REAL CLOSED FIELDS – APPLICATIONS OF THE INTERMEDIATE VALUE PROPERTY

KENNETH R. DRIESSEL

Remark: I mainly follow the books Basu, Pollack and Roy(2003) and van der Waerden(1970)

Date: November 20, 2006.

Definition: Let α be a term in the language of rings and let X be a variable. Then the **(partial) derivative of α with respect to X**, which is denoted $D(\alpha, X)$, is defined as follows:

- If α is a constant then $D(\alpha, X) := 0$
- If α is a variable then $D(\alpha, X) := 1$ if $\alpha \equiv X$ and $:= 0$ if α is some other variable
- If $\alpha \equiv \beta + \gamma$ then $D(\alpha, X) := D(\beta, X) + D(\gamma, X)$
- If $\alpha \equiv \beta \cdot \gamma$ the $D(\alpha, X) := D(\beta) \cdot \gamma + \beta \cdot D(\gamma)$

Proposition 1. *Let n be a non-negative integer. Then $D(X^n, X) = nX^{n-1}$.*

Definition: If the term α contains no variables other than X then we write α' in place of $D(\alpha, X)$.

Definition: Let R be an ordered ring. Then R has the **intermediate value property** if, for every univariate polynomial P in $R[X]$ and every pair of elements $a < b$ in R, if $P(a)P(b) < 0$ then P has a root in the interval (a, b).

Remark: The phrase *Weierstrass Nullstellensatz* is used by van der Waerden(1970) in place of the phrase "intermediate value property".

As an example note that the real numbers have the intermediate value property. But the rational numbers do not have the intermediate value property: Consider the polynomial $X^2 - 2$.

Definition: Let F be a field. Then F is a **real field** if -1 cannot be written as a sum of squares of elements of F.

Proposition 2. *Let R be an ordered field. Then the following conditions are equivalent:*

- *The field R is real closed.*
- *The field $R[i] = r[X]/(X^2+1)$ obtained by adding the roots of X^2+1 to the field R is algebraically closed.*
- *The field R is a real field that has no non-trivial real algebraic extension.*
- *The field R has the intermediate value property.*

For a proof see Basu, Pollack and Roy(2003) Theorem 2.14 or van der Waerden(1970) .

We shall repeatedly use the intermediate value property.

Proposition 3. *(Rolle's Theorem) Let R be a real closed field. Let $P \in R[X]$ and $a, b \in R$ with $a < b$ and $P(a) = P(b) = 0$. Then the derivative P' of P has a root in the interval (a, b).*

Proof. We may assume that a and b are consecutive roots of P. Then P does not vanish on the open interval (a, b). Note that there exist exponents m and n and a polynomial Q such that

$$P = (X - a)^m (X - b)^n Q$$

and the polynomial Q does not vanish on the closed interval $[a, b]$. Note

$$P' = (X-a)^{m-1}(X-b)^{n-1}Q_1$$

where

$$Q_1 := m(X-b)Q + n(X-a)Q + (X-a)(X-b)Q'.$$

Note $Q_1(a) = m(a-b)Q(a) \neq 0$, $Q_1(b) = n(b-a)Q(b) \neq 0$ and hence $Q_1(a)Q_1(b) < 0$. By the intermiediate value property, Q_1 has a root r in (a, b). Note then $P'(r) = 0$. □

Proposition 4. *(Mean Value Theorem) Let R be a real closed field. Let $P \in R[X]$ and $a, b \in R$ with $a < b$. Then there exists c in the interval (a, b) such that*

$$P(b) - P(a) = (b-a)P'(c).$$

Proof. Let

$$Q(X) := (P(b) - P(a))(X-a) - (b-a)(P(X) - P(a)).$$

Apply Rolle's theorem to this polynomial. In particular, note that $Q(a) = 0$ and $Q(b) = 0$. Hence there is a c in (a, b) such that $Q'(c) = 0$. Also note that $Q'(X) = P(b) - P(a) - (b-a)P'(X)$. □

Proposition 5. *Let R be a real closed field. Let $P \in R[X]$ and $a, b \in R$ with $a < b$. If the derivative P' is positive (respectively, negative) on the interval (a, b) then P is increasing (respectively, decreasing) on the interval $[a, b]$.*

Proof. Use the mean value theorem. □

The next proposition shows that in an ordered field the value of a polynomial at x has the same sign as the value of its leading monomial for x sufficiently large.

Proposition 6. *Let F be an ordered field. Let $P := a_pX^p + \cdots + a_0$ be a polynomial in $F[X]$ with $a_p \neq 0$. Let $b := 2\sum\{|a_i/a_p| : 0 \leq i \leq p\}$. If $|x| > b$ then $P(x)$ and a_px^p have the same sign.*

Proof. Let x satisfy the hypothesis of the implication.

Claim: $2 < x$.

Note that that $1 = |a_p/a_p|$ is one of the terms of the sum.

Claim: $0 < P(x)/(a_px^p)$.

Note that

$$\frac{P(x)}{a_px^p} = 1 + \sum_{i=0}^{p-1} \frac{a_i}{a_p} x^{i-p}.$$

It follows that

$$1 - |\sum_{i=0}^{p-1} \frac{a_i}{a_p} x^{i-p}| \leq \frac{P(x)}{a_px^p}.$$

(In general, $u = 1 + v$ implies $1 - u = -v \le |v|$ which in turn implies $1 - |v| \le u$.) Now

$$
\begin{aligned}
|\sum_{i=0}^{p-1} \frac{a_i}{a_p} x^{i-p}| &\le \sum_{i=0}^{p-1} |\frac{a_i}{a_p}||x^{i-p}| \\
&\le (\sum_{i=0}^{p-1} |\frac{a_i}{a_p}|)(\sum_{i=0}^{p-1} |x|^{i-p}) \\
&\le (\sum_{i=0}^{p-1} |\frac{a_i}{a_p}|)|x|^{-1}(1 + |x|^{-1} + \ldots |x|^{-p+1}) \\
&\le \frac{1}{2}(1 + \frac{1}{2} + \cdots + (\frac{1}{2})^{p-1}) = \frac{1}{2}(\frac{1-(1/2)^p}{1-(1/2)}) = 1 - (\frac{1}{2})^p < 1.
\end{aligned}
$$

□

From the last result we get the following crude root location result.

Proposition 7. *Let F be an ordered field. Let P and b be defined as in the last proposition. Then all the roots of P are between $-b$ and b.*

Proof. Use the last proposition. □