Algebra Univers. (2022) 83:23

1420-8911/22/030001-6
published online June 27, 2022
https://doi.org/10.1007/s00012-022-00781-6

Algebra Universalis

The number fields that are O^*-fields

Jingjing Ma

Abstract. Using the theory on infinite primes of fields developed by Harrison in [2], the necessary and sufficient conditions are proved for real number fields to be O^*-fields, and many examples of O^*-fields are provided.

Mathematics Subject Classification. 06F25.

Keywords. Infinite prime, Real number field, O^*-field.

1. Introduction

Let R be an associative ring. If a partial order on R is contained in a total order on R, then we say that the partial order is extended to a total order. A ring is called an O^*-*ring* if each partial order is extended to a total order. This concept was introduced by Fuchs in [1], and as an open question in [1], he asked establishing ring-theoretical properties of O^*-rings. In [5], Steinberg provided the ring-theoretical characterization of the O^*-rings, and from his characterizations, the question becomes determining the O^*-fields [5, Theorem]. An O^*-field must be a subfield of $\mathbb{R}$, the field of real numbers, and must be algebraic over $\mathbb{Q}$, the field of rational numbers. Steinberg also pointed out that it is sufficient to determine which subfields of $\mathbb{R}$ that is a finite extension of $\mathbb{Q}$ are O^*-fields [5, p. 2557]. He proved that each real quadratic extension field of $\mathbb{Q}$ is an O^*-field, and $\mathbb{Q}[\sqrt[4]{2}]$ is not an O^*-field. In [4], it is shown that a sequence of real quadratic extension of $\mathbb{Q}$ is an O^*-field and $\mathbb{Q}[\sqrt[3]{n}]$, where n is a cubic-free positive integer, is an O^*-field. No other results on O^*-fields seem available in the literature.

In the present paper, by using the theory on the infinite primes of the number fields developed by Harrison in [2], the connection between the maximal partial orders on a number field R and the subfields of R is established, then necessary and sufficient conditions are obtained for a real number field being O^*. As a consequence, we show that, for instance, for a real number

Presented by W. Wm. McGovern.

field R if $[R:\mathbb{Q}]$ is an odd integer, then R is O^*, where $[R:\mathbb{Q}]$ denotes the dimension of R over $\mathbb{Q}$.

We review a few definitions from partially ordered rings. Let R be an associative ring and P be a subset of R. Then P is said to be the positive cone of a partial order if $P+P\subseteq P$, $PP\subseteq P$, and $P\cap -P=\{0\}$. We often just call P as a partial order on R. In this paper, we only consider partial orders on fields. By Zorn's Lemma, each partial order is contained in a maximal partial order. We denote by $\mathbb{Q}^+$ and $\mathbb{R}^+$ the positive cone of the usual total order on $\mathbb{Q}$ and $\mathbb{R}$, respectively. For a maximal partial order P, $\mathbb{Q}^+\subseteq P$ and P is division closed in the sense that for any two elements a,b in the field, if $ab>0$ and $a>0$, then $b>0$.

For more information and undefined terminologies on partially ordered rings, the reader is referred to [1,3].

2. Infinite primes for fields

In this section, we collect some results from [2] that will be used in the following section. Let R be a field. A nonempty subset S is called a *preprime* if S is closed under the addition and multiplication in R, and $-1\notin S$, that is,

$$S+S\subseteq S,\ SS\subseteq S,\ \text{and} -1\notin S.$$

A maximal preprime is called a *prime*. By Zorn's Lemma, each preprime is contained in a prime. A prime S is called *infinite* if $1\in S$, otherwise S is called *finite*. An infinite prime S of R is called *full* if $R=S-S=\{a-b\mid a,b\in S\}$.

Let R be a number field that is n-dimensional over $\mathbb{Q}$. There exist exactly n isomorphisms (or embeddings) $\sigma_1,\sigma_2,\ldots,\sigma_n$ of R into $\mathbb{C}$, the field of complex numbers. Let ρ be the ordinary complex conjugate on $\mathbb{C}$. Assume $\rho\circ\sigma_i=\sigma_i$, for $1\le i\le r$, and $\rho\circ\sigma_i=\sigma_{i+s}$ for $r<i\le r+s$ with $r+2s=n$. Then

$$\sigma_1,\ldots,\sigma_r,\ \sigma_{r+1},\ldots,\sigma_{r+s},\rho\circ\sigma_{r+1},\ldots,\rho\circ\sigma_{r+s}$$

are these isomorphisms, and $\sigma_1,\ldots,\sigma_r$ are called the *real infinite prime divisors* of R, and the sets $\{\sigma_{r+1},\rho\circ\sigma_{r+1}\},\ldots,\{\sigma_{r+s},\rho\circ\sigma_{r+s}\}$ are called the *complex infinite prime divisors* of R.

Theorem 2.1 (1) ([2, Proposition 3.5]). *Let R be a number field and let $\sigma_1,\ldots,\sigma_r$ be the real infinite prime divisors of R. The sets $\sigma_1^{-1}(\mathbb{R}^+),\ldots,\sigma_r^{-1}(\mathbb{R}^+)$ are distinct and consist exactly of all the full infinite primes of R.*

(2) ([2, Proposition 3.6]). *Let R be a number field. Let P be an infinite prime of R which is not full (i.e., $P-P\neq R$). Then there exists a complex infinite prime divisor $\{\sigma,\rho\circ\sigma\}$ of R with $P=\sigma^{-1}(\mathbb{R}^+)$. If R is a normal number field, then this gives a one-one correspondence between all the non-full infinite primes of R and all the complex infinite prime divisors of R.*

In the present paper, we only consider the real number fields which are subfields of $\mathbb{R}$ and finite dimensional over $\mathbb{Q}$. Let R be a real number field. For a subset H of R, define $E_H=H-H=\{a-b\mid a,b\in H\}$. The following result shows that in a real number field, infinite primes are precisely maximal partial orders.

Lemma 2.2. *Let R be a real number field.*

(1) *Let H be subset of R such that $H + H \subseteq H$, $HH \subseteq H$, and $\mathbb{Q}^+ \subseteq H$. Then E_H is a subfield of R.*
(2) *If S is an infinite prime on R, then S is a maximal partial order on R.*
(3) *If P is a maximal partial order on R, then P is an infinite prime on R.*

Proof. (1) It is clear that E_H is a subring of R and a subspace of R over $\mathbb{Q}$. Take $0 \neq a \in E_H$, define $f_a : E_H \to E_H$ by $f_a(u) = au$ for any $u \in E_H$. Then f_a is a linear transformation from E_H to E_H over $\mathbb{Q}$. Since f_a is one-to-one and E_H is finite-dimensional over $\mathbb{Q}$, f_a is onto, so there exists $b \in E_H$ such that $ab = 1$. Thus E_H is a subfield of R.

(2) Let S be an infinite prime on R. From the proof of [2, Proposition 3.5], we have $S \cap -S = \{0\}$, so S is a partial order on R. Assume $S \subseteq P$, where P is a maximal partial order on R. If $-1 \in P$, then $1 \in P \cap -P = \{0\}$, a contradiction. Thus $-1 \notin P$ and P is a preprime. Since S is a maximal preprime and P is a preprime, $S \subseteq P$ implies that $S = P$ and hence S is a maximal partial order on R.

(3) If P is a maximal partial order, then P is a preprime. Let $P \subseteq S$ which is an infinite prime. By (2), S is a maximal partial order, so $P = S$ is an infinite prime. □

Since in a real number field, the maximal partial orders and the infinite primes are the same, we freely use both names.

3. O^*-fields

For a field K and a subfield F of K, $[K : F]$ denotes the dimension of K as an F-vector space. A partial order on a real number field R is called *directed* if each element is a difference of two positive elements. For an embedding σ from R to $\mathbb{C}$, it is clear that $\sigma^{-1}(\mathbb{R}^+)$ is a partial order on R.

Theorem 3.1. *Let R be a real number field. Then following conditions are equivalent.*

(1) *R is an O^*-field,*
(2) *For each complex infinite prime divisor $(\sigma, \rho \circ \sigma)$ of R, $\sigma^{-1}(\mathbb{R}^+)$ is extended to a total order on R,*
(3) *For each maximal partial order P on R, $E_P = R$,*
(4) *Each maximal partial order P on R is directed,*
(5) *Each maximal partial order P on R contains $[R : \mathbb{Q}]$ linearly independent vectors.*

Proof. (1) $\Rightarrow$ (2) is clear.

(2) $\Rightarrow$ (1) Let P be a maximal partial order on R. We show that P must be a total order. Since P is an infinite prime on R by Lemma 2.2, Theorem 2.1

implies that $P = \sigma^{-1}(\mathbb{R}^+)$, where σ is a real or complex infinite prime divisor of R, then P must be a total order by the assumption.

(1) $\Rightarrow$ (3) Assume that there exists a maximal partial order P on R such that $E_P \neq R$. Take $z \in R \setminus E_P$. Then $z \notin P$ and $-z \notin P$, so P is not a total order and R is not O^*.

(3) $\Rightarrow$ (1) Let P be a maximal partial order on R. We show that P must be a total order. By Lemma 2.2, P is an infinite prime. Since $E_P = P - P$ and $E_P = R$, $R = P - P$, that is P is a full infinite prime. By Theorem 2.1, $P = \sigma^{-1}(\mathbb{R}^+)$ for some real infinite prime divisor σ of R. Thus P is a total order on R.

(3) $\Rightarrow$ (4) Let P be a maximal partial order. Then $R = P - P$, so P is a directed partial order.

(4) $\Rightarrow$ (5) Let P be a maximal partial order on R, since P is directed, $R = P - P$, so P is a generating set of R as a vector space over $\mathbb{Q}$. Thus P contains $[R : \mathbb{Q}]$ linearly independent vectors.

(5) $\Rightarrow$ (3) Let P be a maximal partial order on R. Since P contains $[R : \mathbb{Q}]$ linearly independent vectors, $P - P$ is a subspace of $[R : \mathbb{Q}]$-dimensional, and hence $R = P - P$. □

The following result is an immediate consequences of Theorem 3.1.

Theorem 3.2. *Let R be a real number field. If $[R : \mathbb{Q}] = n$ is an odd integer, then R is an O^*-field.*

Proof. Let P be a maximal partial order on R and $[E_P : \mathbb{Q}] = k$. Then $k \mid n$. Since P is a full infinite prime in E_P, there exists a real infinite prime divisor σ of E_P such that $P = \sigma^{-1}(\mathbb{R}^+)$. It is well-known that σ can be extended to $[R : E_P] = n/k$ embeddings from R to $\mathbb{C}$, and since n/k is odd, one of those n/k embeddings must be a real infinite prime divisor of R, denoted by δ. Then $P = \sigma^{-1}(\mathbb{R}^+) \subseteq \delta^{-1}(\mathbb{R}^+)$, and hence $P = \delta^{-1}(\mathbb{R}^+)$ since P is a maximal partial order on R. Thus R is O^*. □

There exist real number fields R in which $E_P = R$ is not true for all the maximal partial orders P, and hence R is not an O^*-field. The following example is due to Steinberg.

Example 3.3. Let $R = \mathbb{Q}[a]$ with $a = \sqrt[4]{2}$. The irreducible polynomial $f(x) = x^4 - 2$ has four roots: $a, -a, ia, -ia$, where $i^2 = -1$. Let σ be the embedding from R to $\mathbb{C}$ that sends a to ia. Then $-a^2 \in \sigma^{-1}(\mathbb{R}^+)$. If $\sigma^{-1}(\mathbb{R}^+) = P$ is not a maximal partial order, then $P \subsetneq P_1$ for some maximal partial order P_1. If P_1 is not a full infinite prime on R, then by Theorem 2.1, there exists a complex infinite prime divisor $\{\gamma, \rho \circ \gamma\}$ such that $P_1 = \gamma^{-1}(\mathbb{R}^+)$. However $\{\sigma, \rho \circ \sigma\}$ is the only complex infinite prime divisor of R, so $P = P_1$, a contradiction. Hence we must have $E_{P_1} = R$ and $P_1 = \delta^{-1}(\mathbb{R}^+)$ for some real infinite prime divisor δ of R. Then δ is either the identity mapping or the embedding that sends a to $-a$. In either case, $a^2 \in P_1$. On the other hand, $-a^2 \in P \subsetneq P_1$, so $a^2 \in P_1 \cap -P_1$, a contradiction. Thus P is a maximal partial order on R. It follows that R is not O^* by Theorem 3.1.

Similar to Steinberg's example, if n is a positive integer divisible by 4, then $\mathbb{Q}[\sqrt[n]{2}]$ is not an O^*-field since the partial ordered $P = \mathbb{Q}^+ + \mathbb{Q}^+(-a^{\frac{n}{2}})$, where $a = \sqrt[n]{2}$, cannot be extended to a total order.

Let R be a real number field with $[R : \mathbb{Q}] = 4$. It is possible for R to be an O^*-field as shown in Example 3.6.

Theorem 3.4. *If $R = \mathbb{Q}[\sqrt[2n]{p}]$, where p is a prime number and n is a odd integer, then R is O^*.*

Proof. Let P be a maximal partial order on R and $a = \sqrt[2n]{p}$, $b = a^n = \sqrt{p}$. Then $b^2 = p$. We first show that either $b \in P$ or $-b \in P$. Assume $-b \notin P$. Define $P' = P + Pb$. It is clear that $P' + P' \subseteq P'$ and $P'P' \subseteq P'$. Suppose that $P' \cap -P' \neq \{0\}$. Let $0 \neq w \in P' \cap -P'$. Then $w = \alpha + \beta b$ and $-w = \alpha' + \beta' b$, where $\alpha, \alpha', \beta, \beta' \in P$. Then $(\alpha + \alpha') + (\beta + \beta')b = 0$ and $w \neq 0$ implies $\beta + \beta' \neq 0$ and hence $-b = (\beta + \beta')^{-1}(\alpha + \alpha') \in P$ since P is division closed, a contradiction. Thus $P' \cap -P' = \{0\}$, so P' is a partial order. It follows that $P = P'$ and $b \in P$. Thus either $b \in P$ or $-b \in P$. Without loss of generality, we may assume $b \in P$.

Since $\mathbb{Q}[b]$ is a subfield of R and $\mathbb{Q}[b] \subseteq E_P$, $2 \mid [E_P : \mathbb{Q}]$, so $[E_P : \mathbb{Q}] = 2k$, where k is a positive integer and $k \mid n$. It follows that $[R : E_P] = n/k$ is an odd integer. By a similar argument of Theorem 3.2, each real infinite prime divisor of E_P is extended to a real infinite prime divisor of R, so P must be a total order. □

In the following we collect some conditions that make a real number field being O^*. Let R be a real number field. By Primitive Element Theorem, R is a simple extension over $\mathbb{Q}$, that is, $R = \mathbb{Q}[a]$ for some $a \in R$.

Theorem 3.5. *Let R be a real number field.*

(1) *Suppose that $R = \mathbb{Q}[a]$. Let $f(x) \in \mathbb{Q}[x]$ be the irreducible polynomial such that $f(a) = 0$. If each root of $f(x)$ is a real number, then R is an O^*-field.*
(2) *Let R be a real number field. If for each complex infinite prime divisor $\{\sigma, \rho \circ \sigma\}$, $\sigma^{-1}(\mathbb{R}^+)$ is not prime, then R is an O^*-field.*
(3) *Let R be a real number field and $R = \mathbb{Q}[a]$ with the minimal polynomial $f(x)$ of a over $\mathbb{Q}$. If $f(x)$ has a pure imaginary root, then R is not an O^*-field.*

Proof. (1) Let P be a maximal partial order on R. If P is not a full infinite prime, then, by Theorem 2.1, $P = \sigma^{-1}(\mathbb{R}^+)$ for a complex infinite prime divisor $\{\sigma, \rho \circ \sigma\}$, a contradiction since the minimal polynomial $f(x)$ of a has only real roots. Thus P is full and $E_P = R$.

(2) Let P be a maximal partial order on R. Then P is an infinite prime by Lemma 2.2. So, by Theorem 2.1, $P = \sigma^{-1}(\mathbb{R}^+)$ for some real infinite prime σ by the assumption, so P is a total order on R.

(3) Suppose that $z = ib, b \in \mathbb{R}$ is a root of $f(x)$. Then there exists an embedding σ from R to $\mathbb{C}$ that sends a to ib. Let $P = \sigma^{-1}(\mathbb{R}^+)$. Then P is a partial order on R. Since $\sigma(-a^2) = -(ib)^2 = b^2 \in \mathbb{R}^+$, $-a^2 \in P$, so P cannot be extended to a total order and R is not O^*. □

As an application of Theorem 3.5, we determine all the O^*-fields R with $[R : \mathbb{Q}] = 4$.

Example 3.6. Let R be a real number field with $[R : \mathbb{Q}] = 4$. Assume that $R = \mathbb{Q}[\alpha]$, where $\alpha \in \mathbb{R}$ is a root of an irreducible polynomial $f(x)$ of degree 4 over $\mathbb{Q}$. We consider following cases.

(1) $f(x)$ has 4 real roots. By Theorem 3.5(1), R is O^*.
(2) $f(x)$ has 2 real roots and 2 pure imaginary roots. By Theorem 3.5(3), R is not O^*.
(3) $f(x)$ has 2 real roots and 2 complex roots with nonzero real part. Let $\{\sigma, \rho \circ \sigma\}$ be the complex infinite prime divisor of R. Let $E = \sigma^{-1}(\mathbb{R})$. Then E is a subfield of R, so $E = R$, $[E : \mathbb{Q}] = 2$, or $E = \mathbb{Q}$. Let r be a real root of $f(x)$ such that $\sigma(r)$ is a complex root of $f(x)$. Then $r, -r \notin E$, so $E \neq R$. If $E = \mathbb{Q}$, then $\sigma^{-1}(\mathbb{R}^+) = \mathbb{Q}^+$ is not a prime. Assume that $[E : \mathbb{Q}] = 2$. Then $E = \mathbb{Q}[\beta]$ for some $\beta \in \mathbb{R}$. Then $\sigma^{-1}(\mathbb{R}^+) = E \cap \mathbb{R}^+$ or $E \cap -\mathbb{R}^+$, and hence $\sigma^{-1}(\mathbb{R}^+) \subsetneq R \cap \mathbb{R}^+$ or $R \cap -\mathbb{R}^+$, respectively. Thus $\sigma^{-1}(\mathbb{R}^+)$ is not a prime. By Theorem 3.5(2), R is O^*.

References

[1] Fuchs, L.: Partially ordered algebraic systems. Pergamon Press, New York (1963)

[2] Harrison, D.: Finite and infinite primes for rings and fields. Mem. Am. Math. Soc. **68** (1966)

[3] Ma, J.: Lecture notes on algebraic structure of lattice-ordered rings. World Scientific Publishing, Singapore (2014)

[4] Ma, J., Yang, Y.: Commutative L^*-rings II. Quaest. Math. **5**, 719–727 (2018)

[5] Steinberg, S.: A characterization of rings in which each partial order is contained in a total order. Proc. Am. Math. Soc. **125**, 2555–2558 (1997)

Jingjing Ma
Department of Mathematics and Statistics
University of Houston-Clear Lake
Houston TX 77058
USA
e-mail: ma@uhcl.edu
URL: http://www.math.uhcl.edu/ma

Received: 27 August 2021.
Accepted: 13 May 2022.