Real Closed Field

Artie2000

June 19, 2025

Lemma 1. *Fix a prime p, and let M/K be a separable Galois extension of degree $p^k \cdot a$, where $p \nmid a$. Then, for $0 \le j \le k$, there are intermediate fields $K \le L_0 \le \cdots \le L_k \le M$, with $[L_j : K] = p^j \cdot a$.*

Proof. Since M/K is Galois, $|\operatorname{Gal}(M/K)| = p^k \cdot a$. A version of Sylow's first theorem says that each subgroup of order p^j with $0 \le j < k$ is contained in a subgroup of order p^{j+1}. By induction, $\operatorname{Gal}(M/K)$ has a chain of subgroups $H_k \le \cdots \le H_0 \le \operatorname{Gal}(M/K)$ with $|H_j| = p^{k-j}$. By the Galois correspondence, $L_j = M^{H_j}$ are the desired subfields. $\square$

Lemma 2. *Let K be a field with $\operatorname{char} K \neq 2$. Then there is a bijection between the quadratic extensions of K (up to K-isomorphism) and the set*

$$\left(\frac{K^*}{(K^*)^2}\right) \setminus \{1 \cdot (K^*)^2\}$$

given by the map $x(K^*)^2 \to K(\sqrt{x})$.

Proof. Consider the map $\Phi : x \to K(\sqrt{x})$ from K^*. We will show it fully respects the relation $x(K^*)^2 = y(K^*)^2$; then Φ descends to a injective map out of the quotient $K^*/(K^*)^2$. In particular, if $x \notin (K^*)^2$, then $\Phi(x) = K(\sqrt{x})$ is not K-isomorphic to K, and is therefore a quadratic extension of K.

Indeed, if $x(K^*)^2 = y(K^*)^2$, then $x = a^2 y$ for some $a \in K$, and so $K(\sqrt{x}) \cong_K K(\sqrt{y})$ via $\sqrt{x} \to a\sqrt{y}$. Conversely, if $\varphi : K(\sqrt{x}) \to K(\sqrt{y})$ is a K-isomorphism, then $\varphi(\sqrt{x}) = a + b\sqrt{y}$ for some $a, b \in K$, and so $x = a^2 + yb^2 + 2ab\sqrt{y}$. Comparing coefficients in the K-basis $\{1, \sqrt{y}\}$, either $a = 0$ or $b = 0$. Therefore, either $x = a^2 y$ and so $x(K^*)^2 = y(K^*)^2$, or $x = a^2$, in which case $K(\sqrt{y}) \cong_K K(\sqrt{x}) \cong_K K$; that is, $x, y \in (K^*)^2$.

It remains to show all quadratic extensions of K are K-isomorphic to some $L \in \operatorname{im} \Phi$. Fix a quadratic extension L/K, and let $\{1, \alpha\}$ be a K-basis for L; then $\alpha^2 = a\alpha + b$ for some $a, b \in K$. Let $\beta = 2\alpha - a$. Since $\operatorname{char} K \neq 2$, $\alpha = (\beta + a)/2$, and so $L = K + \beta K = K(\beta)$. Now, we compute $\beta^2 = a^2 + 4b$. Therefore $L \cong_K \Phi(a^2 + 4b)$ via $\beta \to \sqrt{a^2 + 4b}$. $\square$

Note that we will only use that this map is well-defined and surjective, and not that it is injective (which was the most annoying part to show).

Definition 3. A real closed field is an ordered field in which every non-negative element has a square root and every odd-degree polynomial has a root.

Let R be a real closed field. Note that, since R is ordered, $\operatorname{char} R = 0$. In particular, its algebraic extensions are separable.

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 4. *Nontrivial algebraic extensions of R have even degree.*

Proof. Let K/R be an odd-degree algebraic extension of R. By the primitive element theorem, $K = R(\alpha)$ for some $\alpha \in K$. Let f be the minimal polynomial of α over K. 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, $K = R$. $\square$

Lemma 5. *The field $R(i)$ is the unique quadratic extension of R.*

Proof. Fix $x \in R^*$. Then either $x > 0$ and $x = 1 \cdot (\sqrt{x})^2$, or $x < 0$ and $x = -1 \cdot (\sqrt{-x})^2$. Further, since $-1 \notin (R^*)^2$, $-1 \cdot (R^*)^2 \neq 1 \cdot (R^*)^2$. Therefore $R^*/(R^*)^2 = \{1 \cdot (R^*)^2, -1 \cdot (R^*)^2\}$, and we are done by Lemma 2. $\square$

Lemma 6. *There is no quadratic extension of $R(i)$.*

Proof. By Lemma 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 7. *The only algebraic extensions of R are R itself and $R(i)$.*

Proof. By separability, every algebraic 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. By Lemma 1 with $p = 2$, there is an intermediate extension of degree a. By Lemma 4, $a = 1$ (and $k > 0$). If $k > 1$, then applying Lemma 1 again yields intermediate extensions $K/L/M/R$ with $[L : M] = [M : R] = 2$. By Lemma 5, $M \cong R(i)$, contradicting Lemma 6.$_\#$ Therefore $k = 1$ and (by Lemma 5) $K \cong R(i)$. $\square$

Corollary 8. $\bar{R} = R(i)$.

The converse to Theorem 7 is much easier.

Lemma 9. *Suppose R is an ordered field whose only nontrivial algebraic extension is $R(i)$. Then R is real closed.*

Proof. Let f be an odd-degree polynomial over R; we show f has a root by induction on $\deg f$. If $\deg f = 1$, then f has a root in R since R is a field. Otherwise, $R[X]/(f)$ cannot be a field since R has no nontrivial odd-degree extensions, and so f must have a nontrivial factorisation $f = gh$. Since $\deg f = \deg g + \deg h$, wlog $\deg g$ is odd. By induction, g has a root in R, and therefore so does f.

Now let $a \in R$ be non-negative, and consider the polynomial $f = X^2 - a$. If f is irreducible, 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 f is reducible, and so a has a square root in R. $\square$

As before, let R be a real closed field. Theorem 7 is a powerful tool for deriving more of its properties.

Lemma 10. *R is maximal with respect to algebraic extensions by ordered fields.*

Proof. Since -1 has a square root in $R(i)$, the field $R(i)$ is not formally real and therefore cannot be ordered. We are done by Theorem 7. $\square$

In particular, R is maximal with respect to ordered algebraic extensions.

Lemma 11. *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 an algebraic extension of R, so it is classified by Theorem 7. 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 φ, and suppose $\varphi(X + (f)) = a + bi$ $(a, b \in R)$. Note that $b \neq 0$ since φ^{-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. $\square$

The next property is a little less obvious.

Lemma 12. *R satisfies the intermediate value property for polynomials.*

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

Fix $a, b \in R$ with $a < b$. First, suppose $f \in R[X]$ is linear. Then $f = m(X - c)$ for some $m, c \in R$ with $m \neq 0$; then $f(c) = 0$. If $m > 0$, then $f(x) < 0$ for $x < c$ and $f(x) > 0$ for $x > c$, and vice versa if $m < 0$. In either case, if $c \notin [a, b]$, then $f(a) \cdot f(b) > 0$. Taking into account the cases $c = a$ and $c = b$, if $f(a) \cdot f(b) < 0$ then $c \in (a, b)$.

Now suppose $f(a) \cdot f(b) < 0$, and proceed by induction on $\deg f$. If $\deg f = 0$, write $f = x \in R$; then $f(x) \cdot f(x) = x^2 \leq 0$, so, since squares are non-negative, $x = 0$ and $f((a+b)/2) = 0$. The above validates the property for $\deg f = 1$. Now, take a monic irreducible factor g of f; then g is classified by Lemma 11. 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 $g(a)$ and $g(b)$ have the same sign (they are nonzero since $f(a)$ and $f(b)$ are). In the second case, f has a root in (a, b); in the first and third cases, f/g satsifies the induction hypothesis, so it has a root in (a, b). In all cases, a factor of f has a root in (a, b), and therfore so does f. $\square$

In fact, the converses to Lemmas 10 and 12 both hold! The latter converse is the more obvious one.

Theorem 13. *Let R be an ordered field satisfying the intermediate value property for polynomials. Then R is real closed.*

Proof. Let f be an odd-degree polynomial over R. Write $f = a_n X^n + \cdots + a_0$. 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. By the intermediate value property, f has a root in R.

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 has a square root in R. $\square$

Theorem 14. *Let R be an ordered field maximal with respect to algebraic extensions by ordered fields. Then R is real closed.*

Proof. TODO $\square$

Corollary 15. *Let R be an ordered field maximal with respect to ordered algebraic extensions. Then R is real closed.*

We can therefore "construct" real closed fields.

Definition 16. Let F be an ordered field. A real closure of F is a real closed algebraic extension of F.

Corollary 17. *Let F be an ordered field. Then F has a real closure.*

Proof. Zorn's lemma. □

Corollary 18. *An algebraically closed field of characteristic zero has an index-2 real closed subfield.*

Proof. TODO: do this properly The prime field $\mathbb{Q}$ can be ordered, so it has a real closure R. Given a transcendental element, you can order it anywhere you like. Done by Zorn. □

Just like with the algebraic closure, it makes sense to talk of *the* real closure of an ordered field.

Lemma 19. *Let F be an ordered field. Then the real closure of F is unique up to unique F-automorphism.*

Proof. TODO (abstract nonsense?) □

We could actually have assumed much less in Lemma 9. The following is a weak form of the Artin-Schreier theorem. Its proof requires some more involved algebra.

Theorem 20. *Let R be a field, 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. TODO □

In fact, we can weaken the hypotheses even further.

Theorem 21 (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 □

Corollary 22. *An algebraically closed field of nonzero characteristic has no finite index subfields.*

Proof. Ordered fields have characteristic 0. □

Corollary 23. *$\mathbb{Q}_{alg}$ has a finite index subfield unique up to* $\mathrm{Gal}(\mathbb{Q}_a lg/\mathbb{Q})$*.*

Proof. Any finite-index subfield must be real closed. Let R be a real closed subfield of $\mathbb{Q}_{\mathrm{alg}}$. Then the order on R restricts to an order on $\mathbb{Q}$. Now, $R/\mathbb{Q}$ is algebraic, so R is a real closure of $\mathbb{Q}$. Further, the field ordering on $\mathbb{Q}$ is unique. We are done by Lemma 19. □