REAL ALGEBRAIC GEOMETRY LECTURE NOTES (13: 01/12/2009 - BEARBEITET 6/12/18)

SALMA KUHLMANN

THE TARSKI-SEIDENBERG PRINCIPLE

Main Lemma. For any real closed field R and every sequence of polynomials $f_1, \ldots, f_s \in R[X]$ of degrees $\leq m$, with f_s nonconstant and none of the $f_1, \ldots, f_{s-1}$ identically zero, we have
$SIGN_R(f_1, \ldots, f_s) \in W_{s,m}$ is completely determined by
$SIGN_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s) \in W_{2s,m}$, where f_s' is the derivative of f_s, and $g_1, \ldots, g_s$ are the remainders of the euclidean division of f_s *by* $f_1, \ldots, f_{s-1}, f_s'$, respectively.
Equivalently, the map $\varphi : W_{2s,m} \longrightarrow W_{s,m}$

$$SIGN_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s) \longmapsto SIGN_R(f_1, \ldots, f_s)$$

is well defined.
In other words, for any $(f_1, \ldots, f_s), (F_1, \ldots, F_s) \in R[X]$,
$SIGN_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s) = SIGN_R(F_1, \ldots, F_{s-1}, F_s', G_1, \ldots, G_s)$
$\Rightarrow SIGN_R(f_1, \ldots, f_s) = SIGN_R(F_1, \ldots, F_s)$.

Proof. Assume $w = SIGN_R(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$ is given.

Let $x_1 < \ldots < x_N$, with $N \leq 2sm$, be the roots in R of those polynomials among $f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s$ that are not identically zero. Extract from these the subsequence $x_{i_1} < \ldots < x_{i_M}$ of the roots of the polynomials $f_1, \ldots, f_{s-1}, f_s'$. By convention, let $x_{i_0} := x_0 = -\infty$; $x_{i_{M+1}} := x_{N+1} = +\infty$.
Note that the sequence $x_{i_1} < \ldots < x_{i_M}$ depends only on w.
For $k = 1, \ldots, M$ one of the polynomials $f_1, \ldots, f_{s-1}, f_s'$ vanishes at x_{i_k}. This allows to choose a map (determined by w)

$$\theta : \{1, \ldots, M\} \to \{1, \ldots, s\}$$

such that $f_s(x_{i_k}) = g_{\theta(k)}(x_{i_k})$
(This goes via polynomial division $f_s = f_{\theta(k)} q_{\theta(k)} + g_{\theta(k)}$, where $f_{\theta(k)}(x_{i_k}) = 0$).

Claim I. The existence of a root of f_s in an interval $]x_{i_k}, x_{i_{k+1}}[$, for $k = 0, \ldots, M$ depends only on w.

Proof of Claim I.
Case 1: f_s has a root in $]-\infty, x_{i_1}[$ (if $M \neq 0$) if and only if
$$sign\big(f_s'(\,]-\infty, x_1[\,)\big)sign\big(g_{\theta(1)}(x_{i_1})\big) = 1,$$
equivalently iff
$$sign\big(f_s'(\,]-\infty, x_1[\,)\big) = sign f_s(x_{i_1}).$$

($\Leftarrow$) We want to show that if $sign\big(f_s'(\,]-\infty, x_1[\,)\big) = sign f_s(x_{i_1})$, then f_s has a root in $]-\infty, x_{i_1}[$.
Suppose on contradiction that f_s has no root in $]-\infty, x_{i_1}[$, then $sign f_s$ must be constant and nonzero on $]-\infty, x_{i_1}]$, so we get
$0 \neq sign f_s(\,]-\infty, x_1[\,) = sign f_s(\,]-\infty, x_{i_1}]\,) = sign f_s(x_{i_1}) = sign f_s'(\,]-\infty, x_1[\,)$
$\Rightarrow sign f_s(\,]-\infty, x_1[\,) = sign f_s'(\,]-\infty, x_1[\,)$, a contradiction $\Big[$because on $]-\infty, -D[\,:\;\; sign f(x) = (-1)^m sign(d)$ for $f = dx^m + \ldots + d_0$ and $sign f'(x) = (-1)^{m-1} sign(md)$ for $f' = mdx^{m-1} + \ldots$, see Corollary 2.1 of lecture 6 (05/11/09)$\Big]$.

($\Rightarrow$) Assume that f_s has a root (say) $x \in\,]-\infty, x_{i_1}[$.
Note that $sign f_s(x_{i_1}) \neq 0$ $\Big[$otherwise $f_s(x_{i_1}) = f(x_{i_1}) = 0$, so (by Rolle's theorem) f_s' has a root in $]x, x_{i_1}[$ and the only possibility is $x_1 \in\,]x, x_{i_1}[$ (by our listing), but then $x_1 = x_{i_1}$, a contradiction$\Big]$.
Note also that f_s cannot have two roots (counting multiplicity) in $]-\infty, x_{i_1}[$ $\Big[$otherwise f_s' will be forced to have a root in $]-\infty, x_{i_1}[$, a contradiction as before$\Big]$.
So
$$-sign f_s\big(\,]-\infty, x[\,\big) = sign f_s\big(\,]x, x_{i_1}]\,\big) = sign f_s(x_{i_1}),$$
also (by same argument as before)
$$-sign f_s\big(\,]-\infty, x[\,\big) = sign f_s'\big(\,]-\infty, x_1[\,\big),$$
therefore, we get
$$sign f_s'\big(\,]-\infty, x_1[\,\big) = sign f_s(x_{i_1}).$$
□ (case 1)

Case 2: Similarly one proves that: f_s has a root in $]x_{i_M}, +\infty[$ (if $M \neq 0$) if and only if
$$sign\big(f_s'(\,]x_N, +\infty[\,)\big)sign\big(g_{\theta(M)}(x_{i_M})\big) = -1,$$
$$\Big(\text{i.e. iff } sign f_s'(\,]x_N, +\infty[\,) = -sign f_s(x_{i_M}) \neq 0\Big).$$

Case 3: f_s has a root in $]x_{i_k}, x_{i_{k+1}}[$, for $k = 1, \ldots, M-1$, if and only if
$$sign\big(g_{\theta(k)}(x_{i_k})\big)sign\big(g_{\theta(k+1)}(x_{i_{k+1}})\big) = -1,$$

equivalently iff

$$sign f_s(x_{i_k}) = -sign f_s(x_{i_{k+1}}).$$

(Proof is clear because if f_s has a root in $]x_{i_k}, x_{i_{k+1}}[$, then this root is of multipilicty 1 and therefore a sign change must occur.)

Case 4: f_s has exactly one root in $]-\infty, +\infty[$ if $M = 0$. □ (claim I)

Claim II. $SIGN_R(f_1, \ldots, f_s)$ depends only on w.

Proof of Claim II.

Notation: Let $y_1 < \ldots < y_L$, with $L \leq sm$, be the roots in R of the polynomials $f_1, \ldots, f_s$. As before, let $y_0 := -\infty$, $y_{L+1} := +\infty$.

Set $I_k :=]y_k, y_{k+1}[$, $k = 0, \ldots, L$.

Define

$$\rho : \{0, \ldots, L+1\} \longrightarrow \{0, \ldots, M+1\} \cup \{(k, k+1) \mid k = 0, \ldots, M\}$$

$$l \longmapsto \begin{cases} k & \text{if } y_l = x_{i_k}, \\ (k, k+1) & \text{if } y_l \in]x_{i_k}, x_{i_{k+1}}[\end{cases}$$

Note that by Claim I, L and ρ depends only on w. So, to prove claim II it is enough to show that $SIGN_R(f_1, \ldots, f_s)$ depends only on ρ and w.

Also,

$$SIGN_R(f_1, ..., f_s) := \begin{pmatrix} sign f_1(I_0) & sign f_1(y_1) & \ldots & sign f_1(y_L) & sign f_1(I_L) \\ \vdots & \vdots & & \vdots & \vdots \\ sign f_{s-1}(I_0) & sign f_{s-1}(y_1) & \ldots & sign f_{s-1}(y_L) & sign f_{s-1}(I_L) \\ sign f_s(I_0) & sign f_s(y_1) & \ldots & sign f_s(y_L) & sign f_s(I_L) \end{pmatrix}$$

is an $s \times (2L+1)$ matrix with coefficients in $\{-1, 0, +1\}$.

Case 1: $j = 1, \ldots, s-1$

For $l \in \{0, \ldots, L+1\}$ we have

- if $\rho(l) = k \Rightarrow sign\big(f_j(y_l)\big) = sign\big(f_j(x_{i_k})\big)$,
- if $\rho(l) = (k, k+1) \Rightarrow sign\big(f_j(y_l)\big) = sign\big(f_j(\,]x_{i_k}, x_{i_{k+1}}[\,)\big)$.

So, $sign\big(f_j(y_l)\big)$ is known from w and ρ, for all $j = 1, \ldots, s-1$ and $l \in \{0, \ldots, L+1\}$.

We also have

- if $\rho(l) = k$ or $(k, k+1) \Rightarrow sign\big(f_j(\,]y_l, y_{l+1}[\,)\big) = sign\big(f_j(\,]x_{i_k}, x_{i_{k+1}}[\,)\big)$.

So, $sign\big(f_j(\ ]y_l, y_{l+1}[\ )\big)$ is known from w and ρ, for all $j = 1, \dots, s-1$ and $l \in \{0, \dots, L+1\}$.
Thus one can reconstruct the first $s-1$ rows of $SIGN_R(f_1, ..., f_s)$ from w.

Case 2: $j = s$
For $l \in \{0, \dots, L+1\}$ we have

- if $\rho(l) = k \Rightarrow sign\big(f_s(y_l)\big) = sign\big(g_{\theta(k)}(x_{i_k})\big)$,
- if $\rho(l) = (k, k+1) \Rightarrow sign\big(f_s(y_l)\big) = 0$.

So, $sign\big(f_s(y_l)\big)$ is known from w and ρ, for all $l \in \{0, \dots, L+1\}$ and therefore can also be reconstructed from w.
Now remains the most delicate case that concerns $sign\big(f_s(\ ]y_l, y_{l+1}[\ )\big)$:
For $l \in \{0, \dots, L+1\}$ we have

- if $l \neq 0$, $\rho(l) = k \Rightarrow$
$$sign\big(f_s(\ ]y_l, y_{l+1}[\ )\big) = \begin{cases} sign\big(g_{\theta(k)}(x_{i_k})\big) & \text{if it is } \neq 0, \\ sign\big(f_s'(\ ]x_{i_k}, x_{i_{k+1}}[\ )\big) & \text{otherwise.} \end{cases}$$
[This is because $\big(\rho(l) = k$ if $y_l = x_{i_k}$, so$\big)$:
- if $g_{\theta(k)}(x_{i_k}) = f_s(x_{i_k}) \neq 0$, then by continuity sign is constant, and
- if $g_{\theta(k)}(x_{i_k}) = f_s(x_{i_k}) = 0$, then on $]x_{i_k}, x_{i_{k+1}}[$:
$$\begin{cases} f_s' \geq 0 \Rightarrow f_s(x_{i_k}) < f_s(y) \text{ for } y < x_{k+1}, \text{ so } f_s(y) > 0, \\ f_s' \leq 0 \Rightarrow -f_s(x_{i_k}) < -f_s(y) \text{ for } y < x_{k+1}, \text{ so } f_s(y) < 0 \end{cases}$$
(using 6. Lecture, Cor. 2.4: In a real closed ordered field, if P is a nonconstant polynomial s.t. $P' \geq 0$ on $[a, b]$, $a < b$, then $P(a) < P(b)$).]
- if $l \neq 0$, $\rho(l) = (k, k+1) \Rightarrow sign\big(f_s(\ ]y_l, y_{l+1}[\ )\big) = sign\big(f_s'(\ ]x_{i_k}, x_{i_{k+1}}[\ )\big)$.
[We argue as follows (noting that $\rho(l) = (k, k+1)$ if $y_l \in]x_{i_k}, x_{i_{k+1}}[$):
$sign\big(f_s(\ ]y_l, y_{l+1}[\ )\big)$ is constant so at any rate is equal to $sign\big(f_s(\ ]y_l, x_{i_{k+1}}[\ )\big)$, now using the fact that $f_s(y_l) = 0$ and the same lemma (stated above) we get, for any $a \in\ ]y_l, x_{i_{k+1}}[$:
$$\begin{cases} f_s' \geq 0 \Rightarrow f_s(y_l) < f_s(a), \text{ so } f_s(a) > 0, \\ f_s' \leq 0 \Rightarrow -f_s(y_l) < -f_s(a), \text{ so } f_s(a) < 0 \end{cases}$$
i.e. f_s has same sign as f_s'.]
- if $l = 0 \Rightarrow sign\big(f_s(\ ]-\infty, y_1[\ )\big) = sign\big(f_s'(\ ]-\infty, x_1[\ )\big)$ (as before). □