CHAPTER XI

Real Fields

§1. ORDERED FIELDS

Let K be a field. An **ordering** of K is a subset P of K having the following properties:

ORD 1. Given $x \in K$, we have either $x \in P$, or $x = 0$, or $-x \in P$, and these three possibilities are mutually exclusive. In other words, K is the disjoint union of P, $\{0\}$, and $-P$.

ORD 2. If $x, y \in P$, then $x + y$ and $xy \in P$.

We shall also say that K is **ordered by** P, and we call P the set of **positive elements**.

Let us assume that K is ordered by P. Since $1 \neq 0$ and $1 = 1^2 = (-1)^2$ we see that $1 \in P$. By **ORD 2**, it follows that $1 + \cdots + 1 \in P$, whence K has characteristic 0. If $x \in P$, and $x \neq 0$, then $xx^{-1} = 1 \in P$ implies that $x^{-1} \in P$.

Let $x, y \in K$. We define $x < y$ (or $y > x$) to mean that $y - x \in P$. If $x < 0$ we say that x is **negative**. This means that $-x$ is positive. One verifies trivially the usual relations for inequalities, for instance:

$$x < y \quad \text{and} \quad y < z \qquad \text{implies} \qquad x < z,$$

$$x < y \quad \text{and} \quad z > 0 \qquad \text{implies} \qquad xz < yz,$$

$$x < y \quad \text{and} \quad x, y > 0 \qquad \text{implies} \qquad \frac{1}{y} < \frac{1}{x}.$$

We define $x \leqq y$ to mean $x < y$ or $x = y$. Then $x \leqq y$ and $y \leqq x$ imply $x = y$.

If K is ordered and $x \in K$, $x \neq 0$, then x^2 is positive because $x^2 = (-x)^2$ and either $x \in P$ or $-x \in P$. Thus a sum of squares is positive, or 0.

Let E be a field. Then a product of sums of squares in E is a sum of squares. If $a, b \in E$ are sums of squares and $b \neq 0$ then a/b is a sum of squares.

The first assertion is obvious, and the second also, from the expression $a/b = ab(b^{-1})^2$.

If E has characteristic $\neq 2$, and -1 is a sum of squares in E, then every element $a \in E$ is a sum of squares, because $4a = (1 + a)^2 - (1 - a)^2$.

If K is a field with an ordering P, and F is a subfield, then obviously, $P \cap F$ defines an ordering of F, which is called the **induced** ordering.

We observe that our two axioms **ORD 1** and **ORD 2** apply to a ring. If A is an ordered ring, with $1 \neq 0$, then clearly A cannot have divisors of 0, and one can extend the ordering of A to the quotient field in the obvious way: A faction is called positive if it can be written in the form a/b with $a, b \in A$ and $a, b > 0$. One verifies trivially that this defines an ordering on the quotient field.

Example. We define an ordering on the polynomial ring $\mathbf{R}[t]$ over the real numbers. A polynomial

$$f(t) = a_n t^n + \cdots + a_0$$

with $a_n \neq 0$ is defined to be positive if $a_n > 0$. The two axioms are then trivially verified. We note that $t > a$ for all $a \in \mathbf{R}$. Thus t is infinitely large with respect to $\mathbf{R}$. The existence of infinitely large (or infinitely small) elements in an ordered field is the main aspect in which such a field differs from a subfield of the real numbers.

We shall now make some comment on this behavior, i.e. the existence of infinitely large elements.

Let K be an ordered field and let F be a subfield with the induced ordering. As usual, we put $|x| = x$ if $x > 0$ and $|x| = -x$ if $x < 0$. We say that an element α in K is **infinitely large** over F if $|\alpha| \geqq x$ for all $x \in F$. We say that it is **infinitely small** over F if $0 \leqq |\alpha| < |x|$ for all $x \in F, x \neq 0$. We see that α is infinitely large if and only if α^{-1} is infinitely small. We say that K is **archimedean** over F if K has no elements which are infinitely large over F. An intermediate field F_1, $K \supset F_1 \supset F$, is **maximal archimedean over** F in K if it is archimedean over F, and no other intermediate field containing F_1 is archimedean over F. If F_1 is archimedean over F and F_2 is archimedean over F_1 then F_2 is archimedean over F. Hence by Zorn's lemma there always exists a maximal archimedean subfield F_1 of K over F. We say that F is **maximal archimedean in** K if it is maximal archimedean over itself in K.

Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the set of elements of K which are not infinitely large over F. Then it is clear that $\mathfrak{o}$ is a ring, and that for any $\alpha \in K$, we have α or $\alpha^{-1} \in \mathfrak{o}$. Hence $\mathfrak{o}$ is what is called a valuation ring, containing F. Let $\mathfrak{m}$ be the ideal of all $\alpha \in K$ which are infinitely small over F. Then $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{o}$, because any element in $\mathfrak{o}$ which is not in $\mathfrak{m}$ has an inverse in $\mathfrak{o}$. We call $\mathfrak{o}$ the **valuation ring determined by the ordering of K/F.**

Proposition 1.1. *Let K be an ordered field and F a subfield. Let $\mathfrak{o}$ be the valuation ring determined by the ordering of K/F, and let $\mathfrak{m}$ be its maximal ideal. Then $\mathfrak{o}/\mathfrak{m}$ is a real field.*

Proof. Otherwise, we could write

$$-1 = \sum \alpha_i^2 + a$$

with $\alpha_i \in \mathfrak{o}$ and $a \in \mathfrak{m}$. Since $\sum \alpha_i^2$ is positive and a is infinitely small, such a relation is clearly impossible.

§2. REAL FIELDS

A field K is said to be **real** if -1 is not a sum of squares in K. A field K is said to be **real closed** if it is real, and if any algebraic extension of K which is real must be equal to K. In other words, K is maximal with respect to the property of reality in an algebraic closure.

Proposition 2.1. *Let K be a real field.*

(i) *If $a \in K$, then $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real. If a is a sum of squares in K, then $K(\sqrt{a})$ is real. If $K(\sqrt{a})$ is not real, then $-a$ is a sum of squares in K.*

(ii) *If f is an irreducible polynomial of odd degree n in $K[X]$ and if α is a root of f, then $K(\alpha)$ is real.*

Proof. Let $a \in K$. If a is a square in K, then $K(\sqrt{a}) = K$ and hence is real by assumption. Assume that a is not a square in K. If $K(\sqrt{a})$ is not real, then there exist $b_i, c_i \in K$ such that

$$\begin{aligned} -1 &= \sum (b_i + c_i\sqrt{a})^2 \\ &= \sum (b_i^2 + 2c_i b_i\sqrt{a} + c_i^2 a). \end{aligned}$$

Since $\sqrt{a}$ is of degree 2 over K, it follows that

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

If a is a sum of squares in K, this yields a contradiction. In any case, we conclude that

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

is a quotient of sums of squares, and by a previous remark, that $-a$ is a sum of squares. Hence $K(\sqrt{a})$ is real, thereby proving our first assertion.

As to the second, suppose $K(\alpha)$ is not real. Then we can write

$$-1 = \sum g_i(\alpha)^2$$

with polynomials g_i in $K[X]$ of degree $\leqq n-1$. There exists a polynomial h in $K[X]$ such that

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

The sum of $g_i(X)^2$ has even degree, and this degree must be > 0, otherwise -1 is a sum of squares in K. This degree is $\leqq 2n-2$. Since f has odd degree n, it follows that h has odd degree $\leqq n-2$. If β is a root of h then we see that -1 is a sum of squares in $K(\beta)$. Since deg $h <$ deg f, our proof is finished by induction.

Let K be a real field. By a **real closure** we shall mean a real closed field L which is algebraic over K.

Theorem 2.2. *Let K be a real field. Then there exists a real closure of K. If R is real closed, then R has a unique ordering. The positive elements are the squares of R. Every positive element is a square, and every polynomial of odd degree in $R[X]$ has a root in R. We have $R^a = R(\sqrt{-1})$.*

Proof. By Zorn's lemma, our field K is contained in some real closed field algebraic over K. Now let R be a real closed field. Let P be the set of non-zero elements of R which are sums of squares. Then P is closed under addition and multiplication. By Proposition 2.1, every element of P is a square in R, and given $a \in R$, $a \neq 0$, we must have $a \in P$ or $-a \in P$. Thus P defines an ordering. Again by Proposition 2.1, every polynomial of odd degree over R has a root in R. Our assertion follows by Example 5 of Chapter VI, §2.

Corollary 2.3. *Let K be a real field and a an element of K which is not a sum of squares. Then there exists an ordering of K in which a is negative.*

Proof. The field $K(\sqrt{-a})$ is real by Proposition 1.1 and hence has an ordering as a subfield of a real closure. In this ordering, $-a > 0$ and hence a is negative.

Proposition 2.4. *Let R be a field such that $R \neq R^a$ but $R^a = R(\sqrt{-1})$. Then R is real and hence real closed.*

Proof. Let P be the set of elements of R which are squares and $\neq 0$. We contend that P is an ordering of R. Let $a \in R$, $a \neq 0$. Suppose that a is not a square in R. Let α be a root of $X^2 - a = 0$. Then $R(\alpha) = R(\sqrt{-1})$, and hence there exist $c, d \in R$ such that $\alpha = c + d\sqrt{-1}$. Then

$$\alpha^2 = c^2 + 2cd\sqrt{-1} - d^2.$$

Since $1, \sqrt{-1}$ are linearly independent over R, it follows that $c = 0$ (because $a \notin R^2$), and hence $-a$ is a square.

We shall now prove that a sum of squares is a square. For simplicity, write $i = \sqrt{-1}$. Since $R(i)$ is algebraically closed, given $a, b \in R$ we can find $c, d \in R$ such that $(c + di)^2 = a + bi$. Then $a = c^2 - d^2$ and $b = 2cd$. Hence

$$a^2 + b^2 = (c^2 + d^2)^2,$$

as was to be shown.

If $a \in R$, $a \neq 0$, then not both a and $-a$ can be squares in R. Hence P is an ordering and our proposition is proved.

Theorem 2.5. *Let R be a real closed field, and $f(X)$ a polynomial in $R[X]$. Let $a, b \in R$ and assume that $f(a) < 0$ and $f(b) > 0$. Then there exists c between a and b such that $f(c) = 0$.*

Proof. Since $R(\sqrt{-1})$ is algebraically closed, it follows that f splits into a product of irreducible factors of degree 1 or 2. If $X^2 + \alpha X + \beta$ is irreducible ($\alpha, \beta \in R$) then it is a sum of squares, namely

$$\left(X + \frac{\alpha}{2}\right)^2 + \left(\beta - \frac{\alpha^2}{4}\right),$$

and we must have $4\beta > \alpha^2$ since our factor is assumed irreducible. Hence the change of sign of f must be due to the change of sign of a linear factor, which is trivially verified to be a root lying between a and b.

Lemma 2.6. *Let K be a subfield of an ordered field E. Let $\alpha \in E$ be algebraic over K, and a root of the polynomial*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with coefficients in K. Then $|\alpha| \leqq 1 + |a_{n-1}| + \cdots + |a_0|$.

Proof. If $|\alpha| \leqq 1$, the assertion is obvious. If $|\alpha| > 1$, we express $|\alpha|^n$ in terms of the terms of lower degree, divide by $|\alpha|^{n-1}$, and get a proof for our lemma.

Note that the lemma implies that an element which is algebraic over an ordered field cannot be infinitely large with respect to that field.

Let $f(X)$ be a polynomial with coefficients in a real closed field R, and assume that f has no multiple roots. Let $u < v$ be elements of R. By a **Sturm sequence** for f over the interval $[u, v]$ we shall mean a sequence of polynomials

$$S = \{f = f_0, f' = f_1, \ldots, f_m\}$$

having the following properties:

ST 1. The last polynomial f_m is a non-zero constant.

ST 2. There is no point $x \in [u, v]$ such that $f_j(x) = f_{j+1}(x) = 0$ for any value $0 \leqq j \leqq m - 1$.

ST 3. If $x \in [u, v]$ and $f_j(x) = 0$ for some $j = 1, \ldots, m - 1$, then $f_{j-1}(x)$ and $f_{j+1}(x)$ have opposite signs.

ST 4. We have $f_j(u) \neq 0$ and $f_j(v) \neq 0$ for all $j = 0, \ldots, m$.

For any $x \in [u, v]$ which is not a root of any polynomial f_i we denote by $W_S(x)$ the number of sign changes in the sequence

$$\{f(x), f_1(x), \ldots, f_m(x)\},$$

and call $W_S(x)$ the **variation of signs in the sequence**.

Theorem 2.7. (Sturm's Theorem). *The number of roots of f between u and v is equal to $W_S(u) - W_S(v)$ for any Sturm sequence S.*

Proof. We observe that if $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ is the ordered sequence of roots of the polynomials f_j in $[u, v]$ $(j = 0, \ldots, m - 1)$, then $W_S(x)$ is constant on the open intervals between these roots, by Theorem 2.5. Hence it will suffice to prove that if there is precisely one element α such that $u < \alpha < v$ and α is a root of some f_j, then $W_S(u) - W_S(v) = 1$ if α is a root of f, and 0 otherwise. Suppose that α is a root of some f_j, for $1 \leqq j \leqq m - 1$. Then $f_{j-1}(\alpha)$, $f_{j+1}(\alpha)$ have opposite signs by **ST 3**, and these signs do not change when we replace α by u or v. Hence the variation of signs in

$$\{f_{j-1}(u), f_j(u), f_{j+1}(u)\} \quad \text{and} \quad \{f_{j-1}(v), f_j(v), f_{j+1}(v)\}$$

is the same, namely equal to 2. If α is not a root of f, we conclude that

$$W_S(u) = W_S(v).$$

If α is a root of f, then $f(u)$ and $f(v)$ have opposite signs, but $f'(u)$ and $f'(v)$ have the same sign, namely, the sign of $f'(\alpha)$. Hence in this case,

$$W_S(u) = W_S(v) + 1.$$

This proves our theorem.

It is easy to construct a Sturm sequence for a polynomial without multiple roots. We use the Euclidean algorithm, writing

$$\begin{aligned} f &= g_1 f' - f_2, \\ f_2 &= g_2 f_1 - f_3, \\ &\vdots \\ f_{m-2} &= g_{m-1} f_{m-1} - f_m, \end{aligned}$$

using $f' = f_1$. Since f, f' have no common factor, the last term of this sequence is non-zero constant. The other properties of a Sturm sequence are trivially verified, because if two successive polynomials of the sequence have a common zero, then they must all be 0, contradicting the fact that the last one is not.

Corollary 2.8. *Let K be an ordered field, f an irreducible polynomial of degree $\geqq 1$ over K. The number of roots of f in two real closures of K inducing the given ordering on K is the same.*

Proof. We can take v sufficiently large positive and u sufficiently large negative in K so that all roots of f and all roots of the polynomials in the Sturm sequence lie between u and v, using Lemma 2.6. Then $W_S(u) - W_S(v)$ is the total number of roots of f in any real closure of K inducing the given ordering.

Theorem 2.9. *Let K be an ordered field, and let R, R' be real closures of K, whose orderings induce the given ordering on K. Then there exists a unique isomorphism $\sigma : R \to R'$ over K, and this isomorphism is order-preserving.*

Proof. We first show that given a finite subextension E of R over K, there exists an embedding of E into R' over K. Let $E = K(\alpha)$, and let

$$f(X) = \operatorname{Irr}(\alpha, K, X).$$

Then $f(\alpha) = 0$ and the corollary of Sturm's Theorem (Corollary 2.8) shows that f has a root β in R'. Thus there exists an isomorphism of $K(\alpha)$ on $K(\beta)$ over K, mapping α on β.

Let $\alpha_1, \ldots, \alpha_n$ be the distinct roots of f in R, and let $\beta_1, \ldots, \beta_m$ be the distinct roots of f in R'. Say

$$\alpha_1 < \cdots < \alpha_n \quad \text{in the ordering of } R,$$
$$\beta_1 < \cdots < \beta_m \quad \text{in the ordering of } R'.$$

We contend that $m = n$ and that we can select an embedding σ of $K(\alpha_1, \ldots, \alpha_n)$ into R' such that $\sigma\alpha_i = \beta_i$ for $i = 1, \ldots, n$. Indeed, let γ_i be an element of R such that

$$\gamma_i^2 = \alpha_{i+1} - \alpha_i \quad \text{for} \quad i = 1, \ldots, n-1$$

and let $E_1 = K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1})$. By what we have seen, there exists an embedding σ of E_1 into R', and then $\sigma\alpha_{i+1} - \sigma\alpha_i$ is a square in R'. Hence

$$\sigma\alpha_1 < \cdots < \sigma\alpha_n.$$

This proves that $m \geqq n$. By symmetry, it follows that $m = n$. Furthermore, the condition that $\sigma\alpha_i = \beta_i$ for $i = 1, \ldots, n$ determines the effect of σ on

$K(\alpha_1, \ldots, \alpha_n)$. We contend that σ is order-preserving. Let $y \in K(\alpha_1, \ldots, \alpha_n)$ and $0 < y$. Let $\gamma \in R$ be such that $\gamma^2 = y$. There exists an embedding of

$$K(\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_{n-1}, \gamma)$$

into R' over K which must induce σ on $K(\alpha_1, \ldots, \alpha_n)$ and is such that σy is a square, hence > 0, as contended.

Using Zorn's lemma, it is now clear that we get an isomorphism of R onto R' over K. This isomorphism is order-preserving because it maps squares on squares, thereby proving our theorem.

Proposition 2.10. *Let K be an ordered field, K' an extension such that there is no relation*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K, a_i > 0$, and $\alpha_i \in K'$. Let L be the field obtained from K' by adjoining the square roots of all positive elements of K. Then L is real.

Proof. If not, there exists a relation of type

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K$, $a_i > 0$, and $\alpha_i \in L$. (We can take $a_i = 1$.) Let r be the smallest integer such that we can write such a relation with α_i in a subfield of L, of type

$$K'(\sqrt{b_1}, \ldots, \sqrt{b_r})$$

with $b_j \in K$, $b_j > 0$. Write

$$\alpha_i = x_i + y_i\sqrt{b_r}$$

with $x_i, y_i \in K'(\sqrt{b_1}, \ldots, \sqrt{b_{r-1}})$. Then

$$\begin{aligned} -1 &= \sum a_i(x_i + y_i\sqrt{b_r})^2 \\ &= \sum a_i(x_i^2 + 2x_i y_i\sqrt{b_r} + y_i^2 b_r). \end{aligned}$$

By hypothesis, $\sqrt{b_r}$ is not in $K'(b_1, \ldots, \sqrt{b_{r-1}})$. Hence

$$-1 = \sum a_i x_i^2 + \sum a_i b_r y_i^2,$$

contradicting the minimality of r.

Theorem 2.11. *Let K be an ordered field. There exists a real closure R of K inducing the given ordering on K.*

Proof. Take $K' = K$ in Proposition 2.10. Then L is real, and is contained in a real closure. Our assertion is clear.

Corollary 2.12. *Let K be an ordered field, and K' an extension field. In order that there exist an ordering on K' inducing the given ordering of K, it is necessary and sufficient that there is no relation of type*

$$-1 = \sum_{i=1}^{n} a_i \alpha_i^2$$

with $a_i \in K$, $a_i > 0$, and $\alpha_i \in K'$.

Proof. If there is no such relation, then Proposition 2.10 states that L is contained in a real closure, whose ordering induces an ordering on K', and the given ordering on K, as desired. The converse is clear.

Example. Let $\mathbf{Q}^a$ be the field of algebraic numbers. One sees at once that $\mathbf{Q}$ admits only one ordering, the ordinary one. Hence any two real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ are isomorphic, by means of a unique isomorphism. The real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ are precisely those subfields of $\mathbf{Q}^a$ which are of finite degree under $\mathbf{Q}^a$. Let K be a finite real extension of $\mathbf{Q}$, contained in $\mathbf{Q}^a$. An element α of K is a sum of squares in K if and only if every conjugate of α in the real numbers is positive, or equivalently, if and only if every conjugate of α in one of the real closures of $\mathbf{Q}$ in $\mathbf{Q}^a$ is positive.

Note. The theory developed in this and the preceding section is due to Artin-Schreier. See the bibliography at the end of the chapter.

§3. REAL ZEROS AND HOMOMORPHISMS

Just as we developed a theory of extension of homomorphisms into an algebraically closed field, and Hilbert's Nullstellensatz for zeros in an algebraically closed field, we wish to develop the theory for values in a real closed field. One of the main theorems is the following:

Theorem 3.1. *Let k be a field, $K = k(x_1, \ldots, x_n)$ a finitely generated extension. Assume that K is ordered. Let R_k be a real closure of k inducing the same ordering on k as K. Then there exists a homomorphism*

$$\varphi : k[x_1, \ldots, x_n] \to R_k$$

over k.

As applications of Theorem 3.1, one gets:

Corollary 3.2. *Notation being as in the theorem, let* $y_1, \ldots, y_m \in k[x]$ *and assume*

$$y_1 < y_2 < \cdots < y_m$$

is the given ordering of K. *Then one can choose* φ *such that*

$$\varphi y_1 < \cdots < \varphi y_m.$$

Proof. Let $\gamma_i \in K^a$ be such that $\gamma_i^2 = y_{i+1} - y_i$. Then $K(\gamma_1, \ldots, \gamma_{n-1})$ has an ordering inducing the given ordering on K. We apply the theorem to the ring

$$k[x_1, \ldots, x_n, \gamma_1^{-1}, \ldots, \gamma_{m-1}^{-1}, \gamma_1, \ldots, \gamma_{m-1}].$$

Corollary 3.3. (Artin). *Let* k *be a real field admitting only one ordering. Let* $f(X_1, \ldots, X_n) \in k(X)$ *be a rational function having the property that for all* $(a) = (a_1, \ldots, a_n) \in R_k^{(n)}$ *such that* $f(a)$ *is defined, we have* $f(a) \geqq 0$. *Then* $f(X)$ *is a sum of squares in* $k(X)$.

Proof. Assume that our conclusion is false. By Corollary 2.3, there exists an ordering of $k(X)$ in which f is negative. Apply Corollary 3.2 to the ring

$$k[X_1, \ldots, X_n, h(X)^{-1}]$$

where $h(X)$ is a polynomial denominator for $f(X)$. We can find a homomorphism φ of this ring into R_k (inducing the identity on k) such that $\varphi(f) < 0$. But

$$\varphi(f) = f(\varphi X_1, \ldots, \varphi X_n).$$

contradiction. We let $a_i = \varphi(X_i)$ to conclude the proof.

Corollary 3.3 was a Hilbert problem. The proof which we shall describe for Theorem 3.1 differs from Artin's proof of the corollary in several technical aspects.

We shall first see how one can reduce Theorem 3.1 to the case when K has transcendence degree 1 over k, and k is real closed.

Lemma 3.4. *Let* R *be a real closed field and let* R_0 *be a subfield which is algebraically closed in* R (*i.e. such that every element of* R *not in* R_0 *is transcendental over* R_0). *Then* R_0 *is real closed.*

Proof. Let $f(X)$ be an irreducible polynomial over R_0. It splits in R into linear and quadratic factors. Its coefficients in R are algebraic over R_0, and hence must lie in R_0. Hence $f(X)$ is linear itself, or quadratic irreducible already over R_0. By the intermediate value theorem, we may assume that f is positive

definite, i.e. $f(a) > 0$ for all $a \in R_0$. Without loss of generality, we may assume that $f(X) = X^2 + b^2$ for some $b \in R_0$. Any root of this polynomial will bring $\sqrt{-1}$ with it and therefore the only algebraic extension of R_0 is $R_0(\sqrt{-1})$. This proves that R_0 is real closed.

Let R_K be a real closure of K inducing the given ordering on K. Let R_0 be the algebraic closure of k in R_K. By the lemma, R_0 is real closed.

We consider the field $R_0(x_1, \ldots, x_n)$. If we can prove our theorem for the ring $R_0[x_1, \ldots, x_n]$, and find a homomorphism

$$\psi : R_0[x_1, \ldots, x_n] \to R_0,$$

then we let $\sigma : R_0 \to R_K$ be an isomorphism over k (it exists by Theorem 2.9), and we let $\varphi = \sigma \circ \psi$ to solve our problem over k. This reduces our theorem to the case when k is real closed.

Next, let F be an intermediate field, $K \supset F \supset k$, such that K is of transcendence degree 1 over F. Again let R_K be a real closure of K preserving the ordering, and let R_F be the real closure of F contained in R_K. If we know our theorem for extensions of dimension 1, then we can find a homomorphism

$$\psi : R_F[x_1, \ldots, x_n] \to R_F.$$

We note that the field $k(\psi x_1, \ldots, \psi x_n)$ has transcendence degree $\leqq n - 1$, and is real, because it is contained in R_F. Thus we are reduced inductively to the case when K has dimension 1, and as we saw above, when k is real closed.

One can interpret our statement geometrically as follows. We can write $K = R(x, y)$ with x transcendental over R, and (x, y) satisfying some irreducible polynomial $f(X, Y) = 0$ in $R[X, Y]$. What we essentially want to prove is that there are infinitely many points on the curve $f(X, Y) = 0$, with coordinates lying in R, i.e. infinitely many real points.

The main idea is that we find some point $(a, b) \in R^{(2)}$ such that $f(a, b) = 0$ but $D_2 f(a, b) \neq 0$. We can then use the intermediate value theorem. We see that $f(a, b + h)$ changes sign as h changes from a small positive to a small negative element of R. If we take $a' \in R$ close to a, then $f(a', b + h)$ also changes sign for small h, and hence $f(a', Y)$ has a zero in R for all a' sufficiently close to a. In this way we get infinitely many zeros.

To find our point, we consider the polynomial $f(x, Y)$ as a polynomial in one variable Y with coefficients in $R(x)$. Without loss of generality we may assume that this polynomial has leading coefficient 1. We construct a Sturm sequence for this polynomial, say

$$\{f(x, Y), f_1(x, Y), \ldots, f_m(x, Y)\}.$$

Let $d = \deg f$. If we denote by $A(x) = (a_{d-1}(x), \ldots, a_0(x))$ the coefficients of $f(x, Y)$, then from the Euclidean alogrithm, we see that the coefficients of the

polynomials in the Sturm sequence can be expressed as rational functions

$$\{G_v(A(x))\}$$

in terms of $a_{d-1}(x), \ldots, a_0(x)$.

Let

$$v(x) = 1 \pm a_{d-1}(x) \pm \cdots \pm a_0(x) + s,$$

where s is a positive integer, and the signs are selected so that each term in this sum gives a positive contribution. We let $u(x) = -v(x)$, and select s so that neither u nor v is a root of any polynomial in the Sturm sequence for f. Now we need a lemma.

Lemma 3.5. *Let R be a real closed field, and $\{h_i(x)\}$ a finite set of rational functions in one variable with coefficients in R. Suppose the rational field $R(x)$ ordered in some way, so that each $h_i(x)$ has a sign attached to it. Then there exist infinitely many special values c of x in R such that $h_i(c)$ is defined and has the same sign as $h_i(x)$, for all i.*

Proof. Considering the numerators and denominators of the rational functions, we may assume without loss of generality that the h_i are polynomials. We then write

$$h_i(x) = \alpha \prod (x - \lambda) \prod p(x),$$

where the first product is extended over all roots λ of h_i in R, and the second product is over positive definite quadratic factors over R. For any $\xi \in R$, $p(\xi)$ is positive. It suffices therefore to show that the signs of $(x - \lambda)$ can be preserved for all λ by substituting infinitely many values α for x. We order all values of λ and of x and obtain

$$\cdots < \lambda_1 < x < \lambda_2 < \cdots$$

where possibly λ_1 or λ_2 is omitted if x is larger or smaller than any λ. Any value α of x in R selected between λ_1 and λ_2 will then satisfy the requirements of our lemma.

To apply the lemma to the existence of our point, we let the rational functions $\{h_1(x)\}$ consist of all coefficients $a_{d-1}(x), \ldots, a_0(x)$, all rational functions $G_v(A(x))$, and all values $f_j(x, u(x))$, $f_j(x, v(x))$ whose variation in signs satisfied Sturm's theorem. We then find infinitely many special values α of x in R which preserve the signs of these rational functions. Then the polynomials $f(\alpha, Y)$ have roots in R, and for all but a finite number of α, these roots have multiplicity 1.

It is then a matter of simple technique to see that for all but a finite number of points on the curve, the elements $x_1, \ldots, x_n$ lie in the local ring of the homomorphism $R[x, y] \to R$ mapping (x, y) on (a, b) such that $f(a, b) = 0$ but

$D_2 f(a, b) \neq 0$. (Cf. for instance the example at the end of §4, Chapter XII, and Exercise 18 of that chapter.) One could also give direct proofs here. In this way, we obtain homomorphisms

$$R[x_1, \ldots, x_n] \to R,$$

thereby proving Theorem 3.1.

Theorem 3.6. *Let k be a real field, $K = k(x_1, \ldots, x_n, y) = k(x, y)$ a finitely generated extension such that $x_1, \ldots, x_n$ are algebraically independent over k, and y is algebraic over $k(x)$. Let $f(X, Y)$ be the irreducible polynomial in $k[X, Y]$ such that $f(x, y) = 0$. Let R be a real closed field containing k, and assume that there exists $(a, b) \in R^{(n+1)}$ such that $f(a, b) = 0$ but*

$$D_{n+1} f(a, b) \neq 0.$$

Then K is real.

Proof. Let $t_1, \ldots, t_n$ be algebraically independent over R. Inductively, we can put an ordering on $R(t_1, \ldots, t_n)$ such that each t_i is infinitely small with respect to R, (cf. the example in §1). Let R' be a real closure of $R(t_1, \ldots, t_n)$ preserving the ordering. Let $u_i = a_i + t_i$ for each $i = 1, \ldots, n$. Then $f(u, b + h)$ changes sign for small h positive and negative in R, and hence $f(u, Y)$ has a root in R', say v. Since f is irreducible, the isomorphism of $k(x)$ on $k(u)$ sending x_i on u_i extends to an embedding of $k(x, y)$ into R', and hence K is real, as was to be shown.

In the language of algebraic geometry, Theorems 3.1 and 3.6 state that the function field of a variety over a real field k is real if and only if the variety has a simple point in some real closure of k.

EXERCISES

1. Let α be algebraic over $\mathbf{Q}$ and assume that $\mathbf{Q}(\alpha)$ is a real field. Prove that α is a sum of squares in $\mathbf{Q}(\alpha)$ if and only if for every embedding σ of $\mathbf{Q}(\alpha)$ in $\mathbf{R}$ we have $\sigma\alpha > 0$.
2. Let F be a finite extension of $\mathbf{Q}$. Let $\varphi : F \to \mathbf{Q}$ be a $\mathbf{Q}$-linear functional such that $\varphi(x^2) > 0$ for all $x \in F, x \neq 0$. Let $\alpha \in F, \alpha \neq 0$. If $\varphi(\alpha x^2) \geqq 0$ for all $x \in F$, show that α is a sum of squares in F, and that F is totally real, i.e. every embedding of F in the complex numbers is contained in the real numbers. [*Hint*: Use the fact that the trace gives an identification of F with its dual space over $\mathbf{Q}$, and use the approximation theorem of Chapter XII, §1.]

3. Let $\alpha \leqq t \leqq \beta$ be a real interval, and let $f(t)$ be a real polynomial which is positive on this interval. Show that $f(t)$ can be written in the form

$$c(\sum Q_\nu^2 + \sum (t - \alpha)Q_\mu^2 + \sum (\beta - t)Q_\lambda^2)$$

where Q^2 denotes a square, and $c \geqq 0$. *Hint*: Split the polynomial, and use the identity:

$$(t - \alpha)(\beta - t) = \frac{(t - \alpha)^2(\beta - t) + (t - \alpha)(\beta - t)^2}{\beta - \alpha}.$$

Remark. The above seemingly innocuous result is a key step in developing the spectral theorem for bounded hermitian operators on Hilbert space. See the appendix of [La 72] and also [La 85].

4. Show that the field of real numbers has only the identity automorphism. [*Hint*: Show that an automorphism preserves the ordering.]

Real places

For the next exercises, cf. Krull [Kr 32] and Lang [La 53]. These exercises form a connected sequence, and solutions will be found in [La 53].

5. Let K be a field and suppose that there exists a real place of K; that is, a place φ with values in a real field L. Show that K is real.

6. Let K be an ordered real field and let F be a subfield which is maximal archimedean in K. Show that the canonical place of K with respect to F is algebraic over F (i.e. if $\mathfrak{o}$ is the valuation ring of elements of K which are not infinitely large over F, and $\mathfrak{m}$ is its maximal ideal, then $\mathfrak{o}/\mathfrak{m}$ is algebraic over F).

7. Let K be an ordered field and let F be a subfield which is maximal archimedean in K. Let K' be the real closure of K (preserving the ordering), and let F' be the real closure of F contained in K'. Let φ be the canonical place of K' with respect to F'. Show that $\varphi(K')$ is F'-valued, and that the restriction of φ to K is equivalent to the canonical place of K over F.

8. Define a real field K to be **quadratically closed** if for all $\alpha \in K$ either $\sqrt{\alpha}$ or $\sqrt{-\alpha}$ lies in K. The ordering of a quadratically closed real field K is then uniquely determined, and so is the real closure of such a field, up to an isomorphism over K. Suppose that K is quadratically closed. Let F be a subfield of K and suppose that F is maximal archimedean in K. Let φ be a place of K over F, with values in a field which is algebraic over F. Show that φ is equivalent to the canonical place of K over F.

9. Let K be a quadratically closed real field. Let φ be a real place of K, taking its values in a real closed field R. Let F be a maximal subfield of K such that φ is an isomorphism on F, and identify F with $\varphi(F)$. Show that such F exists and is maximal archimedean in K. Show that the image of φ is algebraic over F, and that φ is induced by the canonical place of K over F.

10. Let K be a real field and let φ be a real place of K, taking its values in a real closed field R. Show that there is an extension of φ to an R-valued place of a real closure of K. [*Hint*: first extend φ to a quadratic closure of K. Then use Exercise 5.]

11. Let $K \subset K_1 \subset K_2$ be real closed fields. Suppose that K is maximal archimedean in K_1 and K_1 is maximal archimedean in K_2. Show that K is maximal archimedean in K_2.

12. Let K be a real closed field. Show that there exists a real closed field R containing K and having arbitrarily large transcendence degree over K, and such that K is maximal archimedean in R.

13. Let R be a real closed field. Let $f_1, \ldots, f_r$ be homogeneous polynomials of odd degrees in n variables over R. If $n > r$, show that these polynomials have a non-trivial common zero in R. (*Comments*: If the forms are generic (in the sense of Chapter IX), and $n = r + 1$, it is a theorem of Bezout that in the algebraic closure R^a the forms have exactly $d_1 \cdots d_m$ common zeros, where d_i is the degree of f_i. You may assume this to prove the result as stated. If you want to see this worked out, see [La 53], Theorem 15. Compare with Exercise 3 of Chapter IX.)

Bibliography

[Ar 24] E. ARTIN, Kennzeichnung des Körpers der reellen algebraischen Zahlen, *Abh. Math. Sem. Hansischen Univ.* **3** (1924), pp. 319–323

[Ar 27] E. ARTIN, Über die Zerlegung definiter Funktionen in Quadrate, *Abh. Math. Sem. Hansischen Univ.* **5** (1927), pp. 100–115

[ArS 27] E. ARTIN and E. SCHREIER, Algebraische Konstruktion reeller Körper, *Abh. Math. Sem. Hansischen Univ.* **5** (1927), pp. 85–99

[Kr 32] W. KRULL, Allgemeine Bewertungstheorie, *J. reine angew. Math.* (1932), pp. 169–196

[La 53] S. LANG, The theory of real places, *Ann. Math.* **57** No. 2 (1953), pp. 378–391

[La 72] S. LANG, *Differential manifolds*, Addison-Wesley, 1972; reprinted by Springer Verlag, 1985; superceded by [La 99a].

[La 85] S. LANG, *Real and functional analysis*. Third edition, Springer Verlag, 1993

[La 99a] S. LANG, *Fundamentals of Differential Geometry*, Springer Verlag, 1999