Positivity (2023) 27:29
https://doi.org/10.1007/s11117-023-00982-w

Positivity

Galois extensions and O^*-fields

Kenneth Evans[1] · Jingjing Ma[1]

Received: 14 August 2022 / Accepted: 9 March 2023

Abstract

A field F is O^* if each partial order that makes F a partially ordered field can be extended to a total order that makes F a totally ordered field. We use the theory of infinite primes developed by Dubois and Harrison to prove the following. For a subfield F of $\mathbb{C}$ that is finite-dimensional over $\mathbb{Q}$, we prove that when F is Galois over $\mathbb{Q}$, F is an O^*-field if and only if is a subfield of $\mathbb{R}$. We find other conditions that make F an O^*-field and provide several examples. As well for an arbitrary field of characteristic 0, we characterize the maximal partial orders that are Archimedean.

Keywords Galois extension · Infinite prime · O^*-field · Normal closure · Number field · Archimedean maximal partial order

Mathematics Subject Classification 06F25

1 Introduction

A field F is called O^* if each partial order on F making F into a partially ordered field can be extended to a total order on F making F into a totally ordered field, that is, if P is the positive cone of a partial order on F, then there exists a total order on F with the positive cone T such that $P \subseteq T$. The concept of O^*-rings was introduced by Fuchs in 1963 [5]. Identifying fields that are O^*-fields is an open question in Steinberg's book "Lattice-ordered Rings and Modules" [14, Open Problem 22].

The first author was supported by the Engaged Learning to Promote STEM Graduation Grant funded by NSF, grant number 1928622.

✉ Jingjing Ma
ma@uhcl.edu

Kenneth Evans
evansk3470@uhcl.edu

1 Department of Mathematics, University of Houston-Clear Lake, 2700 Bay Area Blvd., Houston, TX 77058, USA

Published online: 23 March 2023

A field F is called a *number field* if F is a subfield of $\mathbb{C}$, the field of complex numbers, and F is finite-dimensional over $\mathbb{Q}$, the field of rational numbers. By using the theory of infinite primes for rings and fields developed by Harrison [6], the necessary and sufficient conditions for real number fields being O^*-fields have been proved recently [9]. The current paper continues the previous work and considers the number fields in $\mathbb{C}$, not necessarily in $\mathbb{R}$, the field of real numbers. This gives us the ability to use Galois extensions to get some results on O^*-fields.

Let R be a field. From [6, p. 3], a nonempty subset S of R is called a *preprime* if S is closed under the addition and multiplication in R, and $-1 \notin S$, that is, $S + S \subseteq S$, $SS \subseteq S$, 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 F be a number field that is n-dimensional over $\mathbb{Q}$. As observed on [6, p. 37] there exist exactly n embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n$ of F into $\mathbb{C}$. 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 embeddings, and $\sigma_1, \ldots, \sigma_r$ are called the *real infinite prime divisors* of F, 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 F [6]. An embedding σ of F is called *imaginary* if there exists an element $0 \ne a \in F$ such that $\sigma(a)$ is a pure imaginary complex number.

Theorem 1 (1) (*[6, Proposition 3.5]*) *Let R be a number field and let $\sigma_1, \ldots, \sigma_r$ be the real infinite prime divisors of R. Then 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) (*[6, Proposition 3.6]*) *Let R be a number field. Let P be an infinite prime of R which is not full (i.e., $P - P \ne R$). 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.*

For a number field F, the infinite primes of F are precisely the maximal partial orders on F. If P is a maximal partial order on F. Then $E_P = P - P$ is a subfield of F and P is a total order if and only if $E_P = F$. The proofs of these facts are given in [9, Lemma 2.2 & Theorem 3.1].

For more information on partially ordered rings and undefined terminology, the reader is referred to [1, 2, 5, 6, 9, 11, 13, 14]. In the following, $\mathbb{R}^+$ and $\mathbb{Q}^+$ denote the usual total order on $\mathbb{R}$ and $\mathbb{Q}$, respectively.

2 Galois extension and O^*-fields

We recall a few definitions and notations from Galois theory. Let L be a number field and K a subfield of L. The *Galois group* $\mathrm{Gal}(L/K)$ is the set of all K-automorphisms of L. Let S be a subset of $\mathrm{Galois}(L/K)$. Define

$$\mathcal{F}(S) = \{a \in L \mid f(a) = a, \forall f \in S\}.$$

Then $\mathcal{F}(S)$ is a subfield of L, called the *fixed field* of S, and clearly $K \subseteq \mathcal{F}(S)$. L is called *Galois* over K if $K = \mathcal{F}(\mathrm{Gal}(L/K))$. L is Galois over K if and only if $|\mathrm{Gal}(L/K)| = [L : K]$ [13, Corollary 2.16]. Let $L = K[\alpha]$ and $[L : K] = n$. Then L is Galois over K if and only if the minimal polynomial of α has n roots in L [13, Corollary 2.17].

Theorem 2 *Let F be a number field that is Galois over $\mathbb{Q}$. Then F is O^* if and only if F is a subfield of $\mathbb{R}$.*

Proof "$\Rightarrow$" Assume that F is O^*. Since F is Galois over $\mathbb{Q}$, F is the splitting field of a set of irreducible polynomials $\{f_j\}$ over $\mathbb{Q}$. Suppose that one f_j has a complex root $\alpha = a + ib$ with $a, b \in \mathbb{R}$ and $b \neq 0$. Then $\overline{\alpha} = a - ib$ is a root of f_j as well. So $\alpha - \overline{\alpha} = 2ib \in F$ and $(\alpha - \overline{\alpha})^2 = -(2b)^2 \neq 0$.

Let $P = \mathbb{R}^+ \cap F$. Then P is a partial order on F and $-(\alpha - \overline{\alpha})^2 \in P$. Since F is O^*, $P \subseteq T$, where T is a total order on F. Thus $(\alpha - \overline{\alpha})^2 \in T$, so $0 \neq (\alpha - \overline{\alpha})^2 \in T \cap -T$, a contradiction. Hence each f_j only contains real roots and hence $F \subseteq \mathbb{R}$.

"$\Leftarrow$" Assume $F \subseteq \mathbb{R}$. Then all infinite prime divisors of F are real infinite prime divisors since for any $a \in F$, the roots of the minimal polynomial of a over $\mathbb{Q}$ are in $F \subseteq \mathbb{R}$ [13, Proposition 3.28]. Let P be a maximal partial order on F. Then P is an infinite prime of F by [9, Lemma 2.2], so there exists a real infinite prime divisor δ of F such that $P = \delta^{-1}(\mathbb{R}^+)$ by Theorem 1(1). Thus P is a total order on F and F is O^*. □

Let F be a number field. The *normal closure* F_{nc} of F over $\mathbb{Q}$ is the splitting field over $\mathbb{Q}$ of the set of minimal polynomials of elements of F. If $F = \mathbb{Q}[\alpha]$, then F_{nc} is the splitting field of the minimal polynomial of α over $\mathbb{Q}$ and F_{nc} is Galois over $\mathbb{Q}$ [13, Proposition 5.9]. If the minimal polynomial of α over $\mathbb{Q}$ has only real roots, then $F_{nc} \subseteq \mathbb{R}$. Thus F_{nc} is O^* by Theorem 2 and hence F is O^* as well. On the other hand that F is O^* may not imply that F_{nc} is O^*. After proving the following result, we will give an example of such a field F.

Lemma 1 *Let E be a number field with a total order P and let F be an extension field of E such that $[F : E]$ is odd. Then P can be extended to a total order on F, that is, there exits a total order P_1 on F such that $P \subseteq P_1$.*

Proof Since $E = P \cup -P = P - P$, by Theorem 1(1), there exists a real infinite prime divisor δ of E such that $P = \delta^{-1}(\mathbb{R}^+)$. Let $F = E[\alpha]$ and $f(x) = a_0 + a_1 x + \cdots + x^n$ be the minimal polynomial of α over E, where $a_0, a_1, \ldots$ are in E. Define

$$g(x) = \delta(f(x)) = \delta(a_0) + \delta(a_1)x + \cdots + x^n.$$

Then $g(x)$ is a real irreducible polynomial of degree n over $\delta(E)$ since δ is a real embedding. Since $[F : E] = n$ is odd, $g(x)$ has a real root β. Define $\sigma : F \to \mathbb{C}$ as follows. For all

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in F,$$

$$\sigma(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \delta(a_0) + \delta(a_1)\beta + \cdots + \delta(a_{n-1})\beta^{n-1},$$

where $a_0, a_1, \ldots, a_{n-1} \in E$. Then σ is a real infinite prime divisor of F. Let $P_1 = \sigma^{-1}(\mathbb{R}^+)$. Then, by Theorem 1(1), P_1 is a total order on F and for all $w \in P$, $\sigma(w) = \delta(w) \in \mathbb{R}^+$. So $w \in P_1$, that is, $P \subseteq P_1$. □

Example 1 Let $\omega = e^{2\pi i/3}$ and $F = \mathbb{Q}[\omega\sqrt[3]{2}]$. Let P be a maximal partial order on F and $E_P = P - P$. Then E_P is a subfield of F [9, Theorem 2.2] and hence because $[E_P : \mathbb{Q}]$ divides $[F : \mathbb{Q}] = 3$, $[E_P : \mathbb{Q}]$ is either 3 or 1. We claim $[E_P : \mathbb{Q}] \neq 1$. If $[E_P : \mathbb{Q}] = 1$, then $E_P = \mathbb{Q}$. Since the only total order on $\mathbb{Q}$ is $\mathbb{Q}^+$, $P = \mathbb{Q}^+$. However by Lemma 1, $P = \mathbb{Q}^+$ can be extended to a total order on F, a contradiction. Thus we must have $[E_P : \mathbb{Q}] = 3$, so $E_P = F$ and P is a total order on F. Hence F is O^*. By [13, Example 1.27], $F_{nc} = \mathbb{Q}[\omega, \sqrt[3]{2}]$, so F_{nc} is not O^* by Theorem 2.

Let F be a number field. If F is O^*, then F does not have imaginary embeddings. In fact, if $\delta : F \to \mathbb{C}$ is an embedding such that $\delta(a) = ib$ for some $0 \neq a \in F$ and $b \in \mathbb{R}$, where $i = \sqrt{-1}$. Then $P = \delta^{-1}(\mathbb{R}^+)$ is a partial order on F that cannot be extended to a total order on F since $-a^2 \in P$.

However it is not clear that F having no imaginary embeddings is a sufficient condition for F being O^*. We know that if $[F : \mathbb{Q}]$ is odd, then F is always O^* from Lemma 1 or [9, Theorem 3.2].

In the following result, we collect some equivalent conditions equivalent to F not having imaginary embeddings.

Theorem 3 *Let F be a number field. The following statements are equivalent.*

(1) F does not have imaginary embeddings,
(2) For any pair (E, P), where E is a subfield of F and P is a total order on E, and any subfield K of F which is a quadratic extension over E, there exists $\alpha \in K$ such that $K = E[\alpha]$ and α is a root of irreducible polynomial $f(x) = x^2 - a$ over E for some $a \in P$,
(3) For any subfields E and K of F such that $E \subseteq K$ and $[K : E] = 2$, each total order on E can be extended to a total order on K.

Proof (1) ⇒ (2) Since P is a total order on E, by Theorem 1(1), there exists a real infinite prime divisor δ of E such that $P = \delta^{-1}(\mathbb{R}^+)$. Assume that $K = E[\alpha]$ and α satisfies the irreducible polynomial $f(x) = x^2 - a$ for some $a \in E$. If $a \notin P$, then $-a \in P$, so $-\delta(a) \in \mathbb{R}^+$. It follows that $g(x) = x^2 - \delta(a)$ has pure imaginary roots $\theta = \pm i\sqrt{-\delta(a)}$. Then $\phi : K \to \mathbb{C}$, defined by

$$\phi(c + d\alpha) = \delta(c) + \delta(d)\theta, \ \forall c, d \in E,$$

is an imaginary embedding of K, and it can be extended to an imaginary embedding of F [12, Theorem 50], a contradiction. Therefore we must have $a \in P$.

(2) ⇒ (3) Let P be a total order on E, by Theorem 1(1) there exists a real infinite prime divisor δ of E such that $P = \delta^{-1}(\mathbb{R}^+)$. By the assumption, $K = E[\alpha]$ for some α satisfying the irreducible polynomial $f(x) = x^2 - a$ with $a \in P$. Let θ be a root of $g(x) = x^2 - \delta(a)$. Since $a \in P$, $\delta(a) \in \mathbb{R}^+$ and thus $\theta \in \mathbb{R}$.

Then $\phi : K \to \mathbb{C}$, defined by

$$\phi(c + d\alpha) = \delta(c) + \delta(d)\theta,\ \forall c, d \in E,$$

is a real embedding from K to $\mathbb{C}$ that extends δ, so ϕ is a real infinite prime divisor of K that extends δ. Thus $P_1 = \phi^{-1}(\mathbb{R}^+)$ is a total order on K and $P = \delta^{-1}(\mathbb{R}^+) \subseteq \phi^{-1}(\mathbb{R}^+) = P_1$.

(3) $\Rightarrow$ (1) Let σ be an imaginary embedding of F. Then there exists $0 \neq a \in F$ such that $\sigma(a) = ib$, where $b \in \mathbb{R}$. Define $P = \sigma^{-1}(\mathbb{R}^+)$ and $E_P = P - P$. Then P is a total order on the subfield E_P of F. Since $\sigma(-a^2) = -\sigma(a)^2 = b^2 \in \mathbb{R}^+$, $-a^2 \in P$, so $a^2 \in E_P$. Thus $[E_P[a] : E_P] = 2$. By (3), P can be extended to a total order P_1 on $E_P[a]$, so $a^2 \in P_1$. On the other hand, $-a^2 \in P \subseteq P_1$. Therefore $a^2 \in P_1 \cap -P_1 = \{0\}$, a contradiction. Hence F cannot have imaginary embeddings. □

The following direct consequence of Theorem 3 is useful when showing number fields are O^*.

Corollary 1 *Let F be a number field that does not have imaginary embeddings. For a maximal partial order P on F, E_P cannot be contained in a subfield K of F such that $[K : E_P] = 2$ or m, where $m > 1$ is an odd positive integer.*

Proof Assume $E_P \subseteq K$ and K is a subfield of F with $[K : E_P] = 2$ or m, where $m > 1$ is odd. By Theorem 3 and Lemma 1, the total order P on E_P can be extended to a total order P_1 on K. Since P is a maximal partial order on F and P_1 is also a partial order on F, $P = P_1$, so $K = P_1 \cup (-P_1) = P \cup (-P) = P - P = E_P$, a contradiction. □

Theorem 4 *Let F be a number field that does not have imaginary embeddings. Assume $[F_{nc} : \mathbb{Q}] = 2^a n$, where $a \geq 1$ and n is a positive odd integer. If $G = \mathrm{Gal}(F_{nc}/\mathbb{Q})$ has a normal subgroup of order n, then F is an O^*-field.*

Proof Let P be a maximal partial order on F and $E_P = P - P$. We assume $E_P \neq F$, and get a contradiction. Let

$$N = \mathrm{Gal}(F_{nc}/F),\ H = \mathrm{Gal}(F_{nc}/E_P).$$

Then $N \subsetneq H \subseteq G$. Since $|H|$ divides $|G|$, $|H| = 2^b m$, where $0 \leq b \leq a$ is an integer and m is a positive integer that is odd and divides n. Let M be a maximal proper subgroup of H containing N and $K = \mathcal{F}(M)$. Then $|M| = [F_{nc} : K]$ and $E_P \subsetneq K \subseteq F$.

If $m = 1$ and $b = 0$, then $|H| = [F_{nc} : E_P] = 1$, so $E_P = F_{nc}$ and hence $E_P = F$, a contradiction. If $m = 1$ and $b \geq 1$, then $|H| = 2^b$ and $|M| = 2^{b-1}$ [8, Corollary 5.26]. Thus

$$[K : E_P] = \frac{[F_{nc} : E_P]}{[F_{nc} : K]} = \frac{|H|}{|M|} = 2,$$

a contradiction by Corollary 1. If $b = 0$ and $m > 1$, then $|H| = m$, and hence

$$[K : E_P] = \frac{[F_{nc} : E_P]}{[F_{nc} : K]} = \frac{|H|}{|M|}$$

is an odd integer > 1, a contradiction by Corollary 1.

In the following, assume that $b \geq 1$ and $m > 1$. Let Q be a normal subgroup of G with $|Q| = n$, and $n = p_1^{t_1} \dots p_k^{t_k}$, where $p_1, \dots, p_k$ are distinct odd prime numbers, $k \geq 1$, and $t_i \geq 1$, $i = 1, \dots, k$. For $i = 1, \dots, k$, let Q_i be a Sylow p_i-subgroup of G. Then QQ_i is a subgroup and $Q \subseteq QQ_i \subseteq G$. Since

$$|QQ_i| = \frac{|Q||Q_i|}{|Q \cap Q_i|} \text{ and } |QQ_i| \text{ divides } |G|,$$

we must have $|QQ_i| = n$, so $Q = QQ_i$ and $Q_i \subseteq Q$ for $i = 1, \dots, k$. Let W_i be a Sylow p_i-subgroup of H, $i = 1, \dots, k$. Then W_i is contained in a conjugate of Q_i in G, and hence because Q is normal, $W_i \subseteq Q$ for $i = 1, \dots, k$. Let $W = Q \cap H$. Then W is a normal subgroup of H and $W_i \subseteq W$ for $i = 1, \dots, k$, so $|W_i|$ divides $|W|$ for $i = 1, \dots, k$, and hence $|W| = m$. Since WM is a subgroup of H, either $WM = H$ or $WM = M$.

If $WM = H$, then

$$2^b m = |H| = |WM| = \frac{|W||M|}{|W \cap M|} = \frac{m|M|}{|W \cap M|},$$

so $|M| = 2^b m_1$, where m_1 is a positive integer and $m_1 | m$. Hence,

$$[K : E_P] = \frac{[F_{nc} : E_P]}{[F_{nc} : K]} = \frac{|H|}{|M|} = \frac{m}{m_1}$$

is an odd integer > 1, a contradiction by Corollary 1.

If $WM = M$, then $W \subseteq M$. The quotient group H/W is a 2-group and M/W is a maximal subgroup of H/W. Hence $|M/W| = 2^{b-1}$ [8, Corollary 5.26], so $|M| = 2^{b-1}m$ and

$$[K : E_P] = \frac{[F_{nc} : E_P]}{[F_{nc} : K]} = \frac{|H|}{|M|} = 2,$$

a contradiction by Corollary 1.

Therefore if P is a maximal partial order of F, we must have $E_P = F$, so P is a total order on F by Theorem 1(1). □

Corollary 2 *Let F be a number field that does not have imaginary embeddings. Assume $[F_{nc} : \mathbb{Q}] = 2^a p^b$, where a, b are positive integers and p is an odd prime number. If $p \geq 2^a$, then F is an O^*-field.*

Proof Since $p \geq 2^a$, the Sylow p-subgroup of G is normal, so by Theorem 4, F is O^*. □

Let F be a number field that does not have imaginary embeddings. By Theorem 4, if $[F_{nc} : \mathbb{Q}] = 4p^b$ with $b \geq 1$ and prime number $p > 3$, then F is O^*. We show that if $[F_{nc} : \mathbb{Q}] = 4(3^b)$ with $b \geq 1$, then F is O^* as well. We first have the following result that will be used in the proof.

Lemma 2 *Let G be a group of order $|G| = 4(3^k)$ with $k \geq 2$. Then G has either the normal Sylow 3-subgroup or a normal subgroup of order 3^{k-1}.*

Proof If the number of Sylow 3-subgroups of G is 1, then G has the normal Sylow 3-subgroup. Now suppose that N and M are two different Sylow 3-subgroups of G. Then

$$|N \cap M| = \frac{|N||M|}{|NM|} \geq \frac{|N||M|}{|G|} = \frac{(3^k)(3^k)}{4(3^k)} = \frac{9}{4}(3^{k-2}),$$

so because $|N \cap M|$ divides 3^k, $|N \cap M| = 3^{k-1}$.

We claim that $N \cap M$ is normal in G. It is well known that $N \cap M$ is normal in N and M [8, Corollary (5.26)]. Let $K = N_G(N \cap M)$ be the normalizer of $N \cap M$ in G. Then $NM \subseteq K$ and hence $3^{k+1} = (|N||M|)/|N \cap M| = |NM| \leq |K|$. So since $|K|$ divides $|G|$, $|K| = 4(3^k)$. Therefore $K = G$, so $N \cap M$ is normal in G. □

Example 2 Let F be a real number field that does not have imaginary embeddings. If $[F_{nc} : \mathbb{Q}] = 4(3^b)$ with $b \geq 1$, then F is O^*.

Let P be a maximal partial order on F and $E_P = P - P$. Define

$$G = \mathrm{Gal}(F_{nc}/\mathbb{Q}),\ \ H = \mathrm{Gal}(F_{nc}/E_P),\ \text{ and } N = \mathrm{Gal}(F_{nc}/F).$$

Then $N \subseteq H \subseteq G$, so $|H|$ divides $|G| = 4(3^b)$. In the following, we consider the case that $|H| = 4(3^c)$ with $1 \leq c < b$, and leave the similar verifications of the other cases to the reader.

Assume $E_P \neq F$. We derive a contradiction. Since $E_P \neq F$, $N \neq H$. Let M be a maximal proper subgroup of H containing N and define $E = \mathcal{F}(M)$. Then

$$[E : E_P] = \frac{[F_{nc} : E_P]}{[F_{nc} : E]} = \frac{|H|}{|M|},$$

by the Fundamental Theorem of Galois Theory [13, Theorem 5.1]. We will use this fact repeatedly in the argument.

(1) Assume $c = 1$, so $|H| = 12$. Then H has either a normal Sylow 2-subgroup or a normal Sylow 3-subgroup [8, Theorem (5.14)].

First assume that H has a normal Sylow 3-subgroup Q. Since QM is a subgroup and $M \subseteq QM \subseteq H$, $QM = M$ or $QM = H$. If $QM = M$, then $Q \subseteq M$ and M/Q is a maximal subgroup in H/Q. Since $|H/Q| = 4$, $|M/Q| = 2$ [8, Corollary 5.26], so $|M| = 6$, and hence $[E : E_P] = |H|/|M| = 2$, a contradiction by Corollary 1. Suppose that $H = QM$. If $|Q \cap M| = 3$ then $Q \subseteq M$ and thus $QM = M$, a contradiction. So $|Q \cap M| = 1$, and hence

$$|H| = \frac{|Q||M|}{|Q \cap M|} = 3|M|$$

so that $[E : E_P] = |H|/|M| = 3$, again a contradiction by Corollary 1.

Now assume that H has the normal Sylow 2-subgroup W. If $WM = M$, then $W \subseteq M$, so $|M| = 4$. Then $[E : E_P] = |H|/|M| = 3$, a contradiction by Corollary 1. If $H = WM$ and $|W \cap M| = 2$, then

$$12 = |H| = \frac{|W||M|}{|W \cap M|} = 2|M| \;\Rightarrow\; |M| = 6,$$

so $[E : E_P] = |H|/|M| = 2$, a contradiction by Corollary 1. If $H = WM$ and $|W \cap M| = 1$, then $|M| = 3$. Let $K = \mathcal{F}(W)$. We have

$$[K : E_P] = \frac{|H|}{|W|} = 3 \;\text{ and }\; [E : E_P] = \frac{|H|}{|M|} = 4,$$

so $[KE : E_P] = 12$ [13, Problem 17, p. 14]. We also have

$$[E_P : \mathbb{Q}] = \frac{[F_{nc} : \mathbb{Q}]}{[F_{nc} : E_P]} = \frac{4(3^b)}{4(3)} = 3^{b-1}.$$

It follows that $[KE : \mathbb{Q}] = [KE : E_P][E_P : \mathbb{Q}] = 4(3^b)$, and hence $KE = F_{nc}$.

Since $[K : E_P] = 3$, $K = E_P[\alpha]$ and α is a root of an irreducible polynomial $f(x)$ of degree 3 over E_P. Since $E_P \subseteq F \subseteq \mathbb{R}$, we may take α as a real root of $f(x)$, so $K \subseteq \mathbb{R}$, and hence since $E \subseteq F \subseteq \mathbb{R}$, $F_{nc} = KE \subseteq \mathbb{R}$. So F_{nc} is O^* by Theorem 2 and thus F is also O^*. But then $E_p = F$, a contradiction of our initial assumption.

(2) Assume $|H| = 4(3^c)$ with $c \geq 2$. By Lemma 2, H has a normal subgroup Q of order 3^c or 3^{c-1}.

(2a) Suppose that $|Q| = 3^c$. If $QM = M$, then $Q \subseteq M$, so $|M| = 2(3^c)$. Thus $[E : E_P] = |H|/|M| = 2$, a contradiction by Corollary 1. If $QM = H$, then

$$4(3^c) = |H| = |QM| = \frac{|Q||M|}{|Q \cap M|} \Rightarrow |M| = 4|Q \cap M|,$$

so $[E : E_P] = 3^c/|Q \cap M|$ is an odd integer > 1 since $|Q \cap M| \neq 3^c$, a contradiction by Corollary 1.

(2b) Suppose that $|Q| = 3^{c-1}$. If $QM = M$, then $Q \subseteq M$. Since Q is contained in a Sylow 3-subgroup of H and M is maximal, $Q \neq M$. Since $|H/Q| = 12$ and M/Q

is maximal in H/Q, $|M/Q| = 3, 6$, or 4, and hence $|M| = 3^c, 2(3^c)$ or $4(3^{c-1})$. If $|M| = 2(3^c)$ or $4(3^{c-1})$, then $[E : E_P] = |H|/|M|$ is either 2 or 3, a contradiction by Corollary 1.

Consider the case that $|M| = 3^c$. Let W be a Sylow 2-subgroup of H and $K = \mathcal{F}(W)$. Then $[K : E_P] = |H|/|W| = 3^c$. It follows that $[EK : E_P] = [E : E_P][K : E_P] = 4(3^c)$ [13, Problem 17, p. 14]. Since

$$[E_P : \mathbb{Q}] = \frac{[F_{nc} : \mathbb{Q}]}{[F_{nc} : E_P]} = \frac{4(3^b)}{4(3^c)} = 3^{b-c},$$

we have $[EK : \mathbb{Q}] = 4(3^b)$, so $EK = F_{nc}$. Similar to the argument used in (1), it follows that $F_{nc} \subseteq \mathbb{R}$, a contradiction.

If $QM = H$, then

$$4(3^c) = |H| = \frac{|Q||M|}{|Q \cap M|} = \frac{3^{c-1}|M|}{|Q \cap M|} \Rightarrow |M| = 12|Q \cap M|,$$

so $[E : E_P] = |H|/|M|$ is an odd integer > 1, a contradiction again by Corollary 1.

Therefore, we have proved that if $[F_{nc} : \mathbb{Q}] = 4(3^b)$ with $b \geq 1$, then F is O^*.

Theorem 5 *Let F be a real number field that does not have any imaginary embeddings and $[F_{nc} : \mathbb{Q}] = 4p^b$, where p is an odd prime number and $b \geq 1$, then F is O^*.*

Proof The case for $p = 3$ is demonstrated in Example 2, leaving only $p \geq 4$, for which the Sylow p-subgroup of G is normal so by Theorem 4, F is O^* □

Let F be a number field and F_{nc} be its normal closure. Define

$$G = \text{Gal}(F_{nc}/\mathbb{Q}) \text{ and } N = \text{Gal}(F_{nc}/F).$$

Suppose that $|N| = 2^a n$ where $a \geq 1$ and n is a positive odd integer. Let S be a Sylow 2-subgroup of N and $E = \mathcal{F}(S)$. Then $F \subseteq E \subseteq F_{nc}$ with $[E : F] = n$ and $[F_{nc} : E] = 2^a$ [13, Theorem 5.1].

Although it is not certain if F is O^* when F does not have imaginary embeddings, F is indeed O^* in case that E does not have imaginary embeddings.

Theorem 6 *Let E be defined as above. If E does not have imaginary embeddings, then F is an O^*-field.*

Proof Let P be a maximal partial order on F and $E_P = P - P$. Define $H = \text{Gal}(F_{nc}/E_P)$ and assume $|H| = 2^t k$ where $t \geq 1$ and k is a positive odd integer. Since $N \subseteq H$, $|N|$ divides $|H|$ implies that $a \leq t$ and $n \mid k$. Let W be a Sylow 2-subgroup of H such that $S \subseteq W$, where S is a Sylow 2-subgroup of N, and let $K = \mathcal{F}(W)$. So $|W| = 2^t$. Then there exists a chain of subgroups of W:

$$S \subseteq S_1 \subseteq \ldots \subseteq S_{t-a-1} \subseteq W,$$

such that $|S_i| = 2^{a+i}$ for $i = 1, \ldots, t-a-1$ [8, Corollary 5.23]. Let $E_i = \mathcal{F}(S_i)$ for $i = 1, \ldots, t-a-1$. We have

$$K \subseteq E_{t-a-1} \subseteq \ldots \subseteq E_1 \subseteq E$$

and $[E : E_1] = 2, [E_1 : E_2] = 2, \ldots, [E_{t-a-1} : K] = 2$.

Now that P is a total order on E_P and $[K : E_P] = |H|/|W| = k$ is odd implies that P can be extended to a total order P_K on K by Lemma 1. Since E does not have imaginary embeddings, by Theorem 3, P_K can be extended to a total order P_{t-a-1} on E_{t-a-1}, so P can also be extended to the total order P_{t-a-1}. Continuing this process, we have that P can be extended to a total order P_E on E. Thus P can be extended to a total order $P_E \cap F$ on F since $F \subseteq E$. Therefore, since P is maximal on F, $P = P_E \cap F$ is a total order on F and F is O^*. □

The following is a direct consequence of Theorem 6.

Corollary 3 *If a number field F has no imaginary embeddings and $[F_{nc} : F] = 2^k$ where k is a positive integer, then F is O^*.*

3 Archimedean maximal partial orders on fields

Harrison and Dubois obtained many important results not only for the infinite primes on the number fields, but also for the infinite primes on arbitrary fields as well [2–4, 6, 7]. In this section, we use the connection between Archimedean maximal partial orders and infinite primes on an arbitrary field of characteristic 0 to study Archimedean maximal partial orders.

Let $(R, \leq)$ be a partially ordered field. The partial order $\leq$ on R is called *Archimedean* if for any $a, b \in R$, $\mathbb{Z}a \leq b$ implies that $a = 0$, where $\mathbb{Z}$ is the set of all integers and $\mathbb{Z}a \leq b$ means that $ma \leq b$ for all integers m. The partial order $\leq$ on R is called *strong Archimedean* if $0 \leq 1$ and for any $0 \leq a \in R$, there is a positive integer n such that $0 \leq n - a$. The above definition for Archimedean is widely used in partially ordered groups and rings, see [1, 5, 9, 15] and the above definition for strong Archimedean is called Archimedean in [2, 6].

Lemma 3 *Let $(R, \leq)$ be a partially ordered field.*

(1) If $\leq$ is a total order, then $\leq$ is Archimedean if and only if it is strong Archimedean.
(2) If $\leq$ is a lattice order that is strong Archimedean, then it is a total order. However a lattice order that is Archimedean may not be a total order.

Proof (1) Since $\leq$ is a total order, $1 \geq 0$. Assume that $(R, \leq)$ is Archimedean and $0 \leq a$. Then $\mathbb{Z}1 \not\leq a$, so there exists a positive integer n such that $n > a$, so $0 \leq n - a$. Thus $(R, \leq)$ is strong Archimedean. Now assume that $(R, \leq)$ is strong Archimedean and $\mathbb{Z}a \leq b$ for some $a, b \in R$. Suppose that $a \neq 0$. If $a > 0$, then for any positive integer n, $na \leq b$ implies that $n \leq a^{-1}b$ for all integers n, so there is no positive integer m such that $0 \leq m - a^{-1}b$, a contradiction. If $a < 0$, then for all positive integers n, $n(-a) \leq b$ implies that $n \leq (-a)^{-1}b$, a contradiction again. Thus we must have $a = 0$, that is, $(R, \leq)$ is Archimedean.

(2) Let $(R, \leq)$ be a lattice-ordered field that is strong Archimedean and $a \in R$. Since $a^+ = a \vee 0 < n$ and $a^- = -a \vee 0 < m$ for some positive integers n, m, we have

$$a^+a^- = a^+a^- \wedge a^+a^- \leq na^- \wedge ma^+ \leq nm(a^+ \wedge a^-) = 0.$$

Hence $a^+a^- = 0$, so $a^+ = 0$ or $a^- = 0$, that is, $(R, \leq)$ is a totally ordered field. □

An example of an Archimedean lattice order that is not a total order is $R = \mathbb{Q}[\sqrt{2}]$ with the coordinate-wise ordering $R^+ = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}^+\}$.

Let P be a partial order on R and suppose that $1 \in P$. Define

$$J_P = \{a \in R \mid 1 + \mathbb{Z}a \subseteq P\}, \text{ where } \mathbb{Z}a = \{na \mid n \in \mathbb{Z}\}.$$

Lemma 4 *For any Archimedean partial order P with $1 \in P$, $J_P = \{0\}$.*

Proof It is clear that $0 \in J_P$. Let $a \in J_P$. Then $1 + \mathbb{Z}a \geq_P 0$, where $\geq_P$ is the partial order with the positive cone P. Then we have $\mathbb{Z}a \leq_P 1$, so $a = 0$ since P is Archimedean. Therefore $J_P = \{0\}$. □

Theorem 7 *Let R be a field and let P be a maximal partial order on R.*

(1) Then $1 \in P$, P is an infinite prime of R, and $E_P = P - P$ is a subfield of R.
(2) If P is Archimedean, then P is strong Archimedean.

Proof (1) We first show that if $0 \neq a \in P$, then $a^{-1} \in P$. It is easy to see that,

$$P' = \{x \in R \mid wx \in P \text{ for some } 0 \neq w \in P\}$$

is a partial order on R and $P \subseteq P'$. Since P is maximal, $P = P'$. Then $a^{-1} \in P' = P$ because $a^2a^{-1} = a \in P$. In particular, since P is maximal, there exists $0 \neq a \in P$, and thus $1 = aa^{-1} \in P$.

It is clear that P is a preprime. Assume that $P \subsetneq P_1$, where P_1 is a preprime. We derive a contradiction. Take $t \in P_1 \backslash P$. Define

$$P[t] = \{f(t) \mid f(t) \text{ is a polynomial in } t \text{ with coefficients in } P\}.$$

It is clear that $P \subseteq P[t]$ and $P[t]$ is closed under the addition and multiplication of R. If $P[t] \cap (-P[t]) = \{0\}$, then $P[t]$ is a partial order on R, so $P = P[t]$ since P is a maximal partial order. Then $t \in P$, a contradiction. Thus $P[t] \cap (-P[t]) \neq \{0\}$. Let $w \in P[t] \cap (-P[t])$ and $w \neq 0$. Then $w = f(t)$ and $-w = g(t)$ for some $f(t), g(t) \in P[t]$, so $f(t) + g(t) = 0$. Thus we have $c_nt^n + \ldots + c_1t + c_0 = 0$ with $c_i \in P$ and $c_0 \neq 0$, so $c_0^{-1} \in P$ implies that

$$-1 = c_0^{-1}c_nt^n + \ldots + c_0^{-1}c_1t \in P[t] \subseteq P_1,$$

a contradiction. Therefore P is a maximal preprime with $1 \in P$, that is, P is an infinite prime.

To see that E_P is subfield of R, take $0 \neq t \in E_P$. If $t \in P$, then $t^{-1} \in P$. Assume that $t \notin P$. Define $P[t]$ as above. If $P[t] \cap (-P[t]) = \{0\}$ then $P[t]$ is a partial order on R that contains P, so $P = P[t]$ and hence $t \in P$, a contradiction. Therefore, $P[t] \cap (-P[t]) \neq \{0\}$. So the same argument as in the previous paragraph gives

$$1 = -(c_0^{-1} c_n t^{n-1} + \cdots + c_0^{-1} c_1) t,$$

where $c_0 \neq 0, c_1, \ldots, c_n \in P$ and $n \geq 1$. So $t^{-1} = -(c_0^{-1} c_n t^{n-1} + \cdots + c_0^{-1} c_1) \in E_P$, and hence E_P is a subfield of F.

(2) By Lemma 4, $J_P = \{0\}$, so P is strong Archimedean [7, Corollary 1.4]. □

For a number field F and a maximal partial order P on F, P is a strong Archimedean infinite prime divisor of F [6, 9]. Thus if P is directed, $P = \delta^{-1}(\mathbb{R}^+)$ for a real embedding σ of F, and if P is not directed, $P = \sigma^{-1}(\mathbb{R}^+)$ for a complex embedding δ on F by Theorem 1. We generalize this result to Archimedean maximal partial orders on an arbitrary field of characteristic 0.

Corollary 4 *Let R be a field of characteristic 0 and suppose that P is a maximal partial order on R that is Archimedean.*

(1) If P is directed, then there exists an embedding σ from R to $\mathbb{R}$ such that $P = \sigma^{-1}(\mathbb{R}^+)$. In particular, P is a total order on R.
(2) If P is not directed, then there exists an embedding δ from R to $\mathbb{C}$ such that $P = \delta^{-1}(\mathbb{R}^+)$ and $\delta(R) \not\subseteq \mathbb{R}$.

Proof (1) By Theorem 6, P is a strong Archimedean infinite prime of R. Since P is directed, $R = P - P$. It follows from [6, Proposition 1.7] or [2, 4.9] that there exists an embedding $\sigma : R \to \mathbb{R}$ such that $P = \sigma^{-1}(\mathbb{R}^+)$, so P is a total order on R.

(2) By [7, Corollary 1.4], there is an embedding δ from R to $\mathbb{C}$ such that $P = \delta^{-1}(\mathbb{R}^+)$. Since P is not directed, $\delta(R) \not\subseteq \mathbb{R}$. □

Example 3 A directed maximal partial order may not be a total order if it is not Archimedean. For instance, let $\mathbb{R}$ be equipped with a non-Archimedean total order $\leq$. So there exists $z \in \mathbb{R}$ such that $n \leq z$ for all positive integers n. Define the positive cone on $\mathbb{C}$ as follows.

$$P = \{a + bi \mid 0 \leq a \text{ and } n|b| \leq a \text{ for all } n > 0, a, b \in \mathbb{R}\},$$

where $|b| = b$ if $b \geq 0$ in $\mathbb{R}$ and $|b| = -b$ if $b < 0$ in $\mathbb{R}$. Then P is a directed partial order that is not Archimedean [10, Theorem 1]. This maximal partial order is not a total order because $\mathbb{C}$ cannot have a total order with respect to which it is a totally ordered field.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Birkhoff, G., Pierce, R.R.S.: Lattice-ordered rings. An. Acad. Brasil Ci. **28**, 41–69 (1956)
2. Dubois, D. W.: Infinite prime and ordered fields, Dissertations Math. (Rozprawy Math.), 69 (1971)
3. Dubois, D.W.: A note on David Harrison's theory of preprimes. Pacific J. Math. **21**, 15–19 (1967)
4. Dubois, D.W.: On partly ordered fields. Proc. Amer. Math. Soc. **7**, 918–930 (1956)
5. Fuchs, L.: Partially ordered algebraic systems, Dover Publications, Inc. Mineola, New York (2011)
6. Harrison, D.K.: Finite and infinite primes for rings and fields, Memoirs of the American Mathematical Society, 68, Providence, Rhode Island (1966)
7. Harrison, D.K., Warner, H.D.: Infinite primes of fields and completions. Pacific J. Math. **45**, 201–216 (1974)
8. Issacs, I.M.: Algebra, a Graduate Course. Brook/Cole Publishing Company, Boston (1994)
9. Ma, J.: The number fields that are O*-fields, Algebra Universalis, **83**, 23 (2022)
10. Ma, J.: Partial orders on C = D + Di and H = D + Di + Dj + Dk. Int. J. Adv. Math. Sci. **3**, 156–160 (2015)
11. Ma, J.: Lecture Notes on Algebraic Structure of Lattice-Ordered Rings. World Scientific Publishing (2014)
12. Marcus, D.A.: Number fields, Universitext, 2nd edn. Springer, NewYork (2018)
13. Monrandi, P.: Field and Galois Theory. Springer, New York (1996)
14. Steinberg, S.A.: Lattice-Ordered Rings and Modules. Springer, New York (2010)
15. Steinberg, S.A.: A characterization of rings in which each partial order is contained in a total order. Proc. Amer. Math. Soc. **125**, 2555–2558 (1997)