Ordered Fields

J. Ignacio Padilla B

University of Costa Rica

Galois Theory

November 27, 2017

1 Introduction

The theory of ordered fields is the branch of field theory (or Galois theory) that studies the properties of fields in which a total order can be defined, usually denoted by $<$. Like many other properties of fields, the axiomatization of ordered fields corresponds to an abstraction of the real numbers $\mathbb{R}$, which is mainly attributed to David Hilbert, Otto Hölder, and Hans Hahn. Eventually this theory was developed by Artin and Schreier.

In this work, an introduction to the concepts of order in fields will be presented, and various definitions of order in fields (and rings) will be presented. The necessary conditions to be able to induce an order in a given field K will also be introduced. Finally, the properties of orders under field extensions will be studied, with the intention of preparing the reader for the results of the theory of real closed fields.

2 Ordered Fields

An **ordered field**, denoted by $(K, <)$ is a field K where $<$ defines a total order. Furthermore, the order must be compatible with the field structure, that is:

- O.F.1 If $x \leq y \Rightarrow x + z \leq y + z$, for all $x, y, z \in K$
- O.F.2 If $x \leq y$ and $z \geq 0$, then $xz \leq yz$, for all $x, y \in K$

Note: Recall that the expression $x \leq y$ corresponds to an abbreviation of $x < y \vee x = y$, therefore when speaking of order, both will be used without distinction.

When one has a field K together with an order $\leq$, it is possible to define the set of *positive* elements of the field. We define:

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

We denote the *negative* elements by:

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

Note that under these conventions, 0 is positive and negative. Furthermore, it can be observed that:

i) $P + P \subseteq P$

ii) $P \cdot P \subseteq P$

iii) $P \cap -P = \{0\}$

iv) $P \cup -P = K$

Proposition 1. Let K be a field. If there exists $P \subseteq K$ that satisfies properties i), ii), iii) and iv), then we can induce a total order $\leq_P$ in the following way:

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

Furthermore, $\leq_P$ satisfies O.F.1 and O.F.2 (that is, it is compatible with the field structure of K). Furthermore, $\leq_P$ satisfies O.F.1 and O.F.2 (that is, it is compatible with the field structure of K).

Proof: We have to see that $\leq_P$ satisfies conditions of reflexivity, antisymmetry, transitivity and totality. Furthermore we must verify that $\leq_P$ satisfies O.F.1 and O.F.2.

- Since $0 \in P$, then for all $x \in P$, $x - x \in P \Rightarrow x \leq_P x$. (*Reflexivity*).
- If $x \leq_P y$, $y \leq_P x$, then we have that $y - x \in P$, and $-(y - x) \in P$. Therefore $y - x = 0 \Rightarrow y = x$ (*Antisymmetry*).
- If $x \leq_P y$, $y \leq_P z$, then $y - x \in P$, and $z - y \in P$. Then $y - x + z - y = z - x \in P$, that is: $x \leq_P z$ (*Transitivity*).
- If $x, y \in P$, then $x - y \in P$ or $x - y \in -P$ (this since $P \cup -P = K$). That is $x \leq_P y$ or $y \leq_P x$ (*Totality*).
- If $x \leq_P y$, then $y - x = y + z - z - x \geq_P 0$. Then $y + z \geq_P x + z$ (*O.F.1*).
- If $x \leq_P y$, $z \geq_P 0$, since $y - x \in P \wedge z \in P$, then $z(y - x) = zy - zx \geq_P 0 \Rightarrow zy \geq_P zx$ (*O.F.2*).

Therefore it is concluded that $(K, \leq_P)$ is an ordered field. ■

What the previous result tells us, is that actually the order of a given field can be determined by first defining the set of numbers that are desired to be positive (as long as they satisfy the hypothesis properties). From now on, when speaking of order, one can consider the set P and the relation $<_P$ ($<$, abbreviated), without any distinction.

As the reader will have noticed, the definition of ordered field does not really use the field properties of the structure (perhaps only commutativity, implicitly). In fact, an **ordered ring** can be defined analogously as a ring A, where there exists a set $P \subseteq A$ such that:

i. $P + P \subseteq P$

ii. $P \cdot P \subseteq P$

iii. $P \cap -P = \{0\}$

iv. $P \cup -P = A$

In this case, one has a more general definition, since it is not needed that this order satisfies O.F.1 nor O.F.2. This definition will be useful to order polynomial rings as will be seen in following sections. Below is an interesting lemma: **Lemma 2:** Let P_1 and P_2, be two orders on a field K, such that $P_1 \subseteq P_2$. Then $P_1 = P_2$

Proof. Suppose there exists $x \in P_2 \setminus P_1$. Then

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

■

Example 3:

- $(\mathbb{R}, \leq)$ is an ordered field, with its usual order. In this case $P = \mathbb{R}^+ \cup \{0\}$. Later we will see that this is the only possible order in $\mathbb{R}$.
- $(\mathbb{Q}, \leq)$ is an ordered field, with the order inherited from $\mathbb{R}$. It also happens that there is a unique order that satisfies the axioms of OF.
- $\mathbb{C}$ is not an ordered field. This will be shown at the end of the chapter.

Proposition 4: If $x, y \in (K, <)$ are such that $x, y < 0$, then $xy > 0$. This since as $-x \in P$ $-y \in P$, then $(-x)(-y) = xy \in P$. In particular: $x^2 \geq 0$ for all x.

We are now going to study some possibilities of order in polynomial rings. More specifically, consider the ring of polynomials with real coefficients $\mathbb{R}[x]$. Let $p(x) \in \mathbb{R}[x]$,

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

We define the **order at infinity** ($>_{+\infty}$) in $\mathbb{R}[x]$ as:

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

By way of clarification:

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

Then we can define the set P of positive polynomials:

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

Proposition 5: $(\mathbb{R}[x], P)$ is an ordered ring.

Proof. We only need to verify:

i. $P + P \subseteq P$

ii. $P \cdot P \subseteq P$

iii. $P \cap -P = \{0\}$

iv. $P \cup -P = A$

Properties i), ii) and iv) are easily deduced. To prove iii), take $p(x) \in P \cap -P$, then if $p(x) \neq 0$, we have that $a_n > 0 \wedge a_n < 0$, which is not possible. Therefore $p(x) = 0$. ■

Some observations:

- If $p, q \in \mathbb{R}[x]$, such that $\deg p > \deg q$, then $p(x) - q(x) > 0$ if and only if $p(x) > 0$. In other words, $p(x) > q(x)$, for all q with degree less than p.
- In a particular case of this observation, it can be noted that for all $r \in \mathbb{R}$:
$$x - r >_{+\infty} 0$$
That is:
$$x >_{+\infty} r$$
We obtained an element in $\mathbb{R}[x]$ that is greater than all real numbers, something that is not possible with the order $>$ of the reals. We call these elements **infinite** elements.
- $>_{+\infty}$ extends the usual order of $\mathbb{R}$, in the sense that, if we consider $a \in \mathbb{R}$ as a constant polynomial, then:
$$a >_{+\infty} 0 \iff a > 0$$
That is, for constants, $>_{+\infty}$ coincides with $>$.

Soon we will study other possible orders in $\mathbb{R}[x]$. For now let us consider the following lemma:
Lemma 6: Let (A, P) be an ordered commutative integral domain. Then $K = \text{Frac}(A)$ is an ordered field (K, Q) where the set Q of positive elements is defined as:

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

Proof. It is necessary to verify that:

i. $Q + Q \subseteq Q$

ii. $Q \cdot Q \subseteq Q$

iii. $Q \cap -Q = \{0\}$

iv. $Q \cup -Q = K$

i) Let $\frac{a}{b}, \frac{c}{d} \in Q$ Recall that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Then we have to see that:
$$bd(ad + bc) = abd^2 + b^2cd \in P$$
But $ab \in P$ and $cd \in P$, and since every square is positive, we obtain that Q is closed under addition.

ii) Let $\frac{a}{b}, \frac{c}{d} \in Q$ Then it is trivial that $\frac{ac}{bd} \in Q$, since $abcd \in P$

iii) Clearly $0 \in Q$, since $0 = \frac{0}{1} = -\frac{0}{1}$. If $\frac{a}{b} \in Q \cap -Q$, then $ab \in P$ and $ab \in -P$. Then $ab = 0 \Rightarrow a = 0$.

iv) Clearly $Q \cup -Q \subseteq K$. If $\frac{a}{b} \in K$, then consider $ab \in A$. Now:

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

That is:

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

$\blacksquare$

Example 7:

1. Let us return to the order $>_{+\infty}$ that was defined previously in $\mathbb{R}[x]$. Now we can extend it to the field of rational fractions in one variable:

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

Then consider the order extension given by lemma 6:

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

Observe that the leading coefficient of $p(x)q(x)$ is the product of the leading coefficients of p and q, therefore the sign of the expression $\frac{p(x)}{q(x)}$ depends on the sign of the fraction a_n/b_m, where a_n and b_m are the leading coefficients of $p(x)$ and $q(x)$, respectively. Furthermore, it continues to hold that $x >_{+\infty} r$ for any real r, since the order in the field of fractions is an 'extension' of the order of the polynomial ring. More precisely, when the expressions have denominator 1, their order coincides with that defined previously in the ring.

2. Consider now the transformation $x \mapsto -x$ together with the order $>_{+\infty}$. We will define the **order at minus infinity** ("$>_{-\infty}$"), in $\mathbb{R}(x)$ in the following way:

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

Note that the expression $p(-x)$ changes the coefficients a_{2n-1} of sign. In particular it can be appreciated that:

$$\begin{aligned} p(x) {}_{-\infty}0 &\iff p(-x) >_{+\infty} 0 \\ &\iff \begin{cases} a_n > 0, & \text{if } n \text{ is odd} \\ a_n < 0, & \text{if } n \text{ is even} \end{cases} \end{aligned}$$

Observe that:

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

In this order we have that x corresponds to a **negative infinity**, while x^2 corresponds to an infinity.

3. Now consider the transformation $x \mapsto \frac{1}{x}$, again together with the order $\geq_{+\infty}$. We will define the **order at** 0^+ ("$>_{0^+}$") in $\mathbb{R}(x)$ by means of:

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

To study this order in more detail, observe that if we take

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

with $a_n \neq 0$ and $a_k \neq 0$, we have that:

$$\begin{aligned} p(x) >_{0^+} 0 &\iff p(\frac{1}{x}) >_{+\infty} 0 \\ &\iff a_n \frac{1}{x^n} + \cdots + a_k \frac{1}{x^k} >_{+\infty} 0 \\ &\iff \frac{a_n + a_{n-1}x + \cdots + a_k x^{n-k}}{x^n} >_{+\infty} 0 \\ &\iff a_n + a_{n-1}x^{n-1} + \cdots + a_k x^{n-k} >_{+\infty} 0 \\ &\text{since we already know that } x^n >_{+\infty} 0 \\ &\iff a_k > 0. \end{aligned}$$

That is, the order at 0^+ depends on the last non-zero coefficient. Observe that under this order we have the following:

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

That is, for all $r > 0$ we have that:

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

We see that in this order we have an element closer to 0 than any real number. We call these elements **infinitesimals**.

4. Another possibility is considering the transformation $x \mapsto \frac{1}{x}$, and we define **the order at** 0^- "($>_{0^-}$)" in $\mathbb{R}(x)$ as:
$$\frac{p(x)}{q(x)} \geq_{0^-} 0 \iff \frac{p(-\frac{1}{x})}{q(-\frac{1}{x})} \geq_{+\infty} 0$$
Analogously to the order at $-\infty$, it can be seen that:
$$\begin{aligned} p(x) >_{0^-} 0 &\iff p(-x) >_{0^+} \\ &\iff \begin{cases} a_k > 0, & \text{if } k \text{ is odd} \\ a_k < 0, & \text{if } k \text{ is even} \end{cases} \end{aligned}$$
Where a_k is the coefficient that accompanies the lowest power of x. In this order we see that:

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

   Then:
$$r <_{0^-} x <_{0^-} 0 \qquad \forall r < 0$$
We observe that x is a **negative infinitesimal**.

5. **Exercise:** The reader is invited to generalize these orders, and formulate, given $a \in \mathbb{R}$, the orders $>_{a^+}$ and $>_{a^-}$, such that one has that the element x represents a quantity **infinitesimally larger** than a (in the first case), and a quantity **infinitesimally smaller** than a in the second.

The previous examples represent a very interesting view into the possible extensions of a total order in a field, allowing to order the field of rational polynomial expressions over said field. This tool is even useful when formalizing the concepts of infinities and infinitesimals, which are widely used in non-standard analysis.

3 Formally Real Fields

In this section we will study the following question: What conditions must a field K meet, so that a total order can be defined in it (equivalently, a set of positive elements), that satisfies the axioms of ordered fields? **Definition 8:** Let K be a field. Then:

a) We say that K is **formally real** (or just real) (or orderable), if it admits at least one total order, compatible with the field structure (O.F.1 and O.F.2).

b) Let $X \subseteq K$. We say that X is **formally positive** if there exists an order P of K such that $X \subseteq P$.

Lemma 9: Let K be any field. Then K is formally real if and only if $\{0, 1\}$ is formally positive.

Proof.
$\Leftarrow$ Trivial. Follows from the definitions.
$\Rightarrow$ Let $P \subseteq K$ be an order, then we already have that $0 \in P$. We only have to show that $1 \in P$. Suppose not. Then $-1 \in P \Rightarrow 1 = (-1)^2 \in P$, which is contradictory. ■

Thanks to this lemma we can then say that, given any order in a field K, the set $\{0,1\}$ is positive. In particular $1>0$ in any ordered field. **Proposition 10:** If K is a formally real field, then $\operatorname{char} K = 0$. Since otherwise, if $\operatorname{char} K = p$, since $1>0$, then one has the impossible inequality:

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

Given a field K and for $F \subseteq K$ a multiplicatively closed subset ($F \cdot F \subseteq F$), and such that $\{0,1\} \in F$. We will define the following set, which will be of much help in the following results:

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

Which corresponds to the sums of elements of F multiplied by squares of K. **Theorem 11:** Let K be such that $\operatorname{char} K \neq 2$, and let $F \subseteq K$ such that $F \cdot F \subseteq F$, and $\{0,1\} \in F$. Then the following conditions are equivalent.

1) F is formally positive

2) $\Sigma F K^2 \subsetneq K$

3) $-F \cap \Sigma F K^2 = \{0\}$

3'. $-1 \notin \Sigma F K^2$

4) If given $a_1, a_2, \ldots, a_n \in F \setminus \{0\}$, there exist $x_1, x_2, \ldots, x_n \in K$, such that $\sum_{i=1}^{n} a_i x_i^2 = 0$, then $x_1 = x_2 = \cdots = x_n = 0$.

5) There exists $S \subseteq K$ such that:

   i) $F \subseteq S$

   ii) $K^2 \subseteq S$

   iii) $S + S \subset S$

   iv) $S \cdot S \subseteq S$

   v) $S \cap -S = \{0\}$

   That is, at least one partial order can be defined in K that makes the elements of F positive (and the squares).

Proof. It can be easily observed that $3') \Rightarrow 2)$ and that $3) \Rightarrow 3')$. We will prove $1) \Rightarrow 2) \Rightarrow 3) \Rightarrow 4) \Rightarrow 5) \Rightarrow 1)$.

- $1) \Rightarrow 2)$: Take $F \subseteq P$, since $K^2 \subseteq P$, it follows that $\Sigma F K^2 \subseteq P$, since sum and product of positives is positive. Then we have that $\Sigma F K^2 \subseteq P \subsetneq K$, since -1 is never positive. Therefore $\Sigma F K^2 \subsetneq K$.

- $\neg 3) \Rightarrow \neg 2)$: Suppose there exists $a \in F$ non-zero, such that $-a \in \Sigma F K^2$. Then we will see that $\Sigma F K^2 = K$. Let $y \in K$. Since $2a \neq 0$, let us call:

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

  Then $y \in \Sigma F K^2$. Therefore $\Sigma F K^2 = K$ and we obtain the negation of 2).

- $\neg 4) \Rightarrow \neg 3)$: By contraposition, let $a_1, a_2, \cdots, a_n \in F \setminus \{0\}$, and $x_1, x_2, \cdots, x_n \in K$ not all zero, such that $\sum_{i=1}^{n} a_i x_i^2 = 0$. Let us assume, without loss of generality, that $x_1 \neq 0$. Then:

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

  Then it follows that $-a_1 \in -F \cap \Sigma F K^2$, where a_1 is non-zero. We have negated 3).

- $4) \Rightarrow 5)$: We will see that the order we need is $\Sigma F K^2$. Let $S = \Sigma F K^2$. Clearly $F \subseteq S$ and also $K^2 \subseteq S$. It is also easy to see that $S + S \subseteq S$ and that $S \cdot S \subseteq S$. It would only be necessary to see that $S \cap -S = \{0\}$, in particular we only need the inclusion $\subseteq$.
  Let $y \in S \cap -S$. Then:

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

- $5) \Rightarrow 1)$: Let $\mathcal{F}$ be the family of subsets $S \subseteq K$ that verify properties i), ii), iii) and iv) of the hypothesis (5). Then we have that $\mathcal{F}$ is not empty, since $S \in \mathcal{F}$. We verify partially order $\mathcal{F}$ by inclusion, and then we see that if $(S_i)_{i \in I}$ is a chain of elements in $\mathcal{F}$, then $\bigcup_{i \in I} S_i$ is in $\mathcal{F}$ (every chain is bounded above). Then we see that the family $\mathcal{F}$ is a partially ordered set, where every chain has an upper bound. By Zorn's lemma, there exists an element $Q \in \mathcal{F}$ such that is maximal. Since $Q \subseteq K$ is in $\mathcal{F}$, then it satisfies i), ii), iii), iv). It only remains to verify that Q is a total order, that is: $Q \cup -Q = K$

  Let $x \in K$ such that $x \notin Q$, then we must see that $-x \in Q$. Consider the set $Q' = Q - xQ = \{c - xd \quad c, d \in Q\}$. Since $0 \in Q$, then $Q \subseteq Q'$, and therefore $F \subseteq Q'$ and $K^2 \subseteq Q'$. It is simple to see that $Q' + Q' \subseteq Q'$ and $Q' \cdot Q' \subseteq Q'$. Let us see now that $Q' \cap -Q' = \{0\}$. For this, let $y \in Q' \cap -Q'$. Then $y = c_1 - xd_1$ and $-y = c_2 - xd_2$, with $c_1, c_2, d_1, d_2 \in Q$. That is, $(c_1 + c_2) - x(d_1 + d_2) = 0$, and then $c_1 + c_2 = x(d_1 + d_2)$. Suppose now that $d_1 + d_2 \neq 0$, then:

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

Then x is a product between a square and an element in Q, therefore $x \in Q$ (since Q contains K^2 and is multiplicatively closed). But this is a contradiction! Then it must be that $d_1 + d_2 = 0$ and $c_1 + c_2 = 0$. Then $d_1 = -d_2$, that is d_1 is positive and negative, and therefore $d_1 = d_2 = 0$. Analogously we have that $c_1 = c_2 = 0$. Then $y = 0$. Then Q' satisfies hypothesis 5), that is $Q' \in \mathcal{F}$, but since $Q \subseteq Q'$, and by the maximality of Q, we have that $Q = Q'$, therefore $-x \in Q' = Q$. Then Q is the total order we were looking for.

■

This theorem is a very useful tool to determine if a given set in a field is positive in some order. More specifically, apply the previous theorem in a field K, taking $F = \{0, 1\}$. Recall that K is formally real if and only if $\{0, 1\}$ is formally positive. **Corollary 12:** Let K be a field with characteristic distinct from 2. Then the following conditions are equivalent:

i) K is formally real.

ii) If $\sum_{i=1}^{n} x_i^2 = 0$, then $x_1 = x_2 = \cdots = x_n = 0$, for all $x_i \in K$, for all $n \in \mathbb{N}$.

iii) $-1 \notin \Sigma K^2$

Proof. Apply Theorem 11 , with $F = \{0, 1\}$. Observe that $\Sigma F K^2 = \Sigma K^2$. ■

Corollary 13: $\mathbb{C}$ is not formally real. That is $\mathbb{C}$ cannot be ordered.

Proof. Observe that $-1 = i^2 \in \mathbb{C}^2$ ■

Corollary 14: Let (K, P) be an ordered field and $L|K$ a field extension. Then the following are equivalent:

1. L has an order that extends that of K. (That is, if an element is positive in K, it is also positive in L).
2. $\Sigma P L^2 \subsetneq L$
3. $(-P) \cap \Sigma P L^2 = \{0\}$.

3'. $-1 \notin \Sigma P L^2$

4. $\sum_{i=1}^{n} a_i x_i = 0 \Rightarrow x_i = 0, \quad i = 1, .., n$

Proof. Apply Theorem 11 to $P = F$, and to $K = L$. Note that the order P of K is multiplicativamente closed, and contains $\{0, 1\}$. ■

It can even be applied more generally: **Corollary 15:** Let K be a real field. Let $L|K$ be an extension and $F \subseteq K$ a formally positive part. Then the following assertions are equivalent:

1. Every order of K that contains K extends to an order of L.
2. For every order P of K, such that $F \subseteq P$, it holds that $\Sigma P L^2 \subsetneq L$.
3. For every order P of K, such that $F \subseteq P$, if $\sum_{i=1}^{n} a_i x_i = 0 \Rightarrow x_i = 0, i = 1, ..., n$, with $a_i \in P^*$ and $x_i \in L$.

4. For every order P of K, such that $F \subseteq P$, it is satisfied that $(-P) \cap \Sigma PL^2 = \{0\}$

Below, we will give a characterization of the "smallest" possible order that can be defined in a real field.

Proposition 16: Let K be a real field and $a \in K$. Then $a \in P$ for every order P if and only if $a \in \Sigma K^2$. That is:

$$\Sigma K^2 = \bigcap \{P : P \text{ order in } K\}$$

Proof.

$\Leftarrow$ If $a \in \Sigma K^2$, then take any order P of K, as $K^2 \subseteq P \Rightarrow a \in P$.

$\Rightarrow$ Let $a \notin \Sigma K^2$. We need an order P of K such that $-a \in P$ (that is that a is negative). Consider the set $F = \langle 0, 1, -a \rangle$

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

It would suffice then to see that F is formally positive. By theorem 11, this is the same as seeing that there exists a partial order S where F is positive. Then let us take $S = \Sigma FK^2$. Clearly $S + S \subseteq S$, $S \cdot S \subseteq S$, $F \in S$, $K^2 \in S$. We only need to see that $S \cap -S = \{0\}$. If $y \in S \cap -S$, then

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

With $a_i, b_i \in F$. Then, due to the form of the elements of F it can be seen that y can be written in the form:

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

Where $c_1, c_2, d_1, d_2 \in \Sigma K^2$. Solving for a and assuming that $d_1 + d_2 \neq 0$, we have that:

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

Which indicates that $a \in \Sigma K^2$. This is not possible. Then it must be that $d_1 + d_2 = 0$. Then $d_1 = d_2 = 0 \Rightarrow c_1 = c_2 = 0$. Therefore $y = 0$, which is what was sought. ■

Corollary 17: Let K be a real field. The following conditions are equivalent:

i) K has only one order.

ii) ΣK^2 is an order of K.

iii) $\Sigma K^2 \cap -\Sigma K^2 = \{0\}$ and $\Sigma K^2 \cup -\Sigma K^2 = K$

Proof.
1) $\Rightarrow$ 3): Let P be said order. Then $\Sigma K^2 = \bigcap P = P$. Since P satisfies $P \cap -P = \{0\}$ and $P \cup -P = K$, then we immediately obtain 3).
3) $\Rightarrow$ 2): Obviously $\Sigma K^2 + \Sigma K^2 \subseteq \Sigma K^2$, and $(\Sigma K^2)(\Sigma K^2) \subseteq \Sigma K^2$. Adding hypothesis 3), then we have sufficient conditions to be able to induce the order $>_{\Sigma K^2}$
2) $\Rightarrow$ 1): Let P be any order of K. We know that $\Sigma K^2 \subseteq P$. Then by lemma 2, then $\Sigma K^2 = P$. Then K only has the order ΣK^2

■

The previous lemma is very interesting, because it tells us that if the squares of K allow it to be ordered, then the order consisting precisely of the squares of K is the only one compatible with the field structure. This will allow us to conclude that $\mathbb{R}$ only has one order (the usual one), since all positive elements of $\mathbb{R}$ are precisely squares.
By way of comment: throughout this section we have seen some results about the necessary conditions for a field to be real. Possibly the most important of all is the fact that, given a field K, if -1 is a finite sum of squares, then it is not possible to order K. In other words, it is not possible to define an order where sums of squares are less than 0.

4 Algebraic extensions to order extensions

In this section we will examine briefly what happens with the order of a real field, when it is extended finitely, and algebraically
Consider $E|K$ a field extension and $\alpha \in E$ an element algebraic over K. Take $p(x)$ its irreducible polynomial over K. We know that:

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

Note: Recall that $\langle p(x) \rangle = p(x)K[x]$
Theorem 18: Let (K, P) be an ordered field, and $p(x) \in K[x]$ an irreducible polynomial over K. Then the order P of K extends to the field $L = \frac{K[x]}{\langle p(x) \rangle}$, if p changes sign in (K, P). That is, there exist $a, b \in K$ such that $p(a)p(b) <_P 0$

Proof. Let $n = \deg p$. We will use strong induction on n.
If $n = 1 \Rightarrow p(x) = x - \alpha$, with $\alpha \in K$, root of $p(x)$. Then, we have that $L \cong K(\alpha) = K$. The order extends trivially. $(P_L = P_K)$
Now we will assume the validity of the result, for polynomial of degree $m < n$. By a previous corollary, the order of P extends to L if and only if $-1 \notin \Sigma PL^2$. Suppose that $-1 \in \Sigma PL^2$. Then:

$$-1 = \sum_{i=1}^{n} a_1 \left(\frac{q_i(x)}{\langle p(x) \rangle} \right)^2$$

Where the expression $q_i(x)/\langle p(x)\rangle$ must be understood as the remainder of the Euclidean division of $q_i(x)$ and $p(x)$. We will denote this as $(q_i(x))_{\text{mod } p}$ for convenience.
Resuming:

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

See that $\deg q_i \leq n-1$. Then it follows that:

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

Observe that the left side of the last equality, is positive (upon evaluating at any x). That is:

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

Since p changes sign, by hypothesis, then h must also do so, since otherwise $p(x)h(x)$ would not remain positive for all x. Note that, it can be assumed without loss of generality that $h(x)$ is irreducible. Since if it were not, factor it into irreducible factors, and choose any that changes sign (at least one of them must do so). Observe that:

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

That is:

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

Now, since $1 + \sum_{i=1}^{n} a_i q_i^2(x)$ is a multiple of $h(x)$, it is satisfied that:

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

That is that

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

Then now, let $L' = \frac{K[x]}{\langle h(x)\rangle}$. Then we see that L' extends K, and that

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

But we have that:

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

That is, that P cannot be extended to L'. This is a contradiction to the strong induction hypothesis. Then it was not correct to assume that $-1 \in \Sigma PL^2$. Therefore $-1 \notin \Sigma PL^2$, and by Theorem 11, the order can be extended. ■

Example 19: Let (K, P) and $a \in K \setminus K^2$. Then P extends to an order of $K(\sqrt{a})$ if and only if $a \in P$. That is, only positive elements have a square root.

Proof.
$\Leftarrow$ Since $K(\sqrt{a}) \cong \frac{K[a]}{\langle x^2-a\rangle}$, it suffices to see that $x^2 - a$ changes sign. See that $f(0) = -a <_P 0$. Also $f(a+1) = a^2 + a + 1 >_p 0$, since $a^2 + 1 \in \Sigma K^2 \subseteq P$, and $a \in P$.
$\Rightarrow$ Let P' be an order of $K(\sqrt{a})$, such that $P \subseteq P'$. If $a \notin P$, then $-a \in P'$ But $a = (\sqrt{a})^2 \in P'$. Therefore $a = 0$. Which is a contradiction, since it was assumed from the beginning that $a \notin K^2$. ■

5 References

[1] Jorge I Guier. *Teoría de Galois (MA-660).* [*Course Notes*]. Universidad de Costa Rica, 2017

[2] Serge Lang. *Algebra* [*Third Edition*]. Addison-Wesley, Reading Massachusetts, 1993

[3] Paul Ribemboim. *L'arithmetique des corps.* Hermann, Paris. 1972.