

# Real Closed Field

Artie Khovanov

December 29, 2025

We synthesise material from [1], [4], [2] and [3] as convenient.

Note that the meaning of the notation  $F(\sqrt{a})$  depends on whether  $a$  is a square in  $F$ . We take care to write it only in the non-trivial case. The same applies to  $F(i)$ .

## 0.1 Ordered Fields

We begin with a purely algebraic characterisation of an ordered field. This relies on the theory of *ring orderings*, which can be found in [5].

**Definition 1.** A field is real if  $-1$  is not a sum of squares.

**Theorem 2.** *A field can be ordered if and only if it is real.*

We can also characterise algebraically whether a field  $F$  has a unique ordering. This allows us to talk about ‘the ordering’ on  $F$  without ambiguity.

**Lemma 3.** *Let  $F$  be a real field. There is a unique ordering on  $F$  if and only if, for each  $a \in F$ , either  $a$  or  $-a$  is a sum of squares.*

**Corollary 4.** *Let  $F$  be an ordered field. Then  $F$  has a unique field ordering if and only if every non-negative element is a sum of squares.*

*Proof.* □

**Corollary 5.** *There is a unique field ordering on  $\mathbb{Q}$ .*

*Proof.* We use Corollary 4. Let  $x \in \mathbb{Q}$  be non-negative. Then  $x = p/q$  for some integers  $p \geq 0$  and  $q > 0$ , so

$$x = \underbrace{\frac{1}{q^2} + \cdots + \frac{1}{q^2}}_{pq \text{ times}}.$$

□

There is a corresponding algebraic characterisation of an ordered field extension.

**Lemma 6.** *Let  $F$  be an ordered field, and let  $K/F$  be a field extension. Then there is an ordering on  $K$  making the extension  $K/F$  ordered if and only if  $\sum_i x_i \alpha_i^2 \neq -1$  for all choices of  $\alpha_i \in K$  and  $x_i \in F_{\geq 0}$ .*

**Lemma 7.** *Let  $F$  be an ordered field, and let  $K/F$  be a field extension. Suppose that there is an  $F$ -linear functional  $\pi : K \rightarrow F$  such that, for all  $x \in K$ ,  $\pi(x^2) \geq 0$ . Then there is a field ordering on  $K$  making  $K/F$  ordered.*

*Proof.* Consider the sum  $\sum_i x_i \alpha_i^2$  for some  $\alpha_i \in K$  and  $x_i \in F_{\geq 0}$ . By  $F$ -linearity, we compute

$$\pi \left( \sum_i x_i \alpha_i^2 \right) = \sum_i x_i \pi(\alpha_i^2) \geq 0.$$

Since  $\pi(-1) = -1 < 0$ , we are done by Lemma 6. □

**Corollary 8.** *Let  $F$  be a ordered field, and suppose  $a \in F$  is non-negative (and not a square). Then there is a field ordering on  $F(\sqrt{a})$  making  $F(\sqrt{a})/F$  ordered.*

*Proof.* Let  $\pi : F(\sqrt{a}) \rightarrow F$  be the projection induced by the  $F$ -basis  $\{1, \sqrt{a}\}$ . For  $x, y \in F$ , we have  $\pi((x + y\sqrt{a})^2) = x^2 + ay^2 \geq 0$ . We are done by Lemma 7.  $\square$

**Lemma 9.** *Let  $F$  be an ordered field, and let  $K/F$  be an odd-degree extension. Then there is a field ordering on  $K$  making  $K/F$  ordered.*

*Proof.* Since  $\text{char } R = 0$ , we can apply the primitive element theorem. Let  $K = F(\alpha)$  for some  $\alpha \in K$ , and let  $f$  be the minimal polynomial of  $\alpha$  over  $K$ . Then  $\deg f = [K : F]$  is odd. By Lemma 6, we need to show that the congruence

$$\sum_i a_i g_i^2 \equiv -1 \pmod{f} \quad (\star)$$

fails to hold for any non-negative  $a_i \in F$  and polynomials  $g_i \in F[X]$  each of degree at most  $\deg f - 1$ . Proceed by induction on  $\deg f$ ; if  $\deg f = 1$ , then  $(\star)$  reduces to an equality of a non-negative element of  $F$  with a negative one. Otherwise, suppose for a contradiction that  $(\star)$  holds. Without loss of generality, we may assume, for all  $i$ , we have  $a_i \neq 0$  and that  $\deg g_i < \deg f$ .

Rearranging  $(\star)$ , we have  $\sum_i a_i g_i^2 + 1 = hf$  for some  $h \in F[X]$ . Let  $d = \max_i \deg g_i$ ; note that  $d < \deg f$  by construction. Since each  $a_i$  is positive, the  $2d$ th coefficient on the left-hand side must be positive. Therefore

$$\deg h + \deg f = \deg \left( \sum_i a_i g_i^2 + 1 \right) = 2d.$$

Then  $\deg h$  is odd, so  $h$  has an odd-degree irreducible factor  $\tilde{h}$ . We have

$$\deg \tilde{h} \leq \deg h = 2d - \deg f < \deg f,$$

but  $\sum_i a_i g_i^2 \equiv -1 \pmod{\tilde{h}}$ . We are done by induction.  $\square$

There is an easier way to construct ordered field extensions if we don't care about them being algebraic.

**Lemma 10.** *Let  $F$  be an ordered field, and let  $a \in F$ . Then there is a unique ordering on the function field  $F(X)$  making  $F(X)/F$  ordered such that  $X > a$  but  $b > X$  for  $b > a$ , and a unique one such that  $X < a$  but  $b < X$  for  $b < a$ .*

Intuitively,  $X$  is infinitesimally close to  $a$ . When  $a = 0$ , we often write  $R(\varepsilon)$  for  $R(X)$  with the first type of ordering.

## 0.2 Real Closed Fields

**Definition 11.** A real closed field is an ordered field in which every non-negative element is a square and every odd-degree polynomial has a root.

**Lemma 12.** *The ordering on a real closed field is unique.*

*Proof.* Follows directly from Corollary 4.  $\square$

Fix a real closed field  $R$ . In what follows, all algebraic extensions are given up to  $R$ -isomorphism, as is conventional. Observe that, since  $-1$  is not a square in  $R$ ,  $R(i)/R$  is a quadratic extension. We show that this is the **only** nontrivial algebraic extension of  $R$ .

**Lemma 13.** *There is no nontrivial odd-degree finite extension of  $R$ .*

*Proof.* Let  $K/R$  be an odd-degree extension of  $R$ . By the primitive element theorem,  $K = R(\alpha)$  for some  $\alpha \in K$ . Let  $f$  be the minimal polynomial of  $\alpha$  over  $R$ . Then  $f$  is irreducible, but  $\deg f = [K : R]$  is odd, so  $f$  has a root in  $R$ . Therefore,  $[K : R] = \deg f = 1$ ; that is,  $K \cong R$ .  $\square$

**Lemma 14.** *The field  $R(i)$  is the unique quadratic extension of  $R$ .*

*Proof.* Let  $K/R$  be a quadratic extension. Since  $\text{char}(R) \neq 2$ , we have  $K \cong R(\sqrt{a})$  for some  $a \in R$ . Since nonnegative elements of  $R$  are squares,  $a$  is negative and so  $-a$  is a square in  $R$ . Rescaling by  $\sqrt{-a}$ , we get  $R(\sqrt{a}) \cong R(i)$ .  $\square$

**Lemma 15.** *There is no quadratic extension of  $R(i)$ .*

*Proof.* Since  $\text{char } R(i) \neq 2$ , it suffices to show that every element of  $R(i)$  is a square. Indeed, take  $x = a + bi \in R(i)$  with  $a, b \in R$ . If  $b = 0$ , then either  $a \geq 0$  and so  $x$  is a square in  $R$ , or  $a \leq 0$  and so  $a = (i\sqrt{-a})^2$  is a square in  $R$ . Now let  $b \neq 0$ . Then we compute  $x = (c + di)^2$ , where

$$c = \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \text{ and } d = \frac{b}{2c}.$$

To see that  $c$  and  $d$  are well-defined elements of  $R$ , observe that  $a^2 + b^2 > a^2 \geq 0$  (as  $b \neq 0$ ), and so  $a + \sqrt{a^2 + b^2} > 0$ . Therefore the square roots above lie in  $R$  and  $c \neq 0$ .  $\square$

**Theorem 16.** *The only finite extensions of  $R$  are  $R$  itself and  $R(i)$ .*

*Proof.* By separability, every finite extension of  $R$  is contained in a finite Galois extension. Since  $R(i)/R$  has no intermediate fields, it suffices to show the result for finite Galois extensions.

Let  $K/R$  be a nontrivial Galois extension of degree  $2^k \cdot a$ , where  $k \geq 0$  and  $a \geq 1$  is odd. Applying the Galois correspondence to a Sylow 2-subgroup of  $\text{Gal}(K/R)$  yields an intermediate extension of degree  $a$ ; by Lemma 13, we have  $a = 1$  (and  $k > 0$ ). If  $k > 1$ , iterating the last construction yields intermediate extensions  $K/L/M/R$  with  $[L : M] = [M : R] = 2$ . By Lemma 14,  $M \cong R(i)$ , contradicting Lemma 15.  $\#$  Therefore  $k = 1$  and (by Lemma 14)  $K \cong R(i)$ .  $\square$

**Corollary 17.** *The only algebraic extensions of  $R$  are  $R$  itself and  $R(i)$ .*

*Proof.* An infinite algebraic extension contains finite subextensions of arbitrarily large degree.  $\square$

**Corollary 18.**  $\bar{R} = R(i)$ .

*Proof.*  $\square$

The converse to Theorem 16 is much easier.

**Lemma 19.** *Suppose  $R$  is an ordered field whose only nontrivial finite extension is  $R(i)$ . Then  $R$  is real closed.*

*Proof.* Let  $a \in R$  be non-negative. If  $a$  is not a square, then  $R(\sqrt{a}) \cong R(i)$ . Suppose  $i$  maps to  $x + y\sqrt{a}$  for some  $x, y \in R$ ; then  $-1 = x^2 + ay^2 + 2xy\sqrt{a}$ . Comparing coefficients,  $-1 = x^2 + ay^2 \geq 0$ .  $\#$  Therefore  $a$  is a square in  $R$ .

Now, fix a nonlinear odd-degree polynomial  $f \in R[X]$ . Then  $R[X]/(f)$  cannot be a field since  $R$  has no nontrivial odd-degree extensions, and so  $f$  must be reducible. We are done by induction on the degree.  $\square$

As before, let  $R$  be a real closed field. Theorem 16 is a powerful tool for deriving more of its properties.

**Lemma 20.**  *$R$  is maximal with respect to algebraic extensions by ordered fields.*

*Proof.* Since  $-1$  is a square in  $R(i)$ , the field  $R(i)$  is not formally real and therefore cannot be ordered (by Theorem 2). We are done by Corollary 17.  $\square$

In particular,  $R$  is maximal with respect to ordered algebraic extensions.  
The next property is a little less obvious.

**Lemma 21.** *The monic irreducible polynomials over  $R[X]$  have form  $X - c$  for some  $c \in R$  or  $(X - a)^2 + b^2$  for some  $a, b \in R$  with  $b \neq 0$ .*

*Proof.* Let  $f \in R[X]$  be monic and irreducible. The field  $R_f = R[X]/(f)$  is a finite extension of  $R$ , so it is classified by Theorem 16. If  $R_f \cong R$ , then  $\deg f = 1$ , so  $f = X - c$  for some  $c \in R$ . If  $R_f \cong R(i)$ , let the isomorphism be  $\varphi$ , and suppose  $\varphi(X + (f)) = a + bi$  ( $a, b \in R$ ). Note that  $b \neq 0$  since  $\varphi^{-1}$  is constant on  $R$ . Rearranging, we see that  $\varphi((X - a)^2 + b^2 + (f)) = 0$ ; that is,  $(X - a)^2 + b^2 \in (f)$ . Since this polynomial is monic and has the same degree as  $f$ , it must in fact be equal to  $f$ .

Conversely, linear polynomials over a domain are irreducible by degree, and reducible quadratics have a root. A root of  $f = (X - a)^2 + b^2$  with  $a, b \in R$  is an element  $r \in R$  satisfying  $(r - a)^2 = -b^2$ . Since squares are non-negative, if  $b \neq 0$  then  $f$  must be irreducible.  $\square$

**Lemma 22.** *Polynomials over  $R$  satisfy the intermediate value property.*

*Proof.* We will prove that, for all  $f \in R[X]$  and all  $a, b \in R$  with  $a \leq b$ , if  $f(a) \leq 0 \leq f(b)$ , then there is some  $c \in [a, b]$  such that  $f(c) = 0$ .

Fix  $a, b \in R$  with  $a \leq b$ , and proceed by induction on  $\deg f$ . If  $\deg f = 0$ , then  $f$  is constant and the result is clear. Otherwise, take a monic irreducible factor  $g$  of  $f$ ; then  $g$  is classified by Lemma 21.

Observe that, if  $g(a)$  and  $g(b)$  are both positive, then  $f/g$  satisfies the inductive hypothesis, and so has a root in  $[a, b]$ . If  $g = (X - a)^2 + b^2$  with  $a, b \in R$  and  $b \neq 0$ , then  $g$  is everywhere positive. If  $g = X - c$  with  $c \in R$ , then either  $c \in [a, b]$  and  $g(c) = 0$ , or  $c \notin [a, b]$  and  $f(a)$  and  $f(b)$  have the same sign. In this last case, either  $f/g$  or  $f/(-g)$  satisfies the inductive hypothesis. In all cases,  $f$  has a root in  $[a, b]$ .  $\square$

In fact, the converses to Lemmas 20 and 22 also hold!

**Theorem 23.** *Let  $R$  be an ordered field whose polynomials satisfy the intermediate value property. Then  $R$  is real closed.*

*Proof.* Let  $a \in R$  be non-negative, and consider the polynomial  $f = X^2 - a$ . Then  $f(0) = -a \leq 0$ , but  $f(a + 1) = a^2 + a + 1 > 0$ . By the intermediate value property,  $f$  has a root in  $R$ , and so  $a$  is a square in  $R$ .

Let  $f$  be an odd-degree polynomial over  $R$ . Write  $f = a_n X^n + \dots + a_0$ . We will show  $f$  has a root in  $R$ . Replacing  $f$  by  $-f$  if necessary, we may assume  $a_n > 0$ . For  $x > 1$ , we compute

$$f(x) \geq x^{n-1}(a_n x - n \max_i |a_i|).$$

Therefore, when  $x > \max\{1, n \max_i |a_i|/a_n\}$ ,  $f(x) > 0$ . A similar calculation shows that  $f(x) < 0$  for sufficiently large negative values of  $x$ . We are done by the intermediate value property.  $\square$

**Theorem 24.** *Let  $R$  be an ordered field maximal with respect to ordered algebraic extensions. Then  $R$  is real closed.*

*Proof.* Let  $a \in R$  be non-negative, and suppose  $a$  is not a square. By Corollary 8, there is an ordering making the nontrivial extension  $R(\sqrt{a})/R$  ordered, contradicting maximality.<sup>#</sup> Therefore  $a$  is a square in  $R$ .

By induction on degree, it suffices to show that irreducible odd-degree polynomials over  $R$  are all linear. Let  $f \in R[X]$  be such a polynomial, and consider the odd-degree field extension  $R_f = R[X]/(f)$ . By Lemma 9, there is an ordering making  $R_f/R$  an ordered extension; by maximality,  $R_f \cong R$ , and therefore  $\deg f = [R_f : R] = 1$ .  $\square$

In particular, an ordered field maximal with respect to algebraic extensions by ordered fields is real closed.

Theorem 24 gives us a way to “construct” real closed fields.

**Lemma 25.** *An algebraically closed field of characteristic 0 has an index-2 real closed subfield.*

*Proof.* Let  $C$  be an algebraically closed field of characteristic 0. Observe that the prime subfield  $\mathbb{Q}$  can be ordered. Further, given an ordered subfield  $F$  with  $\bar{F} \neq C$ , we can use Lemma 10 to adjoin an element transcendental over  $F$ , obtaining a strictly bigger ordered subfield.

Apply Zorn’s lemma to obtain a maximal ordered subfield  $R \subseteq C$ ; then  $\bar{R} = C$ . By Theorem 24,  $R$  must be real closed. By Corollary 18,  $C \cong R(i)$ , and so  $[C : R] = 2$ .  $\square$

In summary, we have proved the following characterisation of real closed fields.

**Theorem 26.** *Let  $R$  be an ordered field. TFAE:*

1.  $R$  is real closed.
2.  $\bar{R} = R(i)$  (and  $-1$  is not a square in  $R$ ).
3. Polynomials over  $R$  satisfy the intermediate value property.
4.  $R$  is maximal with respect to ordered algebraic extensions.
5.  $R$  is maximal with respect to algebraic extensions by ordered fields.

*Proof.*  $\square$

### 0.3 Real Closures

**Definition 27.** Let  $F$  be an ordered field. A real closure of  $F$  is a real closed ordered algebraic extension of  $F$ .

**Lemma 28.** *Let  $F$  be an ordered field. Then  $F$  has a real closure.*

*Proof.* Apply Zorn’s lemma to ordered algebraic extensions of  $F$ . We are done by Theorem 24.  $\square$

Just like with the algebraic closure, it makes sense to talk of *the* real closure of an ordered field. Proving this uniqueness result requires a method of root-counting in real fields known as Sturm’s theorem.

**Theorem 29** (Corollary to Sturm’s Theorem). *Let  $F$  be an ordered field, and let  $f$  be a polynomial over  $F$ . Then  $f$  has the same number of roots in any real closure of  $F$ .*

*Proof.* TODO : decide on the generality of the statement of Sturm's Theorem  $\square$

**Lemma 30.** *Let  $F$  be an ordered field with a real closure  $R$ , and let  $K/F$  be a finite ordered extension. Then there is an  $F$ -homomorphism  $K \rightarrow R$ .*

*Proof.* By the primitive element theorem,  $K = F(\alpha)$  for some  $\alpha \in K$ . Let  $f$  be the minimal polynomial of  $\alpha$  over  $F$ . Since  $F$  has a root in  $K$ , it has a root in a real closure of  $K$  (one exists by Lemma 28). By Theorem 29,  $f$  has a root  $\beta$  in  $R$ . Therefore define  $\varphi : K \rightarrow R$  with  $\varphi(\alpha) = \beta$ .  $\square$

**Lemma 31.** *Let  $F$  be an ordered field with a real closure  $R$ , and let  $K/F$  be a finite ordered extension. Then there is a unique order-preserving  $F$ -homomorphism  $K \rightarrow R$ .*

*Proof.* Fix a real closure  $R'$  of  $K$  (one exists by Lemma 28).

By the primitive element theorem,  $K = F(\alpha)$  for some  $\alpha \in K$ . Let  $f$  be the minimal polynomial of  $\alpha$  over  $F$ , and let  $\alpha_1 < \dots < \alpha_m$  be the roots of  $f$  in  $R'$ , with  $\alpha = \alpha_k$ . By Theorem 29,  $f$  also has  $m$  roots in  $R$ ; let them be  $\beta_1 < \dots < \beta_m$ . Since non-negative elements of  $R'$  are squares, and  $x_1, \dots, x_{m-1} \in R'$  such that  $\alpha_{j+1} - \alpha_j = x_j^2$ , and let  $L = K(\alpha_1, \dots, \alpha_m, r, x_1, \dots, x_{m-1}) \leq R'$ . Now, suppose we have a  $K$ -homomorphism  $\psi : L \rightarrow R$ . Each  $\psi(\alpha_j)$  is equal to a different  $\beta_i$ . Then  $\psi(\alpha_{j+1}) - \psi(\alpha_j) = \psi(x_j)^2 \geq 0$ , so  $\psi(\alpha_1) < \dots < \psi(\alpha_m)$ , and so  $\psi(\alpha_j) = \beta_j$  for all  $j$ .

By Lemma 30, there is in fact an  $F$ -homomorphism  $\varphi : L \rightarrow R$ . We will show that  $\varphi$  is order-preserving. Indeed, fix a non-negative element  $x \in L$ . As before, find  $r \in R'$  such that  $x = r^2$ , and let  $M = L(r) \leq R'$ . Apply Lemma 30 again to obtain an  $L$ -homomorphism  $\psi : M \rightarrow R$ ; then  $\varphi(x) = \psi(x) = \psi(r)^2 \geq 0$ . Therefore  $\varphi$  maps non-negative elements to non-negative elements, and so is order-preserving. Then  $\varphi|_K$  is the map we want. Note that  $\varphi(\alpha) = \beta_k$ .

To see uniqueness, let  $\tilde{\varphi} : K \rightarrow R$  be an order-preserving  $F$ -homomorphism; by existence,  $\tilde{\varphi}$  extends to an order-preserving  $K$ -homomorphism  $\tilde{\psi} : L \rightarrow R$ . Then  $\tilde{\varphi}(\alpha) = \tilde{\psi}(\alpha_k) = \beta_k = \varphi(\alpha)$ , and so  $\tilde{\varphi} = \varphi$ .  $\square$

Taking  $K = F$  above, we see that the order-embedding of a field into its real closure is unique.

**Theorem 32.** *Let  $F$  be an ordered field. Then the real closure of  $F$  is unique up to unique  $F$ -isomorphism.*

*Proof.* Let  $R_1$  and  $R_2$  be real closures of  $F$ . Applying Zorn's lemma to the set of ordered extensions intermediate between  $R_1$  and  $F$  having a unique order-preserving  $F$ -embedding into  $R_2$ , and using Lemma 31, we obtain an intermediate extension  $R_1/K/F$  with no nontrivial finite ordered extensions and a unique order-preserving  $F$ -embedding  $\varphi : K \rightarrow R_2$ . If the ordered algebraic extension  $R_2/\varphi(K)$  were nontrivial, then it would contain a nontrivial ordered finite extension, so  $\varphi$  must be surjective (and so an  $F$ -isomorphism). In particular,  $K \subseteq R_1$  is real closed; by maximality (20), in fact  $K = R_1$  and so  $\varphi$  is an  $F$ -isomorphism between  $R_1$  and  $R_2$ .  $\square$

**Corollary 33.** *A real closed field has no nontrivial field automorphisms.*

*Proof.* Let  $R$  be a real closed field. By Theorem 32,  $R$  has no nontrivial order-preserving automorphisms. Since the ordering on  $R$  is unique (by Lemma 12), every automorphism of  $R$  must be order-preserving.  $\square$

This uniqueness result is stronger than the one in the algebraically closed case: an algebraically closed field has many nontrivial automorphisms.

Uniqueness of algebraic closures allows us to classify ordered algebraic extensions.

**Lemma 34.** *Let  $F$  be an ordered field with real closure  $R$ , and let  $K/F$  be algebraic. Then field orderings on  $K$  making  $K/F$  ordered correspond to  $F$ -homomorphisms  $K \rightarrow R$  via the order obtained by restriction from  $R$ .*

*Proof.* Fix an ordering on  $K$  extending that on  $F$ , and let  $K$  have real closure  $R_K$  (exists by Lemma 28). Then  $R_K/F$  is algebraic, so  $R_K$  is a real closure of  $F$ . By Theorem 32, there is an  $F$ -isomorphism to  $R_K \cong R$ , and this induces an  $F$ -homomorphism  $K \rightarrow R$ . Restricting the order on  $R$  to  $K$  via this map recovers the original order on  $K$  by construction.

Moreover, the inverse to order restriction constructed above is unique. Indeed, an inverse  $\varphi : K \rightarrow R$  is order-preserving by definition, so it is an order-embedding from  $K$  into its real closure. By Theorem 32, such a map is unique.  $\square$

## 0.4 The Artin-Schreier Theorem

We didn't actually need to assume the ordering on  $R$  in Lemma 19.

**Lemma 35.** *Let  $F$  be a field in which  $-1$  is not a square, and suppose every element of  $F(i)$  is a square. Then sums of squares in  $F$  are squares in  $F$ .*

*Proof.* Given  $a, b \in F$ , find  $c, d \in F$  such that  $a + bi = (c + di)^2$  in  $F(i)$ . Then  $a = c^2 - d^2$  and  $b = 2cd$ , so  $a^2 + b^2 = (c^2 + d^2)^2$  is a square in  $F$ . By induction, every sum of squares in  $F$  is a square in  $F$ .  $\square$

**Lemma 36.** *Suppose  $R$  is a field whose only nontrivial algebraic extension is  $R(i)$ . Then there is a unique field ordering on  $R$ , and moreover  $R$  with this ordering is real closed.*

*Proof.* We are very nearly done by Theorem 2, Lemma 19, and Corollary 12; it remains to show that  $R$  is real.

We have  $\bar{R} \cong R(i)$ . Since  $R(i)/R$  is nontrivial,  $-1$  is not a square in  $R$ . Since every element of  $R(i)$  is a square, Lemma 35 says that  $-1$  is not a sum of squares in  $R$ .  $\square$

In fact, we can go further. The following is a weak form of the Artin-Schreier theorem. Removing the condition on characteristic is possible, but requires some more involved algebra.

**Theorem 37.** *Let  $R$  be a field with  $\text{char } R \neq 2$ , and suppose  $[\bar{R} : R] = 2$ . Then there is a unique field ordering on  $R$ , and moreover  $R$  with this ordering is real closed.*

*Proof.* By Lemma 36, it suffices to show that  $\bar{R} \cong R(i)$ .

Since  $\text{char } \bar{R} \neq 2$ , we have  $\bar{R} \cong R(\sqrt{a})$  for some non-square  $a \in R$ . Since  $R(\sqrt{a})$  is algebraically closed,  $\sqrt{a}$  is a square in  $R(\sqrt{a})$ ; find  $x, y \in R$  such that  $\sqrt{a} = (x + y\sqrt{a})^2$ . Expanding and comparing coefficients,  $x^2 + y^2a = 0$  and  $2xy = 1$ . Rearranging,  $a = -(4x^4) = -1 \cdot (2x^2)^2$ . Rescaling by  $2x^2$ ,  $R(i) \cong R(\sqrt{a}) = \bar{R}$ .  $\square$

We can weaken the hypotheses even further. Here is the full Artin-Schreier theorem.

**Theorem 38** (Artin-Schreier Theorem). *Let  $R$  be a field, and suppose  $\bar{R}$  is a finite extension of  $R$ . Then there is a unique field ordering on  $R$ , and moreover  $R$  with this ordering is real closed.*

*Proof.* TODO: this needs a lot more preliminaries eg Artin-Schreier theory, Kummer theory  $\square$

**Corollary 39.** *An algebraically closed field of nonzero characteristic has no finite-index subfields.*

*Proof.* Ordered fields have characteristic 0.  $\square$

**Theorem 40.** *The finite-index subfields of  $\bar{\mathbb{Q}}$  are isomorphic copies of  $\mathbb{Q}_{alg} = \bar{\mathbb{Q}} \cap \mathbb{R}$  indexed by  $\text{Gal}(\mathbb{Q}_{alg}/\mathbb{Q}(i))$ .*

*Proof.* Since  $\mathbb{Q}_{alg}(i) = \bar{\mathbb{Q}}$ , the field  $\mathbb{Q}_{alg}$  is a finite-index subfield.

By Theorem 38, any finite-index subfield has a unique ordering making it real closed. Let  $R$  be a real closed subfield. Then the ordering on  $R$  restricts to the ordering on  $\mathbb{Q}$  (unique by Corollary 5). Since  $R/\mathbb{Q}$  is algebraic,  $R$  is a real closure of  $\mathbb{Q}$ . By Theorem 32, there is a unique  $\mathbb{Q}$ -isomorphism  $\psi : \mathbb{Q}_{alg} \cong R$ . Since  $\mathbb{Q}_{alg}(i) = R(i) = \bar{\mathbb{Q}}$ ,  $\psi$  extends uniquely to  $\varphi \in \text{Gal}(\mathbb{Q}_{alg}/\mathbb{Q}(i))$  by mapping  $i \rightarrow i$ . The subfield  $R$  is then recovered from  $\varphi \in \text{Gal}(\mathbb{Q}_{alg}/\mathbb{Q}(i))$  by taking  $\varphi^{-1}(\mathbb{Q}_{alg})$ .  $\square$

# Bibliography

- [1] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. Springer Berlin Heidelberg, Berlin, Heidelberg, 1998.
- [2] N. Jacobson. *Basic Algebra I: Second Edition*. Dover Books on Mathematics. Dover Publications, 2012.
- [3] N. Jacobson. *Basic Algebra II: Second Edition*. Dover Books on Mathematics. Dover Publications, 2012.
- [4] Manfred Knebusch and Claus Scheiderer. *Real Algebra: A First Course*. Springer International Publishing, Cham, 2022.
- [5] Tsit Lam. An introduction to real algebra. *Rocky Mountain Journal of Mathematics - ROCKY MT J MATH*, 14, 12 1984.