

Cuerpos Ordenados

J. Ignacio Padilla B

Universidad de Costa Rica

Teoría de Galois

27 de Noviembre, 2017

1 Introducción

La teoría de cuerpos ordenados es la rama de la teoría de cuerpos (o de Galois) que estudia las propiedades de los cuerpos en los cuales se puede definir un orden total, usualmente denotado por $<$. Al igual que muchas otras propiedades de cuerpos, la axiomatización de los cuerpos ordenados corresponde a una abstracción de los números reales \mathbb{R} , la cual se atribuye principalmente a David Hilbert, Otto Hölder, y Hans Hahn. Eventualmente esta teoría se desarrolló por Artin y Schreier.

En este trabajo se presentará una introducción a los conceptos de orden en cuerpos, y se presentarán varias definiciones de orden en cuerpos (y anillos). También se introducirán las condiciones necesarias para poder inducir un orden en un cuerpo K dado. Por último, se estudiarán las propiedades de los órdenes bajo las extensiones de cuerpos, con la intención de preparar al lector a los resultados de la teoría de cuerpos real cerrados.

2 Cuerpos Ordenados

Un **cuerpo ordenado**, denotado por $(K, <)$ es un cuerpo K en donde $<$ define un orden total. Además, el orden debe ser compatible con la estructura de cuerpo, es decir:

- C.O.1 Si $x \leq y \Rightarrow x + z \leq y + z$, para todo $x, y, z \in K$
- C.O.2 Si $x \leq y$ and $z \geq 0$, entonces $xz \leq yz$, para todo $x, y \in K$

Nota: Recuerde que la expresión $x \leq y$ corresponde a una abreviación de $x < y \vee x = y$, por lo tanto al hablar de orden, se usarán ambas sin distinción.

Cuando se tiene un cuerpo K junto a un orden \leq , es posible definir el conjunto de los elementos *positivos* del cuerpo. Definimos:

$$P = \{x \in K : x \geq 0\}$$

Denotamos los elementos *negativos* por:

$$-P = \{-x : x \in P\} = \{x \in K : x \leq 0\}$$

Note que bajo estas convenciones, 0 es positivo y negativo. Además, puede observarse que:

- i) $P + P \subseteq P$
- ii) $P \cdot P \subseteq P$
- iii) $P \cap -P = \{0\}$
- iv) $P \cup -P = K$

Proposición 1. Sea K un cuerpo. Si existe $P \subseteq K$ que cumple las propiedades i), ii), iii) y iv), entonces podemos inducir un orden total \leq_P de la siguiente manera:

$$x \leq_P y \iff y - x \in P$$

Además, \leq_P satisface C.O.1 y C.O.2 (o sea, es compatible con la estructura de cuerpo de K). Además, \leq_P satisface C.O.1 y C.O.2 (o sea, es compatible con la estructura de cuerpo de K).

Demostración: Tenemos que ver que \leq_P satisface condiciones de reflexividad, antisimetría, transitividad y totalidad. Además hay que verificar que \leq_P satisface C.O.1 y C.O.2.

- Como $0 \in P$, entonces para todo $x \in P$, $x - x \in P \Rightarrow x \leq_P x$. (*Reflexividad*).
- Si $x \leq_P y$, $y \leq_P x$, entonces se tiene que $y - x \in P$, $y - (y - x) \in P$. Por lo tanto $y - x = 0 \Rightarrow y = x$ (*Antisimetría*).
- Si $x \leq_P y$, $y \leq_P z$, entonces $y - x \in P$, $y - z \in P$. Entonces $y - x + z - y = z - x \in P$, es decir: $x \leq_P z$ (*Transitividad*).
- Si $x, y \in P$, entonces $x - y \in P$ ó $x - y \in -P$ (esto pues $P \cup -P = K$). O sea que $x \leq_P y$ ó $y \leq_P x$ (*Totalidad*).
- Si $x \leq_P y$, entonces $y - x = y + z - z - x \geq_P 0$. Entonces $y + z \geq_P x + z$ (*C.O.1*).
- Si $x \leq_P y$, $z \geq_P 0$, como $y - x \in P \wedge z \in P$, entonces $z(y - x) = zy - zx \geq_P 0 \Rightarrow zy \geq_P zx$ (*C.O.2*).

Por lo tanto se concluye que (K, \leq_P) es un cuerpo ordenado. ■

Lo que nos dice el resultado anterior, es que en realidad el orden de un cuerpo dado puede ser determinado definiendo primero el conjunto de los números que se desean positivos (siempre y cuando cumplan las propiedades de la hipótesis). De ahora en adelante, cuando se hable de orden, se puede considerar el conjunto P y la relación $<_P$ ($<$, brevemente), sin distinción alguna.

Como el lector habrá notado, la definición de cuerpo ordenado no utiliza realmente las propiedades de cuerpo de la estructura (tal vez únicamente la conmutatividad, implícitamente). De hecho, se puede definir análogamente un **anillo ordenado** como un anillo A , en donde existe un conjunto $P \subseteq A$ tal que:

- i. $P + P \subseteq P$
- ii. $P \cdot P \subseteq P$
- iii. $P \cap -P = \{0\}$

$$\text{iv. } P \cup -P = A$$

En este caso, se tiene una definición más general, puesto que no se necesita que este orden satisfaga C.O.1 ni C.O.2. Esta definición será útil para ordenar anillos de polinomios como se verá en secciones siguientes. A continuación se tiene un lema interesante: **Lema 2:** Sean P_1 y P_2 , dos órdenes sobre un cuerpo K , tales que $P_1 \subseteq P_2$. Entonces $P_1 = P_2$

Demostración. Supongamos que existe $x \in P_2 \setminus P_1$. Entonces

$$\begin{aligned} x \in -P_1 &\Rightarrow -x \in P_2 \\ &\Rightarrow x = 0 \\ &\Rightarrow 0 \notin P_1 \\ &\Rightarrow 0 < 0 \\ &\Rightarrow \Leftarrow \end{aligned}$$

■

Ejemplo 3:

- (\mathbb{R}, \leq) es un cuerpo ordenado, con su orden usual. En este caso $P = \mathbb{R}^+ \cup \{0\}$. Luego veremos que este es el único orden posible en \mathbb{R} .
- (\mathbb{Q}, \leq) es un cuerpo ordenado, con el orden heredado de \mathbb{R} . También ocurre que hay un único orden que satisface los axiomas de CO.
- \mathbb{C} no es un cuerpo ordenado. Esto se mostrará al final del capítulo.

Proposición 4: Si $x, y \in (K, <)$ son tales que $x, y < 0$, entonces $xy > 0$. Esto pues como $-x \in P$ $-y \in P$, entonces $(-x)(-y) = xy \in P$. En particular: $x^2 \geq 0$ para todo x .

Vamos ahora a estudiar algunas posibilidades de orden en anillos polinomiales. Más específicamente, considere el anillo de polinomios con coeficientes reales $\mathbb{R}[x]$. Sea $p(x) \in \mathbb{R}[x]$,

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

Definimos el **orden en infinito** ($>_{+\infty}$) en $\mathbb{R}[x]$ como:

$$p(x) >_{+\infty} 0 \iff a_n > 0$$

A manera aclaratoria:

$$p(x) \geq_{+\infty} 0 \iff p(x) >_{+\infty} 0 \text{ o } p(x) = 0$$

Entonces podemos definir el conjunto P de polinomios positivos:

$$P = \{p(x) \in \mathbb{R}[x] : p(x) \geq_{+\infty} 0\}$$

Proposición 5: $(\mathbb{R}[x], P)$ es un anillo ordenado.

Demostración. Solo necesitamos verificar:

- i. $P + P \subseteq P$
- ii. $P \cdot P \subseteq P$
- iii. $P \cap -P = \{0\}$
- iv. $P \cup -P = A$

Las propiedades i), ii) y iv) se deducen fácilmente. Para demostrar iii), tome $p(x) \in P \cap -P$, entonces si $p(x) \neq 0$, se tiene que $a_n > 0 \wedge a_n < 0$, lo cual no es posible. Por lo tanto $p(x) = 0$. ■

Algunas observaciones:

- Si $p, q \in \mathbb{R}[x]$, de tal manera que $\deg p > \deg q$, entonces $p(x) - q(x) > 0$ si y sólo si $p(x) > 0$. En otras palabras, $p(x) > q(x)$, para todo q con grado menor a p .
- En un caso particular de esta observación, se puede notar que para todo $r \in \mathbb{R}$:

$$x - r >_{+\infty} 0$$

Es decir:

$$x >_{+\infty} r$$

Obtuvimos un elemento en $\mathbb{R}[x]$ que es mayor a todos los números reales, algo que no es posible con el orden $>$ de los reales. A estos elementos les llamamos **infinitos**.

- $>_{+\infty}$ extiende al orden usual de \mathbb{R} , en el sentido que, si consideramos a $a \in \mathbb{R}$ como un polinomio constante, entonces:

$$a >_{+\infty} 0 \iff a > 0$$

O sea que para las constantes, $>_{+\infty}$ coincide con $>$.

Pronto estudiaremos otros órdenes posibles en $\mathbb{R}[x]$. Por ahora consideremos el siguiente lema:

Lema 6: Sea (A, P) un anillo commutativo entero y ordenado. Entonces $K = \text{Frac}(A)$ es un cuerpo ordenado (K, Q) en donde el conjunto Q de elementos positivos se define como:

$$Q = \left\{ \frac{a}{b} \in K : ab \in P \right\}$$

Demostración. Hay que verificar que:

- i. $Q + Q \subseteq Q$
- ii. $Q \cdot Q \subseteq Q$
- iii. $Q \cap -Q = \{0\}$
- iv. $Q \cup -Q = K$
- i) Sean $\frac{a}{b}, \frac{c}{d} \in Q$ Recuerde que $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Entonces hay que ver que:

$$bd(ad+bc) = abd^2 + b^2cd \in P$$

Pero $ab \in P$ y $cd \in P$, y como todo cuadrado es positivo, obtenemos que Q es cerrado bajo suma.

- ii) Sean $\frac{a}{b}, \frac{c}{d} \in Q$. Entonces es trivial que $\frac{ac}{bd} \in Q$, puesto que $abcd \in P$
- iii) Claramente $0 \in Q$, pues $0 = \frac{0}{1} = -\frac{0}{1}$. Si $\frac{a}{b} \in Q \cap -Q$, entonces $ab \in P$ y $ab \in -P$. Entonces $ab = 0 \Rightarrow a = 0$.
- iv) Claramente $Q \cup -Q \subseteq K$. Si $\frac{a}{b} \in K$, entonces considere $ab \in A$. Ahora:

$$ab \in P \text{ o } ab \in -P$$

Es decir:

$$\Rightarrow \frac{a}{b} \in Q \text{ o } \frac{a}{b} \in -Q$$

■

Ejemplo 7:

- Retomemos el orden $>_{+\infty}$ que se definió anteriormente en $\mathbb{R}[x]$. Ahora podemos extenderlo al cuerpo de fracciones racionales en una variable:

$$\mathbb{R}(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in \mathbb{R}[x], q(x) \neq 0 \right\}$$

Entonces considere la extensión de orden dada por el lema 6:

$$\frac{p(x)}{q(x)} \geq_{+\infty} 0 \iff p(x)q(x) \geq_{+\infty} 0$$

Observe que el coeficiente principal de $p(x)q(x)$ es el producto de los coeficientes principales de p y de q , por lo tanto el signo de la expresión $\frac{p(x)}{q(x)}$ depende del signo de la fracción a_n/b_m , en donde a_n y b_m son los coeficientes principales de $p(x)$ y $q(x)$, respectivamente. Además, se sigue cumpliendo que $x >_{+\infty} r$ para cualquier real r , puesto que el orden en el cuerpo de fracciones es una ‘extensión’ del orden del anillo de polinomios. Más precisamente, cuando las expresiones tienen denominador 1, su orden coincide con el definido anteriormente en el anillo.

- Considere ahora la transformación $x \mapsto -x$ junto con el orden $>_{+\infty}$. Vamos a definir el **orden en menos infinito** (“ $>_{-\infty}$ ”), en $\mathbb{R}(x)$ de la siguiente manera:

$$\frac{p(x)}{q(x)} \geq_{-\infty} 0 \iff \frac{p(-x)}{q(-x)} \geq_{+\infty} 0$$

Note que la expresión $p(-x)$ cambia los coeficientes a_{2n-1} de signo. En particular se puede apreciar que:

$$\begin{aligned} p(x) &\geq_{-\infty} 0 \iff p(-x) >_{+\infty} 0 \\ &\iff \begin{cases} a_n > 0, & \text{si } n \text{ es impar} \\ a_n < 0, & \text{si } n \text{ es par} \end{cases} \end{aligned}$$

Observe que:

- $x^2 + 1 \geq_{-\infty} 0$
- $x + 1 \leq_{-\infty} 0$
- $-x^2 + 1 \leq_{-\infty} 0$
- $-x + 1 \geq_{-\infty} 0$
- $x \leq_{-\infty} r, \quad \forall r \in \mathbb{R}$
- $x^2 \geq_{-\infty} r, \quad \forall r \in \mathbb{R}$

En este orden tenemos que x corresponde a un **infinito negativo**, mientras que x^2 corresponde a un infinito.

3. Ahora considere la transformación $x \mapsto \frac{1}{x}$, otra vez junto al orden $\geq_{+\infty}$. Vamos a definir el **orden en 0^+** (“ $>_{0^+}$ ”) en $\mathbb{R}(x)$ por medio de:

$$\frac{p(x)}{q(x)} \geq_{0^+} 0 \iff \frac{p(\frac{1}{x})}{q(\frac{1}{x})} \geq_{+\infty} 0$$

Para estudiar este orden más detalladamente, observe que si tomamos

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_k x^k$$

con $a_n \neq 0$ y $a_k \neq 0$, se tiene que:

$$\begin{aligned} p(x) >_{0^+} 0 &\iff p\left(\frac{1}{x}\right) >_{+\infty} 0 \\ &\iff a_n \frac{1}{x^n} + \cdots + a_k \frac{1}{x^k} >_{+\infty} 0 \\ &\iff \frac{a_n + a_{n-1}x + \cdots + a_k x^{n-k}}{x^n} >_{+\infty} 0 \\ &\iff a_n + a_{n-1}x^{n-1} + \cdots + a_k x^{n-k} >_{+\infty} 0 \\ &\text{pues ya sabemos que } x^n >_{+\infty} 0 \\ &\iff a_k > 0. \end{aligned}$$

O sea que el orden en 0^+ depende del último coeficiente no 0. Observe que bajo este orden se tiene lo siguiente:

$$\begin{aligned} x &>_{0^+} 0 \\ x - r &<_{0^+} 0 \quad \forall r > 0 \end{aligned}$$

Es decir, para todo $r > 0$ se tiene que:

$$0 <_{0^+} x <_{0^+} r$$

Vemos que en este orden tenemos un elemento más cercano a 0 que cualquier número real. A estos elementos les llamamos **infinitésimos**.

4. Otra posibilidad es considerando la transformación $x \mapsto \frac{1}{x}$, y definimos **el orden en 0^-** “($>_{0^-}$)” en $\mathbb{R}(x)$ como:

$$\frac{p(x)}{q(x)} \geq_{0^-} 0 \iff \frac{p(-\frac{1}{x})}{q(-\frac{1}{x})} \geq_{+\infty} 0$$

Análogamente al orden en $-\infty$, se puede llegar a ver que:

$$\begin{aligned} p(x) >_{0^-} 0 &\iff p(-x) >_{0^+} \\ &\iff \begin{cases} a_k > 0, & \text{si } k \text{ es impar} \\ a_k < 0, & \text{si } k \text{ es par} \end{cases} \end{aligned}$$

En donde a_k es el coeficiente que acompaña a la menor potencia de x . En este orden vemos que:

- $x <_{0^-} 0$
- $x >_{0^-} r \quad \forall r < 0$

Entonces:

$$r <_{0^-} x <_{0^-} 0 \quad \forall r < 0$$

Observamos que x es un **infinitésimo negativo**.

5. **Ejercicio:** Se invita al lector a generalizar estos órdenes, y formular, dado $a \in \mathbb{R}$, los órdenes $>_{a^+}$ y $>_{a^-}$, de tal manera que se tenga que el elemento x represente una cantidad **infinitesimalmente mayor** a a (en el primer caso), y una cantidad **infinitesimalmente menor** a a en el segundo.

Los ejemplos anteriores representan una vista muy interesante a las posibles extensiones de un orden total en un cuerpo, permitiendo ordenar el cuerpo de expresiones polinomiales racionales sobre dicho cuerpo. Incluso, esta herramienta es útil a la hora de formalizar los conceptos de infinitos e infinitésimos, los cuales son ampliamente usados en el análisis no estándar.

3 Cuerpos Formalmente Reales

En esta sección estudiaremos la siguiente interrogante: ¿Qué condiciones debe cumplir un cuerpo K , para que en él se pueda definir un orden total (equivalentemente, un conjunto de elementos positivos), que satisfaga los axiomas de cuerpos ordenados? **Definición 8:** Sea K un cuerpo. Entonces:

- Decimos que K es **formalmente real** (o solo real) (u ordenable), si admite al menos un orden total, compatible con la estructura de cuerpo (C.O.1 y C.O.2).
- Sea $X \subseteq K$. Decimos que X es **formalmente positivo** si existe un orden P de K tal que $X \subseteq P$.

Lema 9: Sea K un cuerpo cualquiera. Entonces K es formalmente real si y sólo si $\{0, 1\}$ es formalmente positivo.

Demostración.

\Leftarrow Trivial. Se sigue de las definiciones.

\Rightarrow Sea $P \subseteq K$ un orden, entonces ya tenemos que $0 \in P$. Solo hay que mostrar que $1 \in P$. Suponga que no. Entonces $-1 \in P \Rightarrow 1 = (-1)^2 \in P$, lo cual es contradictorio. ■

Gracias a este lema podemos entonces decir que, dado cualquier orden en un cuerpo K , el conjunto $\{0, 1\}$ es positivo. En particular $1 > 0$ en cualquier cuerpo ordenado. **Proposición 10:** Si K es un cuerpo formalmente real, entonces $\text{car } K = 0$. Pues del contrario, si $\text{car } K = p$, como $1 > 0$, entonces se tiene la desigualdad imposible:

$$0 < \overbrace{1 + 1 + \cdots + 1}^{p \text{ veces}} = 0$$

Dado un cuerpo K y para $F \subseteq K$ un subconjunto multiplicativamente cerrado ($F \cdot F \subseteq F$), y de manera que $\{0, 1\} \in F$. Vamos a definir el siguiente conjunto, el cual será de mucha ayuda en los resultados siguientes:

$$\Sigma FK^2 := \left\{ \sum_{i=1}^n a_i x_i^2 : a_i \in F, x_i \in K, n \in \mathbb{N}, \text{ con } i = 1, \dots, n \right\}$$

El cual corresponde a la sumas de elementos de F multiplicados por cuadrados de K . **Teorema 11:** Sea K tal que $\text{car } K \neq 2$, y sea $F \subseteq K$ tal que $F \cdot F \subseteq F$, y $\{0, 1\} \in F$. Entonces las siguientes condiciones son equivalentes.

- 1) F es formalmente positivo
- 2) $\Sigma FK^2 \subsetneq K$
- 3) $-F \cap \Sigma FK^2 = \{0\}$
- 3'. $-1 \notin \Sigma FK^2$
- 4) Si dados $a_1, a_2, \dots, a_n \in F \setminus \{0\}$, existen $x_1, x_2, \dots, x_n \in K$, tal que $\sum_{i=1}^n a_i x_i^2 = 0$, entonces $x_1 = x_2 = \dots = x_n = 0$.
- 5) Existe $S \subseteq K$ tal que:
 - i) $F \subseteq S$
 - ii) $K^2 \subseteq S$
 - iii) $S + S \subset S$
 - iv) $S \cdot S \subseteq S$
 - v) $S \cap -S = \{0\}$

Es decir, se puede definir al menos un orden parcial en K que hace positivos a los elementos de F (y a los cuadrados).

Demostración. Se puede observar fácilmente que $3' \Rightarrow 2$ y que $3) \Rightarrow 3'$). Vamos a demostrar $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 5) \Rightarrow 1)$.

- 1) \Rightarrow 2): Tome $F \subseteq P$, como $K^2 \subseteq P$, se sigue que $\Sigma F K^2 \subseteq P$, pues suma y producto de positivos es positivo. Entonces tenemos que $\Sigma F K^2 \subseteq P \subsetneq K$, pues -1 nunca es positivo. Por lo tanto $\Sigma F K^2 \subsetneq K$.
- $\neg 3) \Rightarrow \neg 2)$: Suponga que existe $a \in F$ no cero, de tal forma que $-a \in \Sigma F K^2$. Entonces veremos que $\Sigma F K^2 = K$. Sea $y \in K$. Como $2a \neq 0$, llamemos:

$$\begin{aligned} x &= \frac{y - a}{2a} \\ \Rightarrow y &= 2ax + a \\ &= a(x + 1)^2 - ax^2 \end{aligned}$$

Entonces $y \in \Sigma F K^2$. Por lo tanto $\Sigma F K^2 = K$ y obtenemos la negación de 2).

- $\neg 4) \Rightarrow \neg 3)$: Por contraposición, sean $a_1, a_2, \dots, a_n \in F \setminus \{0\}$, y $x_1, x_2, \dots, x_n \in K$ no todos cero, tal que $\sum_{i=1}^n a_i x_i^2 = 0$. Asumamos, sin pérdida de generalidad, que $x_1 \neq 0$. Entonces:

$$-a_1 = \sum_{i=2}^n a_i \left(\frac{x_i}{x_1} \right)^2 \in \Sigma F K^2$$

Entonces se sigue que $-a_1 \in -F \cap \Sigma F K^2$, donde a_1 no es nulo. Hemos negado 3).

- 4) \Rightarrow 5): Veremos que el orden que necesitamos es $\Sigma F K^2$. Sea $S = \Sigma F K^2$. Claramente $F \subseteq S$ y también $K^2 \subseteq S$. También es fácil ver que $S + S \subseteq S$ y que $S \cdot S \subseteq S$. Solo haría falta ver que $S \cap -S = \{0\}$, en particular solo necesitamos la inclusión \subseteq .
Sea $y \in S \cap -S$. Entonces:

$$\begin{aligned} y &= \sum_{i=1}^n a_i x_i^2 \quad ; \quad -y = \sum_{j=1}^m b_j z_j^2 \quad \text{con } m, n \in \mathbb{N} \\ \Rightarrow \sum_{i=1}^n a_i x_i^2 + \sum_{j=1}^m b_j z_j^2 &= 0 \\ \Rightarrow x_i, z_j &= 0 \end{aligned}$$

- 5) \Rightarrow 1): Sea \mathcal{F} la familia de subconjuntos $S \subseteq K$ que verifican las propiedades i), ii), iii) y iv) de la hipótesis (5). Entonces tenemos que \mathcal{F} no es vacía, pues $S \in \mathcal{F}$. Ordenamos parcialmente a \mathcal{F} por inclusión, y entonces vemos que si $(S_i)_{i \in I}$ es una cadena de elementos en \mathcal{F} , entonces $\bigcup_{i \in I} S_i$ está en \mathcal{F} (toda cadena está acotada superiormente). Entonces vemos que la familia \mathcal{F} es un conjunto ordenado parcialmente, en donde toda cadena tiene una cota superior. Por el lema de Zorn, existe un elemento $Q \in \mathcal{F}$ que es maximal. Como $Q \subseteq K$ está en \mathcal{F} , entonces satisface i), ii), iii), iv). Solo hace falta verificar que Q es un orden total, es decir: $Q \cup -Q = K$

Sea $x \in K$ tal que $x \notin Q$, entonces debemos ver que $-x \in Q$. Consideremos el conjunto $Q' = Q - xQ = \{c - xd \mid c, d \in Q\}$. Como $0 \in Q$, entonces $Q \subseteq Q'$, y por lo tanto $F \subseteq Q'$ y $K^2 \subseteq Q'$. Es sencillo ver que $Q' + Q' \subseteq Q'$ y $Q' \cdot Q' \subseteq Q'$. Veamos ahora que $Q' \cap -Q' = \{0\}$.

Para esto, sea $y \in Q' \cap -Q'$. Entonces $y = c_1 - xd_1$ y $-y = c_2 - xd_2$, con $c_1, c_2, d_1, d_2 \in Q$. Es decir, $(c_1 + c_2) - x(d_1 + d_2) = 0$, y luego $c_1 + c_2 = x(d_1 + d_2)$. Suponga ahora que $d_1 + d_2 \neq 0$, entonces:

$$x = \frac{c_1 + c_2}{d_1 + d_2} = \frac{(c_1 + c_2)(d_1 + d_2)}{(d_1 + d_2)^2}$$

Entonces x es un producto entre un cuadrado y un elemento en Q , por lo tanto $x \in Q$ (pues Q contiene a K^2 y es multiplicativamente cerrado). Pero esto es una contradicción!. Entonces debe cumplirse que $d_1 + d_2 = 0$ y $c_1 + c_2 = 0$. Luego $d_1 = -d_2$, o sea d_1 es positivo y negativo, y por lo tanto $d_1 = d_2 = 0$. Análogamente se tiene que $c_1 = c_2 = 0$. Entonces $y = 0$. Entonces Q' satisface la hipótesis 5), o sea $Q' \in \mathcal{F}$, pero como $Q \subseteq Q'$, y por la maximalidad de Q , de tiene que $Q = Q'$, por lo tanto $-x \in Q' = Q$. Entonces Q es el orden total que estábamos buscando.

■

Este teorema es una herramienta muy útil para determinar si un conjunto dado en un cuerpo, es positivo en algún orden. Más específicamente, apliquemos el teorema anterior en un cuerpo K , tomando $F = \{0, 1\}$. Recuerde que K es formalmente real si y solo si $\{0, 1\}$ es formalmente positivo. **Corolario 12:** Sea K un cuerpo con característica distinta de 2. Entonces las siguientes condiciones son equivalentes:

- i) K es formalmente real.
- ii) Si $\sum_{i=1}^n x_i^2 = 0$, entonces $x_1 = x_2 = \dots = x_n = 0$, para todo $x_i \in K$, para todo $n \in \mathbb{N}$.
- iii) $-1 \notin \Sigma K^2$

Demostración. Aplique el Teorema 11 , con $F = \{0, 1\}$. Observe que $\Sigma F K^2 = \Sigma K^2$.

■

Corolario 13: \mathbb{C} no es formalmente real. O sea \mathbb{C} no puede ser ordenado.

■

Demostración. Observe que $-1 = i^2 \in \mathbb{C}^2$

Corolario 14: Sea (K, P) un cuerpo ordenado y $L|K$ una extensión de cuerpos. Entonces lo siguiente equivale:

1. L tiene un orden que extiende al de K . (Es decir, si un elemento es positivo en K , también lo es en L).
2. $\Sigma P L^2 \subsetneq L$
3. $(-P) \cap \Sigma P L^2 = \{0\}$.
- 3'. $-1 \notin \Sigma P L^2$
4. $\sum_{i=1}^n a_i x_i = 0 \Rightarrow x_i = 0, \quad i = 1, \dots, n$

Demostración. Aplique el Teorema 11 a $P = F$, y a $K = L$. Note que el orden P de K es multiplicativamente cerrado, y contiene a $\{0, 1\}$.

■

Incluso se puede aplicar más generalmente: **Corolario 15:** Sea K un cuerpo real. Sea $L|K$ una extensión y $F \subseteq K$ una parte formalmente positiva. Entonces las siguientes aserciones son equivalentes:

1. Todo orden de K que contiene a K se extiende a un orden de L .
2. Para todo P orden de K , tal que $F \subseteq P$, se tiene que $\Sigma PL^2 \subsetneq L$.
3. Para todo P orden de K , tal que $F \subseteq P$, si $\sum_{i=1}^n a_i x_i = 0 \Rightarrow x_i = 0, i = 1, \dots, n$, con $a_i \in P^*$ y $x_i \in L$.
4. Para todo P orden de K , tal que $F \subseteq P$, se cumple que $(-P) \cap \Sigma PL^2 = \{0\}$

A continuación, daremos una caracterización del “más pequeño” posible orden que se puede definir en un cuerpo real.

Proposición 16: Sea K un cuerpo real y $a \in K$. Entonces $a \in P$ para todo orden P si y sólo si $a \in \Sigma K^2$. Es decir:

$$\Sigma K^2 = \bigcap \{P : P \text{ orden en } K\}$$

Demostración.

\Leftarrow Si $a \in \Sigma K^2$, entonces tome cualquier orden P de K , como $K^2 \subseteq P \Rightarrow a \in P$.

\Rightarrow Sea $a \notin \Sigma K^2$. Necesitamos un orden P de K tal que $-a \in P$ (o sea que a sea negativo). Considere el conjunto $F = \langle 0, 1, -a \rangle$

$$F = \{0, 1, -a, a^2, -a^3, a^4, -a^5, \dots\}$$

Bastaría entonces ver que F es formalmente positivo. Por el teorema 11, esto es lo mismo que ver que existe un orden parcial S en donde F sea positivo. Entonces tomemos $S = \Sigma F K^2$. Claramente $S + S \subseteq S$, $S \cdot S \subseteq S$, $F \in S$, $K^2 \in S$. Solo necesitamos ver que $S \cap -S = \{0\}$. Si $y \in S \cap -S$, entonces

$$y = \sum_{i=1}^n a_i x_i^2 \quad ; \quad -y = \sum_{j=1}^m b_j z_j^2$$

Con $a_i, b_i \in F$. Entonces, debido a la forma de los elementos de F puede verse que y se puede escribir de la forma:

$$y = c_1 - ad_1 = -(c_2 - ad_2)$$

En donde $c_1, c_2, d_1, d_2 \in \Sigma K^2$. Despejando a y suponiendo que $d_1 + d_2 \neq 0$, se tiene que:

$$a = \frac{(c_1 + c_2)(d_1 + d_2)}{(d_1 + d_2)^2}$$

Lo cual indica que $a \in \Sigma K^2$. Esto no es posible. Entonces debe cumplirse que $d_1 + d_2 = 0$. Entonces $d_1 = d_2 = 0 \Rightarrow c_1 = c_2 = 0$. Por lo tanto $y = 0$, que es lo que se buscaba. ■

Corolario 17: Sea K un cuerpo real. Las siguientes condiciones son equivalentes:

- i) K tiene solo un orden.
- ii) ΣK^2 es un orden de K .
- iii) $\Sigma K^2 \cap -\Sigma K^2 = \{0\}$ y $\Sigma K^2 \cup -\Sigma K^2 = K$

Demostración.

- 1) \Rightarrow 3): Sea P dicho orden. Entonces $\Sigma K^2 = \bigcap P = P$. Como P cumple que $P \cap -P = \{0\}$ y $P \cup -P = K$, entonces inmediatamente obtenemos 3).
- 3) \Rightarrow 2): Obviamente $\Sigma K^2 + \Sigma K^2 \subseteq \Sigma K^2$, y $(\Sigma K^2)(\Sigma K^2) \subseteq \Sigma K^2$. Agregando la hipótesis 3), entonces tenemos las condiciones suficientes para poder inducir el orden $>_{\Sigma K^2}$
- 2) \Rightarrow 1): Sea P cualquier orden de K . Sabemos que $\Sigma K^2 \subseteq P$. Entonces por el lema 2, entonces $\Sigma K^2 = P$. Entonces K solo tiene el orden ΣK^2

■

El lema anterior es muy interesante, pues nos dice que si los cuadrados de K , permiten ordenarlo, entonces el orden que consiste precisamente de los cuadrados de K , es el único compatible con la estructura de cuerpo. Esto nos va a permitir concluir que \mathbb{R} solo tiene un orden (el usual), puesto que todos los elementos positivos de \mathbb{R} , son precisamente, cuadrados.

A manera de comentario: a lo largo de esta sección hemos visto algunos resultados acerca de las condiciones necesarias para que un cuerpo sea real. Posiblemente la más importante de todas es el hecho de que, dado un cuerpo K , si -1 es suma finita de cuadrados, entonces no es posible ordenar a K . En otras palabras, no es posible definir un orden en donde las sumas de cuadrados sean menores a 0.

4 Extensiones algebraicas a extensiones de órdenes

En esta sección estudiaremos brevemente, qué sucede con el orden de un cuerpo real, cuando éste se extiende finita, y algebraicamente

Considere $E|K$ una extensión de cuerpos y $\alpha \in E$ un elemento algebraico sobre K . Tome $p(x)$ su polinomio irreducible sobre K . Sabemos que:

$$K(\alpha) \cong \frac{K[x]}{\langle p(x) \rangle}$$

Nota: Recuerde que $\langle p(x) \rangle = p(x)K[x]$

Teorema 18: Sea (K, P) un cuerpo ordenado, y $p(x) \in K[x]$ un polinomio irreducible sobre K . Entonces el orden P de K se extiende al cuerpo $L = \frac{K[x]}{\langle p(x) \rangle}$, si p cambia de signo en (K, P) . Es decir, existen $a, b \in K$ tal que $p(a)p(b) <_P 0$

Demostración. Sea $n = \deg p$. Usaremos inducción fuerte sobre n .

Si $n = 1 \Rightarrow p(x) = x - \alpha$, con $\alpha \in K$, raíz de $p(x)$. Entonces, se tiene que $L \cong K(\alpha) = K$. El orden se extiende trivialmente. ($P_L = P_K$)

Ahora vamos a suponer la validez del resultado, para polinomio de grado $m < n$. Por un corolario anterior, el orden de P se extiende a L si y solo si $-1 \notin \Sigma PL^2$. Suponga que $-1 \in \Sigma PL^2$. Entonces:

$$-1 = \sum_{i=1}^n a_i \left(\frac{q_i(x)}{\langle p(x) \rangle} \right)^2$$

En donde la expresión $q_i(x)/\langle p(x) \rangle$ debe entenderse como el residuo de la división euclídea de $q_i(x)$ y $p(x)$. Denotaremos esto como $(q_i(x))_{\text{mód } p}$ por comodidad.

Retomando:

$$-1 = \sum_{i=1}^n a_i (q_i(x))_{\text{mód } p}^2$$

Vea que $\deg q_i \leq n - 1$. Entonces se sigue que:

$$\begin{aligned} &\Rightarrow 1 + \sum_{i=1}^n a_i (q_i(x))_{\text{mód } p}^2 = 0 \\ &\Rightarrow \left(1 + \sum_{i=1}^n a_i q_i^2(x) \right)_{\text{mód } p} = 0 \\ &\Rightarrow 1 + \sum_{i=1}^n a_i q_i^2(x) = p(x)h(x), \text{ para } h \in K[x] \end{aligned}$$

Obsérvese que el lado izquierdo de la última igualdad, es positivo (al evaluar en cualquier x). Es decir:

$$\forall x \in K, p(x)h(x) >_P 0$$

Como p cambia de signo, por hipótesis, entonces h también debe hacerlo, pues del contrario $p(x)h(x)$ no se mantendría positivo para todo x . Note que, se puede suponer sin pérdida de generalidad que $h(x)$ es irreducible. Pues de no serlo, factorícelo en factores irreducibles, y escoja cualquiera que cambie de signo (al menos uno de ellos debe hacerlo). Observe que:

$$\deg p + \deg h = \deg \left(1 + \sum_{i=1}^n a_i q_i^2(x) \right) \leq \max\{\deg q_i^2\}_{i=1,\dots,n}$$

Es decir:

$$\begin{aligned} n + \deg h &\leq 2 \max\{\deg q_i\}_{i=1,\dots,n} \\ &\leq 2(n-1) \\ &\Rightarrow \deg h \leq n-2 \end{aligned}$$

Ahora, como $1 + \sum_{i=1}^n a_i q_i^2(x)$ es múltiplo de $h(x)$, se cumple que:

$$1 + \sum_{i=1}^n a_i q_i^2(x) \in \langle h(x) \rangle$$

O sea que

$$\left(1 + \sum_{i=1}^n a_i q_i^2(x) \right)_{\text{mód } p} = 1 + \sum_{i=1}^n a_i (q_i^2(x))_{\text{mód } p} = 0$$

Entonces ahora, llámese $L' = \frac{K[x]}{\langle h(x) \rangle}$. Entonces vemos que L' extiende a K , y que

$$[L' : K] \leq \deg h \leq n - 2$$

Pero tenemos que:

$$-1 = \sum_{i=1}^n a_i (q_i^2(x))_{\text{mód } h} \in \Sigma P(L')^2$$

O sea, que P no se puede extender a L' . Esto es una contradicción a la hipótesis de inducción fuerte. Entonces no fue correcto asumir que $-1 \in \Sigma PL^2$. Por lo tanto $-1 \notin \Sigma PL^2$, y por el Teorema 11, el orden puede ser extendido. ■

Ejemplo 19: Sea (K, P) y $a \in K \setminus K^2$. Entonces P se extiende a un orden de $K(\sqrt{a})$ si y sólo si $a \in P$. Es decir, solamente los elementos positivos tienen raíz cuadrada.

Demostración.

\Leftarrow Como $K(\sqrt{a}) \cong \frac{K[a]}{\langle x^2 - a \rangle}$, basta ver que $x^2 - a$ cambia de signo. Vea que $f(0) = -a <_P 0$.

También $f(a+1) = a^2 + a + 1 >_P 0$, pues $a^2 + 1 \in \Sigma K^2 \subseteq P$, y $a \in P$.

\Rightarrow Sea P' un orden de $K(\sqrt{a})$, tal que $P \subseteq P'$. Si $a \notin P$, entonces $-a \in P'$. Pero $a = (\sqrt{a})^2 \in P'$. Por lo tanto $a = 0$. Lo cual es una contradicción, pues se asumió desde el inicio que $a \notin K^2$. ■

5 Referencias

- [1] Jorge I Guier. *Teoría de Galois (MA-660). [Notas del curso]*. Universidad de Costa Rica, 2017
- [2] Serge Lang. *Algebra [Third Edition]*. Addison-Wesley, Reading Massachusetts, 1993
- [3] Paul Ribenboim. *L'arithmetique des corps*. Hermann, Paris. 1972.