0.1 Counting real roots

In this section, we will study *Sturm's method* of counting the number of roots of a separable polynomial with coefficients in a real-closed field L.

Lemma 0.1. *Let $(k, \leq)$ be an ordered field and let $P \in k[t]$ be a separable polynomial. Assume that P has a root $a \in k$. Then there exists $\delta > 0$ such that*

(i) for $x \in]a-\delta, a+\delta[$ and $x \neq a$, $P(x) \neq 0$.

(ii) for $x \in]a, a+\delta[$, $P(x)$ and $P'(x)$ have the same sign.

(iii) for $x \in]a-\delta, a[$, $P(x)$ and $P'(x)$ have opposite signs.

(iv) for $x \in]0, \delta[$, $P(a+h)$ and $P(a-h)$ have opposite signs.

Proof. Since P is separable and $P(a) = 0$, it follows that $P'(a) \neq 0$. By continuity of P', there exists $\delta > 0$ such that P' has constant sign on $]a-\delta, a+\delta[$. Suppose $P'(x) > 0$. Since k is real-closed, this implies that P is strictly increasing on this interval. In particular, $P(x) < P(a) = 0$ for $x \in]a-\delta, a[$ and $P(x) > P(a) = 0$ for $x \in]a, a+\delta[$. The case $P'(x) < 0$ is similar which concludes the proof. □

Definition 0.2. Let $(k, \leq)$ be an ordered field. A finite sequence $(P_0, \ldots, P_n)$ of polynomials $P_i \in k[t]$ is called a *Sturm sequence* if it satisfies the following properties:

(i) $P_1 = P_0'$

(ii) for all $x \in k$ and $i \in \{0, \ldots, n\}$, if $P_i(x) = 0$, then $P_{i+1}(x) \neq 0$.

(iii) for all $x \in k$ and all $i \in \{1, \ldots, n-1\}$, if $P_i(x) = 0$ then $P_{i-1}(x)P_{i+1}(x) < 0$.

(iv) $P_n \in k^\times$.

If $P \in k[t]$ is separable and k has characteristic 0, then the greatest common divisor of P and P' is 1. To determine a Bézout relation between P and P', one proceeds by successive Euclidean divisions:

First set $P_0 = P$ and $P_1 = P'$, next define P_2 such that $P_0 = P_1Q_1 - P_2$ and $\deg(P_2) < \deg(P_1)$. Inductively, this defines $P_i = P_{i+1}Q_{i+1} - P_{i+2}$ with $\deg(P_{i+2}) < \deg(P_{i+1})$. This algorithm stops after at most $\deg(P_0)$ steps with $P_{n-1} = P_nQ_n$ and $P_n \neq 0$. Then P_n is a greatest common divisor of $P = P_0$ and $P' = P_1$. Since P and P' are coprime, P_n is a non-zero constant.

Corollary 0.3. *The sequence of polynomials $(P_0, \ldots, P_n)$ is a Sturm sequence. This is called the to P associated Sturm sequence.*

Proof. (i) and (iv) are clear. For (ii) observe that if there exists $x \in k$ and $i \in \{0, \ldots, n\}$ such that $P_i(x) = P_{i+1}(x) = 0$, then $P_j(x) = 0$ for all $j \geq i$ which contradicts $P_n(x) = P_n \neq 0$. Finally for (iii), if $P_i(x) = 0$, then $P_{i-1}(x) = -P_{i+1}(x)$, so $P_{i-1}(x)$ and $P_{i+1}(x)$ have opposite signs. □

Remark 0.4. Let $(k, \leq)$ be an ordered field. For a finite sequence of elements $(a_0, \ldots, a_n)$ in k with $a_0 \neq 0$, the number of *sign changes* in this sequence is the number of pairs (i, j) such that $i < j$, $a_i \neq 0$ and $a_ia_j < 0$ with either $j = i+1$ or $j > i+1$ and $a_{i+1} = \ldots = a_{j-1} = 0$.

Theorem 0.5 (Sturm's algorithm)**.** *Let k be a real-closed field equipped with its canonical ordering and let $P \in k[t]$ be a separable polynomial. Let $(P_0, \ldots, P_n)$ be the associated Sturm sequence. For all $a \in k$, we denote by $\nu(a)$ the number of sign changes in the sequence $(P_0(a), \ldots, P_n(a))$. Then, for all pair $a, b \in k$ such that $a < b$ and $P_i(a)P_i(b) \neq 0$ for all i, the number of roots of P in the interval $[a, b]$ is equal to $\nu(a) - \nu(b)$.*

Proof. Let $x_1 < \ldots < x_m$ be the elements of the finite set

$$E = \{x \in]a, b[\mid \exists i \in \{0, \ldots, n\}, P_i(x) = 0\}.$$

There exists a partition of $[a, b]$ in subintervals $[\alpha_j, \alpha_{j+1}]$ where $\alpha_0 = a$, $\alpha_m = b$, and for all $j \in \{0, \ldots, m-1\}$, $\alpha_j \notin E$, $[\alpha_j, \alpha_{j+1}] \cap E = \{x_j\}$. Also

$$\sum_{j=0}^{m-1} (\nu(\alpha_j) - \nu(\alpha_{j+1})) = \nu(\alpha_0) - \nu(\alpha_1) + \nu(\alpha_1) - \ldots - \nu(\alpha_m) = \nu(a) - \nu(b).$$

Thus it suffices to show that for fixed $j \in \{0, \ldots, m-1\}$, the number of roots of P in $[\alpha_j, \alpha_{j+1}]$ is equal to $\nu(\alpha_j) - \nu(\alpha_{j+1})$. By construction, P has at most one root in $[\alpha_j, \alpha_{j+1}]$, at x_j, thus we want to show

$$\nu(\alpha_j) - \nu(\alpha_{j+1}) = \begin{cases} 0 & P(x_j) \neq 0 \\ 1 & P(x_j) = 0 \end{cases}.$$

If $P(x_j) = 0$, then $P(\alpha_j)$ and $P(\alpha_{j+1})$ must have opposite sign. Indeed, by 0.1 $P(x_j + h)P(x_j - h) < 0$ for all $h > 0$ small enough, but P cannot change sign on $[\alpha_j, x_j - h]$ nor on $[x_j + h, \alpha_{j+1}]$, for otherwise the intermediate value theorem would imply the existence of a root $x \neq x_j$ in $[\alpha_j, \alpha_{j+1}]$. So $P(\alpha_j)P(\alpha_{j+1}) < 0$. If $P(\alpha_j) > 0$, then $P(\alpha_{j+1}) < 0$. With $P_1 = P'$ and 0.1, it follows that $P_1(x) < 0$ for x close to x_j. But P_1 cannot change sign in $[\alpha_j, \alpha_{j+1}]$, otherwise its root in that interval would be x_j. Since P is separable and $P_1 = P'$, this is impossible. Thus $P' < 0$ and P is strictly decreasing on $[\alpha_j, \alpha_{j+1}]$. So the sequence of signs in the sequence $(P_0(\alpha_j), P_1(\alpha_j), \ldots, P_n(\alpha_j))$ starts with $(+, -, \ldots)$ while the one at α_{j+1} starts with $(-, -, \ldots)$. Similarly, if $P(\alpha_j) < 0$, then the sequences are $(-, +, \ldots)$ and $(+, +, \ldots)$. In either case, there is one more sign change in the sequence corresponding to α_j, so $\nu(\alpha_j) - \nu(\alpha_{j+1}) = 1$.

Now suppose $P(x_j) \neq 0$. Observe that $P_0(\alpha_j)$ and $P_0(\alpha_{j+1})$ have the same sign, otherwise by the intermediate value theorem and the construction, $P_0(x_j) = 0$. Also a difference between $\nu(\alpha_j)$ and $\nu(\alpha_{j+1})$ only occurs if there exists $i \in \{0, \ldots, n-1\}$ such that $P_i(\alpha_j)P_i(\alpha_{j+1}) < 0$. In this case, again by the intermediate value theorem, we have $P_i(x_j) = 0$. By the definition of a Sturm sequence, we have $P_{i-1}(x_j)P_{i+1}(x_j) < 0$. If $P_{i-1}(x_j) < 0$ then $P_{i-1} < 0$ on $[\alpha_j, \alpha_{j+1}]$, because x_j is the only possible root for P_{i-1} in $[\alpha_j, \alpha_{j+1}]$, so P_{i-1} cannot change sign on that interval. Likewise, P_{i+1} has the same sign on $[\alpha_j, \alpha_{j+1}]$ as it does at x_j. Proceeding similarly when $P_{i-1}(x_j) > 0$, we arrive at the following possibilities for the sign sequences of $P_{i-1}(\alpha_j)P_i(\alpha_j)P_{i+1}(\alpha_j)$ and $P_{i-1}(\alpha_{j+1})P_i(\alpha_{j+1})P_{i+1}(\alpha_{j+1})$:

	$P_i(\alpha_j) < 0$	$P_i(\alpha_j) > 0$
$P_{i-1}(x_j) < 0$	$--+$	$-++$
$P_{i-1}(x_j) > 0$	$+--$	$++-$

(a) Sign sequence at α_j

	$P_i(\alpha_j) < 0$	$P_i(\alpha_j) > 0$
$P_{i-1}(x_j) < 0$	$-++$	$--+$
$P_{i-1}(x_j) > 0$	$++-$	$+--$

(b) Sign sequence at α_{j+1}

Since sign sequences located in cells of the two tables corresponding to the same case have the same number of sign changes, equal to 1, we see that $\nu(\alpha_j) - \nu(\alpha_{j+1}) = 0$. □

We deduce from the previous result, this important result:

Corollary 0.6. *Let $(k, \leq)$ be an ordered field and let L_1, L_2 be real-closed, orderable extensions of k. Let $P \in k[t]$ be an irreducible polynomial over k. Then P has the same number of roots in L_1 as it does in L_2.*

Proof. For a polynomial $Q = c_n t^n + c_{n-1} t^{n-1} + \ldots + c_0 \in k[t]$ with $c_n \neq 0$, the roots of Q in an ordered real-closed extension L of k are bounded by

$$M = 1 + \left|\frac{c_{n-1}}{c_n}\right|_L + \ldots + \left|\frac{c_0}{c_n}\right|_L = 1 + \left|\frac{c_{n-1}}{c_n}\right|_k + \ldots + \left|\frac{c_0}{c_n}\right|_k.$$

Note that M is independent from L. So given $P \in k[t]$ irreducible and the associated Sturm sequence $(P_0, P_1, \ldots, P_n)$, there exists $M \in k$ such that all roots of all P_i's in L are contained in the interval $[-M, M] \subseteq L$. Since char $k = 0$, P is separable, by 0.5 the number of roots of P in $[-M, M] \subseteq L$ is equal to $\nu(-M) - \nu(M)$. Since $\pm M \in k$, all $P_i \in k[t]$ and the ordering of L extends the one of k, the number of sign changes $\nu(\pm M)$ in the sequences $(P_0(-M), P_1(-M), \ldots, P_n(-M))$ and $(P_0(M), P_1(M), \ldots, P_n(M))$ does not depend on L. □

Remark 0.7. (i) In particular, if $P \in k[t]$ is an arbitrary polynomial, then if P has a root in a real-closed extension L of k, then it has a root in all real-closed extensions of k.

A polynomial with coefficients in an ordered field $(k, \leq)$ might not have roots in any real-closed extensions of k.

(ii) There is a proof of Sturm's algorithm that does not require P to be separable. As a consequence 0.6 holds for all $P \in k[t]$, not only the irreducible ones.