REAL ALGEBRAIC GEOMETRY LECTURE NOTES
PART II: POSITIVE POLYNOMIALS
(17: BEARBEITET 15/12/2022)

SALMA KUHLMANN

Contents

1. GEOMETRIC VERSION OF POSITIVSTELLENSATZ

Theorem 1.1. (Recall) (Positivstellensatz: Geometric Version) Let $A = \mathbb{R}[\underline{X}]$. Let $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[\underline{X}]$, $f \in \mathbb{R}[\underline{X}]$. Then

(1) $f > 0$ on $K_S \Leftrightarrow \exists\, p, q \in T_S$ s.t. $pf = 1 + q$
(Striktpositivstellensatz)

(2) $f \geq 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{N}_0, \exists\, p, q \in T_S$ s.t. $pf = f^{2m} + q$
(Nonnegativstellensatz)

(3) $f = 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{N}_0$ s.t. $-f^{2m} \in T_S$
(Real Nullstellensatz (first form))

(4) $K_S = \phi \Leftrightarrow -1 \in T_S$.

Proof. It consists of two parts:
-Step I: prove that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)
-Step II: prove (4) [using Tarski Transfer]

We will start with step II:
Clearly $K_S \neq \phi \Rightarrow -1 \notin T_S$ (since $-1 \in T_S \Rightarrow K_S = \phi$), so it only remains to prove the following proposition:

Proposition 1.2. (3.2 of last lecture) If $-1 \notin T_S$ (i.e. if T_S is a proper preordering), then $K_S \neq \phi$.

For proving this we need the following results:

Lemma 1.3.1. (3.4.1 of last lecture) Let A be a commutative ring with 1. Let P be a maximal proper preordering in A. Then P is an ordering.

Proof. We have to show:

(i) $P \cup -P = A$, and

(ii) $\mathfrak{p} := P \cap -P$ is a prime ideal of A.

(i) Assume $a \in A$, but $a \notin P \cup -P$.

By maximality of P, we have: $-1 \in (P + aP)$ and $-1 \in (P - aP)$

Thus

$-1 = s_1 + at_1$ and

$-1 = s_2 - at_2$; for some $s_1, s_2, t_1, t_2 \in P$

So (rewritting)

$-at_1 = 1 + s_1$ and

$at_2 = 1 + s_2$

Multiplying we get:

$-a^2 t_1 t_2 = 1 + s_1 + s_2 + s_1 s_2$

$\Rightarrow -1 = s_1 + s_2 + s_1 s_2 + a^2 t_1 t_2 \in P$, a contradiction.

(ii) Now consider $\mathfrak{p} := P \cap -P$, clearly it is an ideal.

We claim that $\mathfrak{p}$ is prime.

Let $ab \in \mathfrak{p}$ and $a, b \notin \mathfrak{p}$.

Assume w.l.o.g. that $a, b \notin P$.

Then as above in (i), we get:

$-1 \in (P + aP)$ and $-1 \in (P + bP)$

So, $-1 = s_1 + at_1$ and

$-1 = s_2 + bt_2$; for some $s_1, s_2, t_1, t_2 \in P$

Rearranging and multiplying we get:

$(at_1)(bt_2) = (1 + s_1)(1 + s_2) = 1 + s_1 + s_2 + s_1 s_2$

$\Rightarrow -1 = \underbrace{s_1 + s_2 + s_1 s_2}_{\in P} \underbrace{-abt_1 t_2}_{\in \mathfrak{p} \subset P}$

$\Rightarrow -1 \in P$, a contradiction. □

Lemma 1.3.2. (3.4.2 of last lecture) Let A be a commutative ring with 1 and $P \subseteq A$ an ordering. Then P induces uniquely an ordering $\leq_P$ on $F := ff(A/\mathfrak{p})$ defined by:

$$\forall\, a,b \in A, b \notin \mathfrak{p} : \frac{\overline{a}}{\overline{b}} \geq_P 0 \text{ (in } F) \Leftrightarrow ab \in P, \text{ where } \overline{a} = a + \mathfrak{p}. \qquad \square$$

Recall 1.3.3. (Tarski Transfer Principle) Suppose $(\mathbb{R}, \leq) \subseteq (F, \leq)$ is an ordered field extension of $\mathbb{R}$. If $\underline{x} \in F^n$ satisfies a finite system of polynomial equations and inequalities with coefficients in $\mathbb{R}$, then $\exists\, \underline{r} \in \mathbb{R}^n$ satisfying the same system. $\square$

Using lemma 1.3.1, lemma 1.3.2 and TTP (recall 1.3.3), we prove the proposition 1.2 as follows:

Proof of Propostion 1.2. **To show:** $-1 \notin T_S \Rightarrow K_S \neq \phi$.
Set $S = \{g_1, \dots, g_s\} \subseteq \mathbb{R}[\underline{X}]$
$-1 \notin T_S \Rightarrow T_S$ is a proper preordering.
By Zorn, extend T_S to a maximal proper preordering P.
By lemma 1.3.1, P is an ordering on $\mathbb{R}[\underline{X}]$; $\mathfrak{p} := P \cap -P$ is prime.
By lemma 1.3.2, let $(F, \leq_P) = \left(ff\,(\mathbb{R}[\underline{X}]/\mathfrak{p})\,,\ \leq_P\right)$ is an ordered field extension of $(\mathbb{R}, \leq)$.

Now consider the system $\mathcal{S} := \begin{cases} g_1 \geq 0 \\ \quad\vdots \\ g_s \geq 0. \end{cases}$

Claim: The system $\mathcal{S}$ has a solution in F^n, namely $\underline{X} := (\overline{X_1}, \dots, \overline{X_n})$,
i.e. to show: $g_i(\overline{X_1}, \dots, \overline{X_n}) \geq_P 0$; $i = 1, \dots, s$.

Indeed $g_i(\overline{X_1}, \dots, \overline{X_n}) = \overline{g_i(X_1, \dots, X_n)}$, and since $g_i \in T_S \subset P$, it follows by definition of $\leq_P$ that $\overline{g_i} \geq_P 0$.

Now apply TTP (recall 1.3.3) to conclude that:
$\exists\, \underline{r} \in \mathbb{R}^n$ satisfying the system $\mathcal{S}$, i.e. $g_i(\underline{x}) \geq 0$; $i = 1, \dots, s$.
$\Rightarrow \underline{r} \in K_S \Rightarrow K_S \neq \phi$.

This completes step II. $\square$

Now we will do step I:
i.e. we show (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1)

(1) $\Rightarrow$ (2)

Let $f \geq 0$ on K_S, $f \not\equiv 0$.

Consider $S' \subseteq \mathbb{R}[\underline{X}, Y]$, $S' := S \cup \left\{ Yf - 1, -Yf + 1 \right\}$
So, $K_{S'} = \left\{ (\underline{x}, y) \mid g_i(\underline{x}) \geq 0,\ i = 1, ..., n\ ;\ yf(\underline{x}) = 1 \right\}$.

Thus $f(\underline{X}, Y) = f(\underline{X}) > 0$ on $K_{S'}$, so applying (1) $\exists\ p',\ q' \in T_{S'}$ s.t.

$$p'(\underline{X}, Y) f(\underline{X}) = 1 + q'(\underline{X}, Y)$$

Substitute $Y := \frac{1}{f(\underline{X})}$ in above equation and clear denominators by multiplying both sides by $f(\underline{X})^{2m}$ for $m \in \mathbb{N}_0$ sufficiently large to get:

$$p(\underline{X}) f(\underline{X}) = f(\underline{X})^{2m} + q(\underline{X}),$$

with $p(\underline{X}) := f(\underline{X})^{2m} p'\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in \mathbb{R}[\underline{X}]$ and
$q(\underline{X}) := f(\underline{X})^{2m} q'\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in \mathbb{R}[\underline{X}]$.

To finish the proof we **claim** that: $p(\underline{X}),\ q(\underline{X}) \in T_S$ for sufficiently large m.

Observe that $p'(\underline{X}, Y) \in T_{S'}$, so p' is a sum of terms of the form:

$$\underbrace{\sigma(\underline{X}, Y)}_{\in\ \Sigma\mathbb{R}[\underline{X}, Y]^2}\ g_1^{e_1} \dots g_s^{e_s}\ (Yf(\underline{X}) - 1)^{e_{s+1}} (-Yf(\underline{X}) + 1)^{e_{s+2}}\ ;\ e_1, \dots, e_s, e_{s+1}, e_{s+2} \in \{0, 1\}$$

say $\sigma(\underline{X}, Y) = \sum_j h_j(\underline{X}, Y)^2$.

Now when we substitute Y by $\frac{1}{f(\underline{X})}$ in $p'(\underline{X}, Y)$, all terms with e_{s+1} or e_{s+2} equal to 1 vanish.

So, the remaining terms are of the form

$$\sigma\left(\underline{X}, \frac{1}{f(\underline{X})}\right) g_1^{e_1} \dots g_s^{e_s} = \left(\sum_j \left[h_j\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \right]^2 \right) g_1^{e_1} \dots g_s^{e_s}$$

So, we want to choose m large enough so that $f(\underline{X})^{2m}\ \sigma\left(\underline{X}, \frac{1}{f(\underline{X})}\right) \in\ \Sigma\mathbb{R}[\underline{X}]^2$.

Write $h_j(\underline{X}, Y) = \sum_i h_{ij}(\underline{X}) Y^i$

Let $m \geq \deg\ (h_j(\underline{X}, Y))$ in Y, for all j.

Substituting $Y = \frac{1}{f(\underline{X})}$ in $h_j(\underline{X}, Y)$ and multiplying by $f(\underline{X})^m$, we get:

$$f(\underline{X})^m\ h_j\left(\underline{X}, \frac{1}{f(\underline{X})}\right) = \sum_i h_{ij}(\underline{X})\ f(\underline{X})^{m-i},\ \text{ with } (m - i) \geq 0\ \forall\ i$$

so that $f(\underline{X})^m\ h_j\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big) \in \mathbb{R}[\underline{X}]$, for all j.

So $f(\underline{X})^{2m}\ \sigma\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big) = f(\underline{X})^{2m} \left(\sum_j \left[h_j\Big(\underline{X}, \dfrac{1}{f(\underline{X})}\Big) \right]^2 \right)$

$$= \sum_j \left[f(\underline{X})^m\ h_j\Big(\underline{X}, \frac{1}{f(\underline{X})}\Big) \right]^2 \in\ \Sigma\mathbb{R}[\underline{X}]^2$$

Thus p and (similarly) $q \in T_S$, which proves our claim and hence (1) $\Rightarrow$ (2). $\square$

(2) $\Rightarrow$ (3)

Assume $f = 0$ on K_S. Apply (2) to f and $-f$ to get:

$p_1 f = f^{2m_1} + q_1$ and

$-p_2 f = f^{2m_2} + q_2$; for some $p_1, p_2, q_1, q_2 \in T_S$, $m_i \in \mathbb{N}_0$

Multiplying yields:

$$-p_1 p_2 f^2 = f^{2(m_1+m_2)} + f^{2m_1} q_2 + f^{2m_2} q_1 + q_1 q_2$$

$$\Rightarrow -f^{2(m_1+m_2)} = \underbrace{p_1 p_2 f^2 + f^{2m_1} q_2 + f^{2m_2} q_1 + q_1 q_2}_{\in\ T_S}$$

i.e. $-f^{2m} \in T_S$. $\square$

(3) $\Rightarrow$ (4)

Assume $K_S = \phi$

$\Rightarrow$ the constant polynomial $f(\underline{X}) \equiv 1$ vanishes on K_S.

Applying (3), gives $-1 \in T_S$. $\square$

(4) $\Rightarrow$ (1)

Let $S^{'} = S \cup \{-f\}$

Since $f > 0$ on K_S we have $K_{S'} = \phi$, so $-1 \in T_{S'}$ by (4).

Moreover from $S^{'} = S \cup \{-f\}$, we have $T_{S'} = T_S - fT_S$

$\Rightarrow -1 = q - pf$; for some $p, q \in\ T_S$

i.e. $pf = 1 + q$ $\square$

This completes step I and hence the proof of Positivstellensatz. $\square\square$

We will now study other forms of the Real Nullstellensatz that will relate it to Hilbert's Nullstellensatz.

2. EXKURS IN COMMUTATIVE ALGEBRA

Recall 2.1. Let K be a field, $S \subseteq K[\underline{X}]$. Define

$\mathcal{Z}(S) := \{\underline{x} \in K^n \mid g(\underline{x}) = 0 \ \ \forall\, g \in S\}$, the **zero set** of S.

Proposition 2.2. Let $V \subseteq K^n$. Then the following are equivalent:

(1) $V = \mathcal{Z}(S)$; for some finite $S \subseteq K[\underline{X}]$
(2) $V = \mathcal{Z}(S)$; for some set $S \subseteq K[\underline{X}]$
(3) $V = \mathcal{Z}(I)$; for some ideal $I \subseteq K[\underline{X}]$

Proof. (1) $\Rightarrow$ (2) Clear.

(2) $\Rightarrow$ (3) Take $I := < S >$, the ideal generated by S.

(3) $\Rightarrow$ (1) Using Hilbert Basis Theorem (i.e. for a field K, every ideal in $K[\underline{X}]$ is finitely generated):

$I =< S >$, S finite
$\Rightarrow \mathcal{Z}(I) = \mathcal{Z}(S)$. □

Definition 2.3. $V \subseteq K^n$ is an **algebraic set** if V satisfies one of the equivalent conditions of Proposition 2.2.

Definition 2.4. Given a subset $A \subseteq K^n$, we form:

$\mathcal{I}(A) := \{f \in K[\underline{X}] \mid f(\underline{a}) = 0 \ \ \forall\, \underline{a} \in A\}$.

Proposition 2.5. Let $A \subseteq K^n$. Then

(1) $\mathcal{I}(A)$ is an ideal called the **ideal of vanishing polynomials** on A.

(2) If $A = V$ is an algebraic set in K^n, then $\mathcal{Z}(\mathcal{I}(V)) = V$

(3) the map $V \longmapsto \mathcal{I}(V)$ is a 1-1 map from the set of algebraic sets in K^n into the set of ideals of $K[\underline{X}]$. □

Remark 2.6. Note that for an ideal I of $K[\underline{X}]$, the inclusion $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ is always true.

[*Proof.* Say (by Hilbert Basis Theorem) $I =< g_1, \ldots, g_s >$, $g_i \in K[\underline{X}]$. Then

$$\mathcal{Z}(I) = \{\underline{x} \in K^n \mid g_i(\underline{x}) = 0 \ \forall\ i = 1, \dots, s\},$$
$$\mathcal{I}(\mathcal{Z}(I)) = \{f \in K[\underline{X}] \mid f(\underline{x}) = 0 \ \ \forall\ \underline{x} \in \mathcal{Z}(I)\}.$$

Assume $f = h_1 g_1 + \dots + h_s g_s \in I$, then $f(\underline{x}) = 0 \ \forall\ \underline{x} \in \mathcal{Z}(I)$
[since by definition $\underline{x} \in \mathcal{Z}(I) \Rightarrow g_i(\underline{x}) = 0 \ \forall\ i = 1, \dots, s$]
$\Rightarrow f \in \mathcal{I}(\mathcal{Z}(I))$. $\square$]

But in general it is false that $\mathcal{I}(\mathcal{Z}(I)) = I$. Hilbert's Nullstellensatz studies necessary and sufficient conditions on K and I so that this identity holds.