A Real Algebra

We prove some of the algebraic facts needed in Section 7. All of these results are due to Artin and Schreier. See Lang's *Algebra* §XI for more details.

All fields are assumed to be of characteristic 0.

Definition A.1 A field K is *real* if -1 can not be expressed as a sum of squares of elements of K. In general, we let $\sum K^2$ be the sums of squares from K.

If F is orderable, then F is real because squares are nonnegative with respect to any ordering.

Lemma A.2 *Suppose that F is real and $a \in F \setminus \{0\}$. Then, at most one of a and $-a$ is a sum of squares.*

Proof If a and b are both sums of squares, then $\frac{a}{b} = \frac{a}{b^2}b$ is a sum of squares. Thus, if F is real, at least one of a and $-a$ is not in $\sum F^2$.

Lemma A.3 *If F is real and $-a \in F \setminus \sum F^2$, then $F(\sqrt{a})$ is real. Thus, if F is real and $a \in F$, then $F(\sqrt{a})$ is real or $F(\sqrt{-a})$ is real.*

Proof We may assume that $\sqrt{a} \notin F$. If $F(\sqrt{a})$ is not real, then there are $b_i, c_i \in F$ such that

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum (b_i^2 + 2c_ib_i\sqrt{a} + c_i^2 a).$$

Because $\sqrt{a}$ and 1 are a vector space basis for $F(\sqrt{a})$ over F,

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Thus

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2} = \frac{\left(\sum b_i^2\right)\left(\sum c_i^2\right) + \left(\sum c_i^2\right)}{\left(\sum c_i^2\right)^2}$$

and $-a \in \sum F^2$, a contradiction.

Lemma A.4 *If F is real, $f(X) \in F[X]$ is irreducible of odd degree n, and $f(\alpha) = 0$, then $F(\alpha)$ is real.*

Proof We proceed by induction on n. If $n = 1$, this is clear. Suppose, for purposes of contradiction, that $n > 1$ is odd, $f(X) \in F[X]$ is irreducible of degree n, $f(\alpha) = 0$, and $F(\alpha)$ is not real. There are polynomials g_i of degree at most $n-1$ such that $-1 = \sum g_i(\alpha)^2$. Because F is real, some g_i is nonconstant. Because $F(\alpha) \cong F[X]/(f)$, there is a polynomial $q(X) \in F[X]$ such that

$$1 = \sum g_i^2(X) + q(X)f(X).$$

The polynomial $\sum g_i^2(X)$ has a positive even degree at most $2n-2$. Thus, q has odd degree at most $n-2$. Let β be the root of an irreducible factor of q. By induction, $F(\beta)$ is real, but $-1 = \sum g_i^2(\beta)$, a contradiction.

Definition A.5 We say that a field R is *real closed* if and only if R is real and has no proper real algebraic extensions.

If R is real closed and $a \in R$, then, by Lemmas A.2 and A.3, either $a \in R^2$ or $-a \in R^2$. Thus, we can define an order on R by

$$a \geq 0 \Leftrightarrow a \in R^2.$$

Moreover, this is the only way to define an order on R because the squares must be nonnegative. Also, if R is real closed, every polynomial of odd degree has a root in R.

Lemma A.6 *Let F be a real field. There is $R \supseteq F$ a real closed algebraic extension. We call R a* real closure *of F.*

Proof Let $I = \{K \supseteq F : K \text{ real}, K/F \text{ algebraic}\}$. The union of any chain of real fields is real; thus, by Zorn's Lemma, there is a maximal $R \in I$. Clearly, R has no proper real algebraic extensions; thus, R is real closed.

Corollary A.7 *If F is any real field, then F is orderable. Indeed, if $a \in F$ and $-a \notin \sum F^2$, then there is an ordering of F, where $a > 0$.*

Proof By Lemma A.3, $F(\sqrt{a})$ is real. Let R be a real closure of F. We order F by restricting the ordering of R because a is a square in R, $a > 0$.

The following theorem is a version of the Fundamental Theorem of Algebra.

Theorem A.8 *Let R be a real field such that*
i) for all $a \in R$, either $\sqrt{a}$ or $\sqrt{-a} \in R$ and
ii) if $f(X) \in R[X]$ has odd degree, then f has a root in R.
If $i = \sqrt{-1}$, then $K = R(i)$ is algebraically closed.

Proof

Claim 1 Every element of K has a square root in K.

Let $a + bi \in K$. Note that $\frac{a+\sqrt{a^2+b^2}}{2}$ is nonnegative for any ordering of R. Thus, by i), there is $c \in R$ with

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

If $d = \frac{b}{2c}$, then $(c+di)^2 = a + bi$.

Let $L \supseteq K$ be a finite Galois extension of R. We must show that $L = K$. Let $G = Gal(L/R)$ be the Galois group of L/R. Let H be the 2-Sylow subgroup of G.

Claim 2 $G = H$.

Let F be the fixed field of H. Then F/R must have odd degree. If $F = R(x)$, then the minimal polynomial of x over R has odd degree, but the only irreducible polynomials of odd degree are linear. Thus, $F = R$ and $G = H$.

Let $G_1 = Gal(L/K)$. If G_1 is nontrivial, then there is G_2 a subgroup of G_1 of index 2. Let F be the fixed field of G_2. Then, F/K has degree 2. But by Claim 1, K has no extensions of degree 2. Thus, G_1 is trivial and $L = K$.

Corollary A.9 *Suppose that R is real. Then R is real closed if and only if $R(i)$ is algebraically closed.*

Proof

($\Rightarrow$) By Theorem A.8.

($\Leftarrow$) $R(i)$ is the only algebraic extension of R, and it is not real.

Let $(R, <)$ be an ordered field. We say that R has the *intermediate value property* if for any polynomial $p(X) \in R[X]$ if $a < b$ and $p(a) < 0 < p(b)$, then there is $c \in (a, b)$ with $p(c) = 0$.

Lemma A.10 *If $(R, <)$ is an ordered field with the intermediate value property, then R is real closed.*

Proof Let $a > 0$ and let $p(X) = X^2 - a$. Then $p(0) < 0$, and $p(1 + a) > 0$; thus, there is $c \in R$ with $c^2 = a$.

Let

$$f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$$

where n is odd. For M large enough, $f(M) > 0$ and $f(-M) < 0$; thus, there is a c such that $f(c) = 0$.

By Theorem A.8, $R(i)$ is algebraically closed. Because R is real, it must be real closed.

Lemma A.11 *Suppose that R is real closed and $<$ is the unique ordering, then $(R, <)$ has the intermediate value property.*

Proof Suppose $f(X) \in R[X]$, $a < b$, and $f(a) < 0 < f(b)$. We may assume that $f(X)$ is irreducible (for some factor of f must change signs). Because $R(i)$ is algebraically closed, either $f(X)$ is linear, and hence has a root in (a, b), or

$$f(X) = X^2 + cX + d,$$

where $c^2 - 4d < 0$. But then

$$f(X) = \left(X + \frac{c}{2}\right)^2 + \left(d - \frac{c^2}{4}\right)$$

and $f(x) > 0$ for all x.

We summarize as follows.

Theorem A.12 *The following are equivalent.*

i) R is real closed.

ii) For all $a \in R$, either a or $-a$ has a square root in R and every polynomial of odd degree has a root in R.

iii) We can order R by $a \geq 0$ if and only if a is a square and, with respect to this ordering, R has the intermediate value property.

Finally, we consider the question of uniqueness of real closures. We first note that there are some subtleties. For example, there are nonisomorphic real closures of $F = \mathbf{Q}(\sqrt{2})$. The field of real algebraic numbers is one real closure of F. Because $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ is an automorphism of F, $\sqrt{2}$ is not in $\sum F^2$. Thus, by Corollary B.5, $F(\sqrt{-2})$ is real. Let R be a real closure of F containing $F(\sqrt{-2})$. Then, R is not isomorphic to the real algebraic numbers over F.

This is an example of a more general phenomenon. It is proved by successive applications of Lemmas A.2 and A.3.

Lemma A.13 *If $(F,<)$ is an ordered field, then there is a real closure of F in which every positive element of F is a square.*

Because $\mathbb{Q}(\sqrt{2})$ has two distinct orderings, it has two nonisomorphic real closures. The field $\mathbb{Q}(t)$ of rational functions over $\mathbb{Q}$ has $2^{\aleph_0}$ orderings and hence $2^{\aleph_0}$ nonisomorphic real closures.

The next theorem shows that once we fix an ordering of F, there is a unique real closure that induces the ordering.

Theorem A.14 *Let $(F,<)$ be an ordered field. Let R_0 and R_1 be real closures of F such that $(R_i,<)$ is an ordered field extension of $(F,<)$. Then, R_0 is isomorphic to R_1 over F and the isomorphism is unique.*

The proof of Theorem A.14 uses Sturm's algorithm.

Definition A.15 Let R be a real closed field. A *Sturm sequence* is a finite sequence of polynomials $f_0,\ldots,f_n$ such that:

i) $f_1 = f_0'$;

ii) for all x and $0 \leq i \leq n-1$, it is not the case that $f_i(x) = f_{i+1}(x) = 0$;

iii) for all x and $1 \leq i \leq n-1$, if $f_i(x) = 0$, then $f_{i-1}(x)$ and $f_{i+1}(x)$ have opposite signs;

iv) f_n is a nonzero constant.

If $f_0,\ldots,f_n$ is a Sturm sequence and $x \in \mathbb{R}$, define $v(x)$ to be the number of sign changes in the sequence $f_0(x),\ldots,f_n(x)$.

Suppose that $f \in R[X]$ is nonconstant and does not have multiple roots. We define a Sturm sequence as follows:

$f_0 = f$;

$f_1 = f'$.

Given f_i nonconstant, use the Euclidean algorithm to write

$$f_i = g_i f_{i-1} - f_{i+1}$$

where the degree of f_{i+1} is less than the degree of f_{i-1}. We eventually reach a constant function f_n.

Lemma A.16 *If f has no multiple roots, then $f_0, \ldots, f_n$ is a Sturm sequence.*

Proof

iv) If $f_n = 0$, then $f_{n-1}|f_i$ for all i. But f has no multiple roots; thus f and f' have no common factors, a contradiction.

ii) If $f_i(x) = f_{i+1}(x) = 0$, then by induction $f_n(x) = 0$, contradicting iv).

iii) If $1 \leq i \leq n-1$ and $f_i(x) = 0$, then $f_{i-1}(x) = -f_{i+1}(x)$. Thus, $f_{i-1}(x)$ and $f_{i+1}(x)$ have opposite signs.

Theorem A.17 (Sturm's Algorithm) *Suppose that R is a real closed field, $a, b \in R$, and $a < b$. Let f be a polynomial without multiple roots. Let $f = f_0, \ldots, f_n$ be a Sturm sequence such that $f_i(a) \neq 0$ and $f_i(b) \neq 0$ for all i. Then, the number of roots of f in (a, b) is equal to $v(a) - v(b)$.*

Proof Let $z_1 < \ldots < z_m$ be all the roots of the polynomials $f_0, \ldots, f_n$ that are in the interval (a, b). Choose $c_1, \ldots, c_{m-1}$ with $z_i < c_i < z_{i+1}$. Let $a = c_0$ and $b = c_m$. For $0 \leq i \leq m-1$, let r_i be the number of roots of f in the interval (c_i, c_{i+1}). Clearly, $\sum r_i$ is the number of roots of f in the interval (a, b). On the other hand,

$$v(a) - v(b) = \sum_{i=0}^{m-1} (v(c_i) - v(c_{i+1})).$$

Thus, it suffices to show that if $c < z < d$ and z is the only root of any f_i in (c, d), then

$$v(d) = \begin{cases} v(c) - 1 & z \text{ is a root of } f \\ v(c) & \text{otherwise} \end{cases}.$$

If $f_i(b)$ and $f_i(c)$ have different signs, then $f_i(z) = 0$. We need only see what happens at those places.

If z is a root of f_i, $i > 0$, then $f_{i+1}(z)$ and $f_{i-1}(z)$ have opposite signs and f_{i+1} and f_{i-1} do not change signs on $[c, d]$. Thus, the sequences $f_{i-1}(c), f_i(c), f_{i+1}(c)$ and $f_{i-1}(d), f_i(d), f_{i+1}(d)$ each have one sign change. For example, if $f_{i-1}(z) > 0$ and $f_{i-1}(z) < 0$, then these sequences are either $+, +, -$ or $+, -, +$, and in either case both sequences have one sign change.

If z is a root of f_0, then, because $f'(z) \neq 0$, f is monotonic on (c, d). If f is increasing on (c, d), the sequence at c starts $-, +, \ldots$ and the sequence at d starts $+, +, \ldots$. Similarly, if f is decreasing, the sequence at c starts $+, -, \ldots$, and the sequence at b starts $-, -, \ldots$. In either case, the sequence at c has one more sign change than the sequence at d. Thus, $v(c) - v(d) = 1$, as desired.

Corollary A.18 *Suppose that $(F, <)$ is an ordered field. Let f be a nonconstant irreducible polynomial over F. If R_0 and R_1 are real closures of F compatible with the ordering, then f has the same number of roots in both R_0 and R_1.*

Proof Let $f_0, \ldots, f_n$ be the Sturm sequence from Lemma A.16. Note that each $f_i \in F[X]$. We can find $M \in F$ such that any root of f_i is in $(-M, M)$ (if $g(X) = X^n + \sum a_i X^i$, then any root of g has absolute value at most $1 + \sum |a_i|$, for example). Then, the number of roots of f in R_i is equal to $v(-M) - v(M)$, but $v(M)$ depends only on F.

Lemma A.19 *Suppose $(F, <)$ is an ordered field and R_0 and R_1 are real closures of F such that $(R_i, <)$ is an ordered field extension of $(F, <)$. If $\alpha \in R_0 \setminus F$, there is an ordered field embedding of $F(\alpha)$ into R_1 fixing F.*

Proof Let $f \in F[X]$ be the minimal polynomial of α over F. Let $\alpha_1 < \ldots < \alpha_n$ be all zeros of f in R_0. By Corollary B.18, f has exactly n zeros $\beta_1 < \ldots < \beta_n \in R_1$. Let

$$\sigma : F(\alpha_1, \ldots, \alpha_n) \to F(\beta_1, \ldots, \beta_n)$$

be the map obtained by sending α_i to β_i. We claim that σ is an ordered field isomorphism.

For $i = 1, \ldots, n-1$, let $\gamma_i = \sqrt{\alpha_{i+1} - \alpha_i} \in R_0$. By the Primitive Element Theorem, there is $a \in F$ such that

$$F(a) = F(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1}).$$

Let $g \in F[X]$ be the minimal polynomial of a over F. By Corollary B.18, g has a zero $b \in R_1$ and there is a field isomorphism $\phi : F(a) \to F(b)$. Because $F(a)$ contains n zeros of F, so does $F(b)$. Thus $\beta_1, \ldots, \beta_n \in F(b)$ and for each i there is a j such that $\phi(\alpha_i) = \beta_j$. But

$$\phi(\gamma_i)^2 = \phi(\alpha_{i+1}) - \phi(\alpha_i).$$

Thus $\phi(\alpha_i) = \beta_i$ for $i = 1, \ldots, n$. We still must show that σ is order preserving. Suppose $c \in F(\alpha_1, \ldots, \alpha_n)$ and $c > 0$. There is $d \in R_0$ such that $d^2 = c$. Arguing as above, we can find a field embedding

$$\psi : F(\alpha_1, \ldots, \alpha_n, d) \subseteq R_1$$

fixing F. As above, $\psi(\alpha_i) = \beta_i$ and $\psi \supseteq \sigma$. Because

$$\psi(d)^2 = \psi(c) = \sigma(c),$$

we have $\sigma(c) > 0$. Thus σ is order preserving.

Proof of Theorem A.14 Let $\mathcal{P}$ be the set of all order preserving $\sigma : K \to R_1$ where $F \subseteq K \to R_0$ and $\sigma | F$ is the identity. By Zorn's Lemma, there is a maximal $\sigma : K \to R_1$ in $\mathcal{P}$. By identifying K and $\sigma(K)$ and applying the previous lemma, we see that $K = R_0$. A similar argument shows that $\sigma(K) = R_1$.

Uniqueness follows because the ith root of $f(X)$ in R_0 must be sent to the ith root of $f(X)$ in R_1.