Notes on real-closed fields

These notes develop the algebraic background needed to understand the model theory of real-closed fields. To understand these notes, a standard graduate course in algebra is sufficient. We make references to Hungerford below for some of the facts that are used.

A field F is *formally real* iff -1 is not a sum of squares in F. A field F is *real-closed* iff F is formally real, but no proper algebraic extension is formally real. Note also that in a formally real field a sum of nonzero squares is never 0.

Theorem 1. *Every formally real field can be embedded in a real-closed field.*

Proof. Let F be formally real, and let K be the algebraic closure of F. By Zorn's lemma let H be an extension of F which is a subfield of K, maximal in the collection of all formally real subfields of K. Then H is real-closed. In fact, let L be a proper algebraic extension of H. We may assume that L is obtained from H by adjoining a root of an irreducible polynomial $f(x) \in H[x]$. Then $f(x)$ has a root in K also, and by standard field theory there is an isomorphism g from L into K pointwise fixing H. (See Hungerford, p. 236, Corollary 1.9.) Thus $g[L]$ is not formally real, and so also L is not formally real. □

Proposition 2. *If F is a real-closed field, then every sum of squares in F is a square.*

Proof. Suppose that a is a sum of squares in F, but a is not a square. Then $x^2 - a$ is irreducible over F. Let $F(\alpha)$ be obtained from F by adjoining a root of this polynomial. Then $F(\alpha)$ is no longer formally real, so we can write

$$-1 = (a_0 + b_0\alpha)^2 + \cdots + (a_{m-1} + b_{m-1}\alpha)^2$$

for certain elements $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{m-1}$ of F. Multiplying out, we obtain

$$-1 = a_0^2 + b_0^2 a + \cdots + a_{m-1}^2 + b_{m-1}^2 a + u\alpha$$

for some $u \in F$. Hence $-1 = a_0^2 + b_0^2 a + \cdots + a_{m-1}^2 + b_{m-1}^2 a$; but clearly the right side here is a sum of squares of elements of F, contradiction. □

Proposition 3. *If F is a real-closed field, then for every $a \in F$, either a or $-a$ is a square.*

Proof. Suppose that a is not a square. Then $x^2 - a$ is irreducible in $F[x]$, and so if $F(\alpha)$ is the result of adjoining a root α of it, then $F(\alpha)$ is no longer formally real. Hence by the computation in the preceding proof,

$$-1 = a_0^2 + b_0^2 a + \cdots + a_{m-1}^2 + b_{m-1}^2 a.$$

By Proposition 2 write $1 + a_0^2 + \cdots + a_{m-1}^2 = c^2$ and $b_0^2 + \cdots + b_{m-1}^2 = d^2$. Thus this equation becomes $-c^2 = d^2 a$, hence clearly $-a$ is a square. □

An *ordered field* is a field F together with a linear ordering $<$ on F such that for any $a, b, c \in F$, if $a < b$ then $a + c < b + c$, and if $a < b$ and $c > 0$ then $a \cdot c < b \cdot c$.

Proposition 4. *Suppose that F is formally real, and for every element a of F, either a or $-a$ is a square. Then every sum of squares is a square.*

Proof. Suppose that $-(a_0^2 + \cdots + a_{m-1}^2) = b^2$ with all the a_i's nonzero, $m > 0$. Then $a_0^2 + \cdots + a_{m-1}^2 + b^2 = 0$, contradiction. □

Proposition 5. *Suppose that F is formally real and for any $a \in F$, either a is a square or $-a$ is a square. Then there is a linear order $<$ on F which makes F into an ordered field.*

Proof. Define $a < b$ iff $a \neq b$ and $b - a$ is a square. This gives an ordered field:

(1) Clearly $a \not< a$.

(2) If $a < b < c$, then $b - a$ and $c - b$ are squares, hence $c - a$ is a sum of squares, and so is a square by Proposition 4. We must have $c \neq a$, as otherwise 0 would be the sum of the nonzero squares $b - a$ and $c - b$.

(3) Given $a, b \in F$, either $a - b$ or $b - a$ is a square, and so $a < b$, $a = b$, or $b < a$.

(4) If $a < b$, obviously also $a + c < b + c$.

(5) Suppose that $a < b$ and $c > 0$. Thus $b - a$ and c are squares, and hence so is $b \cdot c - a \cdot c$, so $a \cdot c < b \cdot c$. □

So we have shown that any real-closed field can be extended to an ordered field. Clearly any ordered field is of characteristic 0, so any real-closed field has characteristic 0. Also, any formally real field can be extended to an ordered field, and hence also has characteristic 0.

Proposition 6. *If F is formally real, $f(x)$ is a monic irreducible polynomial of odd degree > 1, and $F(\alpha)$ is obtained from F by adjoining a root α of $f(x)$, then $F(\alpha)$ is formally real.*

Proof. Suppose not, and let $f(x)$ be irreducible of minimum odd degree such that $F(\alpha)$ is not formally real, with α a root of $f(x)$ in some extension. Say that $f(x)$ has degree $2n + 1$, with $n > 0$. We use the specific construction of $F(\alpha)$ as $F[x]/(f(x))$. Now -1 is a sum of squares in $F(\alpha)$, and this implies that in $F[x]$ we have polynomials such that

$$(*) \qquad 1 + (g_0(x))^2 + \cdots + (g_{m-1}(x))^2 = f(x)h(x),$$

Here each $g_i(x)$ has degree at most $2n$. Let u be the greatest degree of any of the polynomials $g_i(x)$. For each i such that u is the degree of $g_i(x)$ write $g_i(x) = a_i x^u + h_i(x)$ with $a_i \neq 0$ and $h_i(x)$ of degree less than u. Then the leading term of the left side of $(*)$ is $(\sum\{a_i^2\})x^{2u}$, the sum being taken over all i with $g_i(x)$ of degree u. The coefficient $\sum\{a_i^2\}$ is nonzero since F is formally real. It follows that the left side of $(*)$ has degree $2u \leq 4n$. Hence $h(x)$ has odd degree at most $2n - 1$. By the minimality of n, if β is a root of some irreducible factor of $h(x)$ of odd degree, then $F(\beta)$ is formally real. Substituting β into $(*)$, we see that 0 is a sum of nonzero squares in $F(\beta)$, contradiction. □

Corollary 7. *In a real-closed field, every polynomial of odd degree has a root.* □

Now we go through some material which is a reorganization of the proof of the fundamental theorem of algebra found on pages 265–267 of Hungerford. Let us call a field F *special* iff it is formally real, every polynomial of odd degree has a root, and for every $a \in F$, either a is a square or $-a$ is a square. Thus every real-closed field is special. This is a temporary notation, since we are going to show that conversely every special field is real-closed. Note that every special field can be expanded to an ordered field, by Proposition 5.

Lemma 7. *Let K be special field, and i a root of x^2+1 in an extension of K. Then every element of $K(i)$ has a square root.*

Proof. Let $a+bi$ be any element of $K(i)$, where $a, b \in K$. Then $a^2 \leq a^2+b^2$, so $|a| \leq \sqrt{a^2+b^2}$. It follows that $a+\sqrt{a^2+b^2} \geq 0$, so we can choose $c \geq 0$ so that $a+\sqrt{a^2+b^2} = 2c^2$. Similarly we get $d \geq 0$ such that $-a+\sqrt{a^2+b^2} = 2d^2$. Then

$$c^2 - d^2 = \frac{a+\sqrt{a^2+b^2}}{2} - \frac{-a+\sqrt{a^2+b^2}}{2} = a$$

and

$$2cd = \left(\sqrt{a+\sqrt{a^2+b^2}}\right)\left(\sqrt{-a+\sqrt{a^2+b^2}}\right) = \sqrt{-a^2+a^2+b^2} = |b|.$$

Thus if $b \geq 0$ we have $(c+di)^2 = a+bi$, and if $b<0$ we have $(c-di)^2 = a+bi$. □

Lemma 8. *Let K be a special field, and i a root of x^2+1 in an extension of K. Then every quadratic polynomial in $K(i)[x]$ has a root.*

Proof. Let x^2+sx+t be any monic quadratic in $K(i)[x]$. Thus $x^2+sx+t = (x+\frac{s}{2})^2 + t - \frac{s^2}{4}$. Let $u \in K(i)$ be such that $u^2 = \frac{s^2}{4} - t$. Clearly $u - \frac{s}{2}$ is a root of x^2+sx+t. □

Lemma 9. *Let K be a special field, and i a root of x^2+1 in an extension of K. Then $K(i)$ is algebraically closed.*

Proof. Suppose that L is a finite dimensional extension of $K(i)$. We may assume that L is the splitting field of a set of polynomials in $K[x]$, and hence is Galois over K. It suffices to show that $L = K(i)$. Let $[L:K] = m$. Thus $m \geq 2$. Write $m = 2^n r$ with r odd. Let G be a Sylow 2-subgroup of $\mathrm{Aut}_K L$. Then the fixed field E of G over K is such that $[E:K] = [\mathrm{Aut}_K L : G]$ by the fundamental theorem of Galois theory (Theorem 2.5, page 245, in Hungerford). That degree is thus odd. By Lemma 3.17, page 266, in Hungerford, there is thus an irreducible polynomial of odd degree over K. Since K is special, it follows that this degree is 1.

Thus $r = 1$ and $m = 2^n$. Hence $\mathrm{Aut}_{K(i)} L = 2^{n-1}$. Suppose that $n > 1$. By one of the Sylow theorems, $\mathrm{Aut}_{K(i)} L$ has a subgroup H of index 2. Let F be the fixed field of H. Then $[F : K(i)] = [\mathrm{Aut}_{K(i)} L : H] = 2$. This contradicts Lemma 8. □

Lemma 10. *If K is special, then K is real-closed.*

Proof. Suppose that L is a proper algebraic extension of K. By Lemma 9 we may assume that it is a subfield of $K(i)$; hence it equals $K(i)$, and is not formally real. □

Theorem 11. *K is real-closed iff it is special.*

Corollary 12. *Let $(K, <)$ be an ordered field. Then it is real-closed iff every positive element has a square root and every polynomial over K of odd degree has a root in K.*

Proof. $\Rightarrow$: By Theorem 11 and Proposition 5. $\Leftarrow$: by Theorem 11. □

Proposition 13. *If K is a real-closed field, then every polynomial over K splits into linear and quadratic factors.*

Proof. If $f(x)$ is an irreducible polynomial in $K[x]$, then if α is a root of it in $K(i)$, we have $2 = [K(i) : K] = [K(i) : K(\alpha)] \cdot [K(\alpha) : K]$, and so $[K(\alpha) : K]$ is 1 or 2. □

Proposition 14. *Suppose that K is a real-closed field and $f(x)$ is an irreducible quadratic polynomial in $K[x]$. Then either $f(a) > 0$ for all $a \in K$, or $f(a) < 0$ for all $a \in K$.*

Proof. Write $f(x) = bx^2 + cx + d$. Actually for this proposition clearly we may assume that $b = 1$. Now $f(x) = (x + \frac{c}{2})^2 + d - \frac{c^2}{4}$. Since $f(x)$ is irreducible and every positive element of K has a square root, we must have $d - \frac{c^2}{4} > 0$. Hence the desired conclusion is clear. □

Proposition 15. *Suppose that K is a real-closed field, and $f(x) \in K[x]$. Suppose that $a < b$ in K and $f(a) \cdot f(b) < 0$. Then there is a c with $a < c < b$ such that $f(c) = 0$.*

Proof. Write $f(x) = g_0(x) \cdot \ldots \cdot g_{m-1}(x)$ with each $g_i(x)$ irreducible, and hence by Proposition 13, either linear or quadratic. From Proposition 14 it follows that some linear factor $ux + v$ must have different signs at a and at b. By symmetry say that $ua+v < 0 < ub+v$. Thus $ua < -v < ub$, hence $u > 0$ and $a < \frac{-v}{u} < b$ and $f(\frac{-v}{u}) = 0$. □

Proposition 16. *Suppose that K is a real-closed field and F is a subfield of K. Then there is a smallest real-closed field H such that $F \subseteq H \subseteq K$. Moreover, if K' is any real-closed field such that $F \subseteq K'$, then H is embeddable in K' by an embedding whcih is the identity on F.*

Proof. Let $\langle f_\alpha(x) : \alpha < \kappa \rangle$ list out all irreducible polynomials in $F[x]$ of odd degree plus all irreducible polynomials $x^2 - a$ with a a sum of squares of F. Now form a sequence of extensions G_α of F, each a subfield of K, adjoining a root in K of each of these polynomials if they have remained irreducible. Call the union of all fields obtained in this way L_1. Then repeat this process with L_1, forming L_2, L_3, etc. The union of all these is the desired real-closed field H.

Given K' as in the second part of the Proposition, the identity on F can be extended to embeddings of the G_α's and the L_m's one after the other by standard field theory. □

Finally, we need to go into the question of what structures can be isomorphically embedded into real-closed ordered fields. The answer is: ordered integral domains. We prove a strong version of this. Generalizing the notion of ordered field as defined on page one, we say that an ordered integral domain is a pair $(D, <)$ such that D is an integral domain and $<$ is a linear ordering of D such that for any $a, b, c \in D$, if $a < b$ then $a + c < b + c$, and if $a < b$ and $c > 0$ then $a \cdot c < b \cdot c$.

Proposition 17. *If $(D, <)$ is a substructure of an ordered field, then $(D, <)$ is an ordered integral domain.* □

Proposition 18. *Suppose that D is an integral domain, and P is a set of nonzero elements of D closed under $+$ and $\cdot$, and such that for any nonzero $a \in D$, $a \in P$ or $-a \in P$. Then there is a relation $<$ such that $(D, <)$ is an ordered integral domain and $P = \{a \in D : 0 < a\}$.*

Proof. Define $a < b$ iff $b - a \in P$. Since $0 \notin P$, it follows that $<$ is irreflexive. Suppose that $a < b < c$. Then $b - a \in P$ and $c - b \in P$, so $c - a = c - b + b - a \in P$; so $a < c$. Finally, given distinct elements $a, b \in D$, we have $a - b \in P$ or $b - a \in P$, hence $a < b$ or $b < a$. So $<$ is a linear ordering of D.

Suppose that $a < b$ and $c \in D$. Then $b + c - (a + c) = b - a \in P$, so $a + c < b + c$.

Suppose that $a < b$ and $0 < c$. Then $b - a, c \in P$, so $b \cdot c - a \cdot c = (b - a) \cdot c \in P$, so $a \cdot c < b \cdot c$.

Thus $(D, <)$ is an ordered integral domain. Clearly $P = \{a \in D : 0 < a\}$. □

Lemma 19. *Suppose that $(F, <)$ is an ordered field, G is an extension field of F, $m \in \omega$, $a_0, \ldots, a_{m-1}$ are positive elements of F, and*

$$F \subset F(\sqrt{a_0}) \subset F(\sqrt{a_0}, \sqrt{a_1}) \subset \ldots \subset F(\sqrt{a_0}, \sqrt{a_1}, \ldots, \sqrt{a_{m-1}}) = G.$$

Note that all inclusions here are proper.

Under these conditions, G is formally real.

Proof. As is well-known, any element of G can be written in the form

$$\sum_{M \subseteq m} b_M \cdot \sqrt{\prod_{i \in M} a_i}$$

with each b_M in F. The square of such an element has the form

$$\sum_{M \subseteq m} b_M^2 \cdot \prod_{i \in M} a_i + \sum_{\emptyset \neq M \subseteq M} c_M \cdot \sqrt{\prod_{i \in M} a_i}$$

where each $c_M \in F$. It follows that if -1 is a sum of squares in G, then -1 is a sum of elements of the form

$$\sum_{M \subseteq m} b_M^2 \cdot \prod_{i \in M} a_i.$$

Note, however, that each such element is positive, contradiction. □

Lemma 20. *Let $(F, <)$ be an ordered field, and let P be the set of all positive elements of F. Let $\prec$ be any well-order of P. We now define an increasing sequence of extensions G_ξ of F by recursion for $\xi < \alpha$, where α will also be determined in the construction. Let $G_0 = F$. Suppose that G_η has been constructed for all $\eta < \xi$, with $\xi \geq 1$. Let $H_\xi = \bigcup_{\eta < \xi} G_\eta$. If each member of P has a square root in H_ξ, we let $\alpha = \xi$ and the*

construction stops. Otherwise we let a_ξ be the $\prec$-first element of P not having a square root in H_ξ, and define $G_\xi = H(\sqrt{a_\xi})$. This finishes the construction.

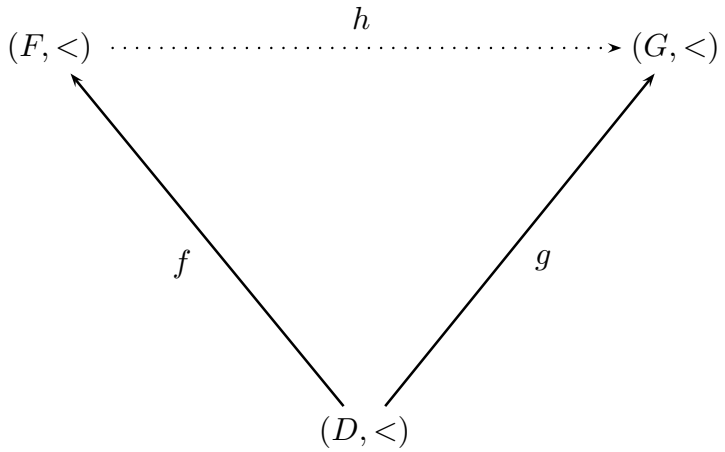
The conclusion is that H_α is formally real and every positive element of F has a square root in H_α.

Proof. If -1 is a sum of squares in H_α, then there is a finite subset N of α such that -1 is a sum of squares in $F(\langle a_\xi : \xi \in N\rangle)$. This contradicts Lemma 19.

The other part of the conclusion is assured by the construction. □

Theorem 21. *Suppose that $(D, <)$ is an ordered integral domain. Then there is a real-closed ordered field $(F, <)$ and a function f such that f is an isomorphism from $(D, <)$ into $(F, <)$, and for any real-closed ordered field $(G, <)$ and isomorphism g from $(D, <)$ into $(G, <)$, there is an isomorphism h of $(F, <)$ into $(G, <)$ such that $h \circ f = g$.*

This is illustrated by the following diagram:



Proof. We recall the standard embedding of an integral domain D into a field H. A relation $\sim$ is defined on $D \times (D\backslash\{0\})$ by setting $(a, b) \sim (c, d)$ iff $ad = bc$. This is an equivalence relation on $D \times (D\backslash\{0\})$, and H is the collection of equivalence classes. There are operations $+$ and $\cdot$ on H such that $[(a, b)] + [(c, d)] = [ad + bc, bd]$ and $[(a, b)] \cdot [(c, d)] = [(ac, bd)]$. This makes H into a field. The function f taking a to $[(a, 1)]$ for each $a \in D$ is an isomorphism from D into H.

Now we define $P = \{[(a, b)] \in H : ab > 0\}$.

(1) If $[(c, d)] = [(a, b)]$ and $ab > 0$, then $cd > 0$.

In fact, $cb = da$; multiplying by bd, we get $cdb^2 = abd^2$. Since $ab > 0$ and $d^2 > 0$, it follows that $cdb^2 > 0$. So $cd > 0$ as otherwise, multiplying by b^2 would give $cdb^2 \leq 0$. Thus (1) holds.

If $ab > 0$ and $cd > 0$, then $abcd > 0$. Hence P is closed under $\cdot$.

If $ab > 0$ and $cd > 0$, then $(ad + bc)(bd) = abd^2 + cdb^2 > 0$. Hence P is closed under $+$.

Given $[(a, b)] \neq [(0, 1)]$, we have $a \neq 0$. Hence $ab > 0$ or $-ab > 0$. So for any non-zero element x of H we have $x \in P$ or $-x \in P$.

Let $<$ on H be defined from P as in Proposition 17.

From all of this it follows that f is an isomorphism from $(D, <)$ into $(H, <)$. Next we apply the construction in Lemma 19 to get a formally real extension K of H such that every positive element of H has a square root in K. By Theorem 1 let L be a real-closed extension of K; by Theorem 15 let M be the smallest real-closed field such that $K \subseteq M \subseteq L$. By Propositions 3 and 5 there is a relation $<$ making M an ordered field. The construction in Proposition 5 assures that every nonzero element of M which is a square is positive in the order $<$. Our construction shows that every positive element of H is a square in K and hence in M. It follows that $(H, <)$ is a substructure of $(M, <)$.

Now suppose that N is a real-closed ordered field and g is an isomorphism from $(D, <)$ into N. We would like to define $h : H \to N$ by setting $h([(a, b)]) = g(a) \cdot g(b)^{-1}$ for any $[a, b] \in H$. To show that h is well-defined, suppose that $[(a, b)] = [(c, d)]$. Thus $ad = bc$, so $g(a)g(d) = g(b)g(c)$ and hence

$$g(a) \cdot g(b)^{-1} = g(a)g(d)g(d)^{-1}g(b)^{-1} = g(b)g(c)g(d)^{-1}g(b)^{-1} = g(c)g(d)^{-1}.$$

Hence h is well-defined. Similarly h is one-one. It is straighforward to check that h really is an isomorphism from H into N.

By standard uniqueness facts in field theory, h extends to an isomorphism k from M into N. Now $a \in M$ is nonnegative in M iff it is a square in M iff $k(a)$ is a square in N iff $k(a)$ is nonnegative in N. So k is in fact an isomorphism from M into N. Clearly $k \circ f = g$. □