POSITIVE POLYNOMIALS LECTURE NOTES (04: 22/04/10)

SALMA KUHLMANN

Contents

1. EXKURS IN COMMUTATIVE ALGEBRA

Recall 1.1. Let K be a field and I an ideal of $K[\underline{X}]$, then the inclusion $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ is always true.

But in general it is false that

$$\mathcal{I}(\mathcal{Z}(I)) = I \tag{1}$$

Note 1.2. In other words we study the map

$$\mathcal{I} : \left\{\text{algebraic sets in } K^n\right\} \rightsquigarrow \left\{\text{Ideals of } K[\underline{X}]\right\}$$
$$V \longmapsto \mathcal{I}(V)$$

- Clearly this map is 1-1 (proposition 2.5 of last lecture).
- What is the image of $\mathcal{I}$? (2)

  Let I an ideal, $I = \mathcal{I}(V)$

  $\Rightarrow \mathcal{Z}(I) = \underbrace{\mathcal{Z}(\mathcal{I}(V)) = V}_{\text{(prop. 2.5 of last lecture)}}$

  Thus an ideal I is in the image $\Leftrightarrow I = \mathcal{I}(\mathcal{Z}(I))$

So studying the equality (1) amounts to studying (2).

2. RADICAL IDEALS AND REAL IDEALS

Remark 2.1. For an ideal $I \subseteq K[\underline{X}]$, answer to $I = \mathcal{I}(\mathcal{Z}(I))$ is known
• when K is algebraically closed (Hilbert's Nullstellensatz),
or
• when K is real closed (Real Nullstellensatz).

To formulate these two important theorems we need to introduce some terminology:

Definition 2.2. Let A be a commutative ring with 1, $I \subseteq A$, I an ideal of A. Define

(i) $\sqrt{I} := \{a \in A \mid \exists\, m \in \mathbb{N} \text{ s.t. } a^m \in I\}$, the **radical** of I.

(ii) $\sqrt[R]{I} := \{a \in A \mid \exists\, m \in \mathbb{N} \text{ and } \sigma \in \Sigma A^2 \text{ s.t. } a^{2m} + \sigma \in I\}$, the **real radical** of I.

Remark 2.3. It follows from the definition that $I \subseteq \sqrt{I} \subseteq \sqrt[R]{I}$.

Definition 2.4. Let I be an ideal of A. Then

(1) I is called **radical ideal** if $I = \sqrt{I}$, and

(2) I is called **real radical ideal** (or just **real ideal**) if $I = \sqrt[R]{I}$.

Remark 2.5. (i) Every prime ideal is radical, but the converse does not hold in general.

(ii) I real radical $\Rightarrow$ I radical (follows from Remark 2.3 and Definition 2.4).

Proposition 2.6. Let A be a commutative ring with 1, $I \subseteq A$ an ideal. Then

(1) I is radical $\Leftrightarrow \forall\, a \in A : a^2 \in I \Rightarrow a \in I$

(2) I is real radical $\Leftrightarrow$ for $k \in \mathbb{N}, \forall\, a_1, \ldots, a_k \in A : \sum_{i=1}^{k} a_i^2 \in I \Rightarrow a_1 \in I$.

Proof. (1) ($\Rightarrow$) Trivially follows from definition.

($\Leftarrow$) Let $a \in \sqrt{I}$, then $\exists\, m \geq 1$ s.t. $a^m \in I$.
Let k (big enough) s.t. $2^k \geq m$, then

$$a^{2^k} = a^m a^{2^k-m} \in I$$

Now we show by induction on k that:

$$[a^2 \in I \Rightarrow a \in I] \Rightarrow [a^{2^k} \in I \Rightarrow a \in I]$$

For $k = 1$, it is clear.

Assume it true for k and show it true for $k+1$, i.e. let $a^{2^{k+1}} \in I$, then

$$a^{2^{k+1}} = \left(a^{2^k}\right)^2 \in I \underbrace{\Rightarrow}_{\text{(by assumption)}} a^{2^k} \in I \underbrace{\Rightarrow}_{\text{(induction hypothesis)}} a \in I.$$

(2) ($\Rightarrow$) Trivially follows from definition.

($\Leftarrow$) Let $a \in \sqrt[R]{I}$, then $\exists\, m \geq 1,\ \sigma = \Sigma a_i{}^2\ (\in \Sigma A^2)$ s.t. $a^{2m} + \sigma \in I$.

$$\Rightarrow (a^m)^2 + \sigma \in I \underbrace{\Rightarrow}_{\text{(by assumption)}} a^m \in I \underbrace{\Rightarrow}_{\text{(as above in (1))}} a \in I. \qquad \square$$

Remark 2.7. (i) Since real radical ideal $\Rightarrow$ radical ideal, so in particular (2) $\Rightarrow$ (1) in above proposition.

(ii) A prime ideal is always radical (as in Remark 2.5), but need not be real.

Proposition 2.8. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Then
$\mathfrak{p}$ is real $\Leftrightarrow ff(A/\mathfrak{p})$ is a real field.

Proof. $\mathfrak{p}$ is not real

$\Leftrightarrow \exists\, a, a_1, \ldots, a_k \in A;\ a \notin \mathfrak{p}$ such that $a^2 + \sum_{i=1}^{k} a_i^2 \in \mathfrak{p}$

$\Leftrightarrow \overline{a}^2 + \sum_{i=1}^{k} \overline{a_i}^2 = 0$ and $\overline{a} \neq 0$ (in $A/\mathfrak{p}$)

$\Leftrightarrow ff(A/\mathfrak{p})$ is not real. $\square$

Theorem 2.9. Let K be a field, $A = K[\underline{X}], I \subseteq A$ an ideal. Then

(1) (Hilbert's Nullstellensatz) Assume K is algebraically closed, then
$\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$.
(Proved in B5)

(2) (Real Nullstellensatz) Assume K is real closed, then

$\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$.
(Will be deduced from Positivstellensatz)

Corollary 2.10. Consider the map:

$$\mathcal{I} : \left\{\text{algebraic sets in } K^n\right\} \longrightarrow \left\{\text{Ideals of } K[\underline{X}]\right\}$$

(1) If K is algebraically closed, then
Image $\mathcal{I} = \{I \mid I \text{ is a radical ideal}\}$

(2) If K is real closed, then
Image $\mathcal{I} = \{I \mid I \text{ is real ideal}\}$ □

Now we want to deduce the Real Nullstellensatz [Theorem 2.9 (2)] from part (3) of the Positivstellensatz (PSS) [Theorem 1.1 of last lecture].

We need the following 2 (helping) lemmas:

Lemma 2.11. Let A be a commutative ring and M be a quadratic module, then:

(1) $M \cap (-M)$ is an ideal of A.

(2) The following are equivalent for $a \in A$:

(i) $a \in \sqrt{M \cap (-M)}$

(ii) $a^{2m} \in M \cap (-M)$ for some $m \in \mathbb{N}, m \geq 1$

(iii) $-a^{2m} \in M$ for some $m \in \mathbb{N}, m \geq 1$. □

Lemma 2.12. Let A be a ring, $M(= M_S)$ a quadratic module (resp. preordering) of A generated by $S = \{g_1, \ldots, g_s\}; g_1, \ldots, g_s \in A$. Let I be an ideal in A generated by $h_1, \ldots, h_t$, i.e. $I = (h_1, \ldots, h_t); h_1, \ldots, h_t \in A$. Then $M + I$ is the quadratic module (resp. the preordering) generated by $S \cup \{\pm h_i \ ; \ i = 1, \ldots, t\}$. □

Recall 2.13. [(3) of PSS] Let $A = \mathbb{R}[\underline{X}], S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[\underline{X}], f \in \mathbb{R}[\underline{X}]$. Then $f = 0$ on $K_S \Leftrightarrow \exists\, m \in \mathbb{Z}_+$ s.t. $-f^{2m} \in T_S$.

Corollary 2.14. (to Recall 2.13 and Lemma 2.11) Let $K = K_S \subseteq \mathbb{R}^n,\ T = T_S \subseteq \mathbb{R}[\underline{X}]$ (as in PSS), then

$$\mathcal{I}(K_S) = \sqrt{T_S \cap (-T_S)}.$$

Proof. $f = 0$ on $K_S \underbrace{\Leftrightarrow}_{\text{(by(3) of PSS)}} -f^{2m} \in T_S$ for some $m \in \mathbb{Z}_+$

$$\underbrace{\Leftrightarrow}_{\text{(by lemma 2.11)}} f \in \sqrt{T_S \cap (-T_S)}$$ □

Corollary 2.15. (to Lemma 2.11 and 2.12) Let A be a commutative ring with 1. Let I be an ideal of A. Consider the preordering $T := \Sigma A^2 + I$, then

$$\sqrt[R]{I} = \sqrt{T \cap (-T)}.$$ □

Now Corollary 2.14 and Corollary 2.15 give the proof of the Real Nullstellensatz (RNSS) as follows:

Proof of RNSS [Theorem 2.9 (2)]. Let I be an ideal of $\mathbb{R}[\underline{X}]$

We **show that:** $\mathcal{I}(\mathcal{Z}(I)) = \sqrt[R]{I}$

$\mathbb{R}[\underline{X}]$ Noetherian $\Rightarrow I = (h_1, \ldots, h_t)$ (by Hilbert Basis Theorem) .
Consider $S := \{\pm h_i \,;\, i = 1, \ldots, t\}$
Then $K_S = \mathcal{Z}(I)$ [clearly]

Now by Lemma 2.12, we have:

$T = T_S = \Sigma \mathbb{R}[\underline{X}]^2 + I$

So we get,

$$\mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(K_S) \underbrace{=}_{\text{(Cor 2.14)}} \sqrt{T \cap (-T)} \underbrace{=}_{\text{(Cor 2.15)}} \sqrt[R]{I}$$ □

3. THE REAL SPECTRUM

Definition 3.1. Let A be a commutative ring with 1. Then:

$\mathcal{S}pec(A) := \{\mathfrak{p} \mid \mathfrak{p}$ is prime ideal of A $\}$ is called the **Spectrum** of A.

$\mathcal{S}per(A) = \mathcal{S}pec_r(A) := \Big\{(\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a prime ideal of A and $\leq$ is an ordering on the (formally real) field $ff(A/\mathfrak{p})\Big\}$ is called the **Real Spectrum** of A.

Remark 3.2. (i) Several orderings may be defined on $ff(A/\mathfrak{p})$,
$(\mathfrak{p}, \leq_1) \neq (\mathfrak{p}, \leq_2)$.

(ii) $(\mathfrak{p}, \leq) \in \mathcal{S}per(A) \Rightarrow \mathfrak{p}$ is real radical ideal. [see Proposition 2.8 and Remark 2.5 (i).]

Note 3.3. $\mathcal{S}per(A) := \{\alpha = (\mathfrak{p}, \leq) \mid \mathfrak{p}$ is a real prime and $\leq$ an ordering on $ff(A/\mathfrak{p})\}$.