_1 = \widetilde{\mathbb{K}}/_{\sim}$$

Debemos ver que $\mathbb{K}_1$ es un cuerpo totalmente ordenado intuicionista que contiene una copia de $\mathbb{K}$ y de las raíces cuadradas de todos sus elementos positivos junto con la propiedad universal correspondiente.

Proposición 5.5. $\mathbb{K}_1$ *es un cuerpo totalmente ordenado intuicionista. Más aún, todo elemento positivo de* $\mathbb{K}$ *tiene raíz cuadrada en* $\mathbb{K}_1$.

Demostración. Veamos los puntos principales de la demostración y el resto quedará a cargo del lector. Todas las operaciones y la relación de orden se definen tomando representantes en $\mathbb{K}[\sqrt{\gamma_1}, \sqrt{\gamma_2}, ..., \sqrt{\gamma_s}]$, para un índice $K = \{\gamma_1, \gamma_2, \ldots \gamma_s\}$ suficientemente grande. Por ejemplo, para $\eta = [(x, I)]$ y $\mu = [(y, J)]$ elementos de $\mathbb{K}_1$, definimos

$$\eta + \mu = [(\psi_{I,K}(x) + \psi_{J,K}(y)), K)]$$

donde K es cualquiera tal que $K \supset I$, $K \supset J$ (podemos fijar $K = I \cup J$ para definir el algoritmo que calcula la suma). Si hubiésemos tomado otros representantes $\eta = [(x, I')]$ y $\mu = [(y, J')]$, se tiene

$$[(\psi_{I,K}(x) + \psi_{J,K}(y)), K)] = [(\psi_{I',K'}(x) + \psi_{J',K'}(y)), K')]$$

pues ambos resultan iguales a $[(\psi_{I,K''}(x) + \psi_{J,K''}(y)), K'')]$ para cualquier $K'' \supset K$, $K'' \supset K'$. Notar que de nuevo las ecuaciones 5.2 resultan fundamentales, junto con el hecho que los morfismos de transición $\psi_{I,J}$ preservan la suma.

El resto de las operaciones algebraicas se tratan de la misma manera, y la relación de orden también. Definimos

$$\eta < \mu \iff \psi_{I,K}(x) < \psi_{J,K}(y).$$

donde K es cualquiera tal que $K \supset I$, $K \supset J$. Esta relación resulta bien definida y un orden total debido a las ecuaciones 5.2, a que los morfismos de transición son morfismos de cuerpos ordenados, y a que cada uno de los cuerpos $\mathbb{K}[\sqrt{\gamma_1}, \sqrt{\gamma_2}, ..., \sqrt{\gamma_s}]$ es totalmente ordenado.

Resulta claro además que los algoritmos para calcular las operaciones en cada uno de estos cuerpos definen un algoritmo para las respectivas operaciones en en $\mathbb{K}_1$. La relación de equivalencia que define $\mathbb{K}_1$ es decidible, de donde se sigue que la relación de orden y la igualdad en $\mathbb{K}_1$ también lo son debido a que así es el caso en cada uno de los cuerpos $\mathbb{K}[\sqrt{\gamma_1}, \sqrt{\gamma_2}, ..., \sqrt{\gamma_s}]$.

Veamos finalmente que todo elemento positivo de $\mathbb{K}$ tiene raíz cuadrada en $\mathbb{K}_1$. Sea $\alpha \in \mathbb{K}$, $\alpha > 0$. Entonces $[(\sqrt{\alpha}, I)]$, donde $I = \{\alpha\}$ es la raíz cuadrada de α. Pero esto esta claro puesto que lo es en el cuerpo $\mathbb{K}[\sqrt{\alpha}]$ (notar aquí un ligero abuso de notación, pues nos falta definir la immersión de $\mathbb{K}$ en $\mathbb{K}_1$, lo que haremos a continuacion). □

Para cada subconjunto $I \subset \mathbb{K}$, $I = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ se tiene un morfismo de cuerpos ordenados $\mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}] \xrightarrow{\lambda_I} \mathbb{K}_1$ definido por $\lambda(x) = [(x, I)]$. Vemos así que cada uno de estos cuerpos tiene una immersión en $\mathbb{K}_1$, y que este cuerpo resulta ser la unión de todos esos subcuerpos. Para $I = \emptyset$, se tiene $\mathbb{K} \xrightarrow{\lambda} \mathbb{K}_1$, $\lambda(x) = [(x, \emptyset)]$.

Vale la siguiente propiedad universal:

5.6. ***Propiedad universal de*** $\mathbb{K}_1$

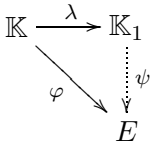
i) Se tiene un cuerpo totalmente ordenado intuicionista $\mathbb{K}_1$ *y un morfismo de cuerpos ordenados*

$$\mathbb{K} \xrightarrow{\lambda} \mathbb{K}_1, \quad \forall \alpha \in \mathbb{K},\ \alpha > 0,\ \ \lambda(\alpha) = [(\sqrt{\alpha}, \{\alpha\})]^2, \quad [(\sqrt{\alpha}, \{\alpha\})] > 0.$$

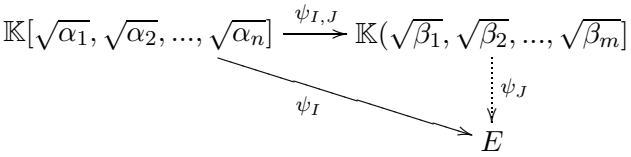
ii) Para todo cuerpo intuicionista totalmente ordenado E *y morfismo de cuerpos ordenados*

$$\varphi : \mathbb{K} \to E, \quad \forall \alpha \in \mathbb{K},\ \alpha > 0, \quad e_\alpha \in E, \quad \varphi(\alpha) = e_\alpha^2, \quad e_\alpha > 0,$$

existe un único morfismo de cuerpos totalmente ordenados $\psi : \mathbb{K}_1 \to E$ *tal que* $\psi([(\sqrt{\alpha}, \{\alpha\})]) = e_\alpha$ *y que hace conmutar el siguiente diagrama.*



Demostración. De 5.1 se sigue que para todo índice $I = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ se tiene un único morfismo de cuerpos ordenados $\psi_I : \mathbb{K}[\sqrt{\alpha_1}, \sqrt{\alpha_2}, ..., \sqrt{\alpha_n}] \to E$ tal que $\psi(\sqrt{\alpha_i}) = e_{\alpha_i}$. Notar que dado $I = \{\alpha_1, \alpha_2, ..., \alpha_n\} \subset J = \{\beta_1, \beta_2, ..., \beta_m\}$, el siguiente diagrama commuta:



Dado $[(x, I)] \in \mathbb{K}_1$, definimos $\psi([(x, I)]) = \psi_I(x)$. La verificación que ψ está bien definido, y que verifica todos los demás requerimientos es de rutina. □

Hemos sumergido a $\mathbb{K}$ en un cuerpo $\mathbb{K}_1$, $\mathbb{K} \hookrightarrow \mathbb{K}_1$, totalmente ordenado intuicionista tal que todo elemento positivo de $\mathbb{K}$ tiene raíz cuadrada en $\mathbb{K}_1$. Repitiendo el proseso, se obtiene $\mathbb{K}_1 \hookrightarrow \mathbb{K}_2$, donde están las raíces cuadradas de los elementos positivos de $\mathbb{K}_1$. Y así se sigue indefinidamente:

$$\mathbb{K} \overset{\psi_{0,1}}{\hookrightarrow} \mathbb{K}_1 \overset{\psi_{1,2}}{\hookrightarrow} \mathbb{K}_2 \overset{\psi_{2,3}}{\hookrightarrow} ... \hookrightarrow \mathbb{K}_n \overset{\psi_{n,n+1}}{\hookrightarrow} ...$$

Si $i < j$, definimos $\psi_{i,j} = \varphi_{j-1,j} \circ \psi_{j-2,j-1} \circ ... \circ \psi_{i,i+1}$. Si $i = j$, definimos $\psi_{i,i} = id$. Entonces se tienen las siguientes ecuaciones:

$$i = j,\ \ \psi_{i,i} = id,\ \ y\ si\ i < j < k,\ \ \psi_{i,k} = \psi_{j,k} \circ \psi_{i,j} \tag{5.7}$$

Tenemos así un sistema de cuerpos intuicionistas totalmente ordenados y morfismos de cuerpos ordenados con las mismas propiedades formales que antes, sólo que en lugar de estar indexado por los subconjuntos finitos de $\mathbb{K}$ está vez es una cadena indexada por los números naturales.

Se hace la construcción del colímite filtrante, que resulta ser un cuerpo intuicionista totalmente ordenado, exactamente de la misma manera. Primero se considera la unión disjunta:

$$\widetilde{\mathbb{K}} \ = \coprod_{n \in \mathbb{N}} \mathbb{K}_n \ = \{(\eta, i) \mid \eta \in \mathbb{K}_i\}.$$

y se define la relación de equivalencia:

$$(\eta, i) \sim (\mu, j) \Longleftrightarrow \psi_{i,k}(\eta) = \psi_{j,k}(\mu), \quad \textit{donde } \ k = max\{i, j\}.$$

El conjunto cociente $\overline{\mathbb{K}} = \widetilde{\mathbb{K}}/_{\sim}$ es claramente discreto (en el sentido intuicionista), y tiene una estructura de cuerpo totalmente ordenado intuicionista definiendo:

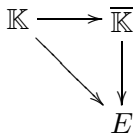
$$\begin{aligned}
[(\eta, i)] + [(\mu, j)] &= [(\psi_{i,k}(\eta) + \psi_{j,k}(\mu),\ k)] \\
[(\eta, i)].[(\mu, j)] &= [(\psi_{i,k}(\eta).\psi_{j,k}(\mu),\ k)] \\
[(\eta, i)]^{-1} &= [(\eta^{-1}, i)] \\
[(\eta, i)] < [(\mu, j)] &\iff \psi_{i,k}(\eta) < \psi_{j,k}(\mu)
\end{aligned}$$

Finalmente, resulta pitagórico, es decir, todo elemento positivo tiene raíz cuadrada. En efecto, si $[(\eta, i)] > 0$ con $\eta > 0$ en $\mathbb{K}_i$, y si $\mu \in \mathbb{K}_{i+1}$, $\mu > 0$ es tal que $\mu^2 = \psi_{i,i+1}(\eta)$, se tiene $[(\mu, i+1)]^2 = [(\psi_{i,i+1}(\eta), i+1)] = [(\eta, i)]$. Podemos escribir:

$$\sqrt{[(\eta, i)]} = [\sqrt{\psi_{i,i+1}(\eta)},\ i+1)]$$

Con una demostración que sigue las mismas líneas que la demostración de 5.6 tenemos:

Teorema 5.8 (Existencia constructiva de la Clausura Pitagórica)**.** *Dado un cuerpo totalmente ordenado intuicionista $\mathbb{K}$, se puede construir un cuerpo totalmente ordenado pitagórico intuicionista $\overline{\mathbb{K}}$ y una immersión de cuerpos ordenados $\mathbb{K} \hookrightarrow \overline{\mathbb{K}}$ que es universal en el sentido que dado cualquier otra immersión $\mathbb{K} \hookrightarrow E$ en un cuerpo totalmente ordenado pitagórico intuicionista E, se tiene $\overline{\mathbb{K}} \hookrightarrow E$ de manera tal que el siguiente diagrama resulta commutativo:*



Terminamos haciendo notar que este cuerpo ha sido construido explícitamente a partir de $\mathbb{K}$, y que se puede obtener una descripción precisa de sus elementos, y de algoritmos que permiten calcular todas las operaciones y decidir la relación de orden. También se tiene un algoritmo que calcula la raíz cuadrada positiva de todo elemento positivo. En consecuencia, si se tiene un software que permite operar en el cuerpo $\mathbb{K}$ con una computadora, también se tendrá un software que permita operar en el cuerpo $\overline{\mathbb{K}}$, incluyendo el cálculo de las raíces cuadradas de los elementos positivos.

Referencias

[1] A. Joyal, *Conferencia no publicada*, Universidad de Quebec en Montreal (1978).
[2] B.L. van der Waerden, *Modern Algebra*, revised english edition, Frederick Ungar Publishing Co, New York (1949-1953).