

REAL ALGEBRAIC GEOMETRY LECTURE NOTES
(10: 20/11/09)

SALMA KUHLMANN

CONTENTS

1. Homomorphism Theorems	1
2. Hilbert's 17 th problem	3

1. HOMOMORPHISM THEOREMS

Theorem 1.1. (*Homomorphism Theorem I*) Let $R \subseteq R_1$ be real closed fields and $I \subset R[x]$ an ideal. Then

$$\exists R\text{-alg. hom. } \varphi: \frac{R[x]}{I} \longrightarrow R_1 \Rightarrow \exists R\text{-alg. hom. } \psi: \frac{R[x]}{I} \longrightarrow R.$$

Corollary 1.2. (*Homomorphism Theorem II*) Suppose R and R_1 are real closed fields, $R \subseteq R_1$. Let A be a finitely generated R -algebra. If there is an R -algebra homomorphism

$$\varphi: A \longrightarrow R_1$$

then there is an R -algebra homomorphism

$$\psi: A \longrightarrow R.$$

Proof. We want to use Homomorphism Theorem I. For this we just prove the following:

Claim 1.3. A is a finitely generated R -algebra if and only if there is a surjective R -algebra homomorphism $\vartheta: R[x_1, \dots, x_n] \longrightarrow A$ (for some $n \in \mathbb{N}$).

Proof.

(\Rightarrow) Let A be a finitely generated R -algebra, say with generators r_1, \dots, r_n . Define $\vartheta: R[x_1, \dots, x_n] \longrightarrow A$ by setting $\vartheta(x_i) := r_i$ for every $i = 1, \dots, n$, and $\vartheta(a) := a$ for every $a \in R$.

(\Leftarrow) Given a surjective homomorphism $\vartheta: R[x_1, \dots, x_n] \longrightarrow A$ set $r_i := \vartheta(x_i) \in A$ for every $i = 1, \dots, n$. Then $\{r_1, \dots, r_n\}$ generate A over R .

□

So we get $A \cong R[x]/I$ with $I = \ker \vartheta$.

□

We can see that Homomorphism Theorem II implies T-T-III:

Let $R \subset R_1$ be real closed fields. $S(\underline{X})$ with coefficients in R has a solution $\underline{x} \in R_1^n$ if and only if it has a solution $\underline{x} \in R^n$.

We first need the following:

Proposition 1.4. *Let*

$$S(\underline{x}) := \begin{cases} f_1(\underline{x}) \triangleleft_1 0 \\ \vdots \\ f_k(\underline{x}) \triangleleft_k 0 \end{cases}$$

be a system with coefficients in R , where $\triangleleft_i \in \{\geq, >, =, \neq\}$. Then $S(\underline{x})$ can be written as a system of the form

$$\sigma(\underline{x}) := \begin{cases} g_1(\underline{x}) \geq 0 \\ \vdots \\ g_s(\underline{x}) \geq 0 \\ g(\underline{x}) \neq 0 \end{cases}$$

for some $g_1, \dots, g_s, g \in R[\underline{x}]$.

Proof.

- Replace each equality in the original system by a pair of inequalities:

$$f_i = 0 \Leftrightarrow \begin{cases} f_i \geq 0 \\ -f_i \geq 0 \end{cases}$$

- Replace each strict inequality

$$f_i > 0 \text{ by } \begin{cases} f_i \geq 0 \\ f_i \neq 0 \end{cases}$$

- Finally collect all inequalities $f_i \neq 0$, $i = 1, \dots, t$ as

$$g := \prod_{i=1}^t f_i \neq 0.$$

□

Now we show that Homomorphism Theorem II implies T-T-III:

Proof. Let $R \subseteq R_1$ and let $S(\underline{x})$ be a system with coefficients in R :

$$S(\underline{x}) := \begin{cases} f_1(\underline{x}) \triangleleft_1 0 \\ \vdots \\ f_k(\underline{x}) \triangleleft_k 0 \end{cases}$$

Rewrite it as

$$S(\underline{x}) := \begin{cases} f_1(\underline{x}) \geq 0 \\ \vdots \\ f_s(\underline{x}) \geq 0 \\ g(\underline{x}) \neq 0 \end{cases}$$

with $f_i(\underline{x}), g(\underline{x}) \in R[x_1, \dots, x_n]$.

Suppose $\underline{x} \in R_1^n$ is a solution of $S(\underline{x})$. Consider

$$A := \frac{R[X_1, \dots, X_n, Y_1, \dots, Y_k, Z]}{\langle Y_1^2 - f_1, \dots, Y_k^2 - f_k; gZ - 1 \rangle},$$

which is a finitely generated R -algebra. Consider the R -algebra homomorphism φ such that

$$\begin{aligned} \varphi: A &\longrightarrow R_1 \\ \bar{X}_i &\mapsto x_i \\ \bar{Y}_j &\mapsto \sqrt{f_j(\underline{x})} \\ \bar{Z} &\mapsto 1/g(\underline{x}). \end{aligned}$$

By Homomorphism Theorem II there is an R -algebra homomorphism $\psi: A \longrightarrow R$. Then $\psi(\bar{X}_1), \dots, \psi(\bar{X}_n)$ is the required solution in R^n . □

2. HILBERT'S 17th PROBLEM

Definition 2.1. Let R be a real closed field. We say that a polynomial $f(\underline{x}) \in R[\underline{x}]$ is **positive semi-definite** if $f(x_1, \dots, x_n) \geq 0 \forall (x_1, \dots, x_n) \in R^n$. We write $f \geq 0$.

We know that

$$f \in \sum R[\underline{x}]^2 \Rightarrow f \geq 0.$$

Now take $R = \mathbb{R}$. Conversely, for any $f \in \mathbb{R}[\underline{x}]$ is it true that

$$f \geq 0 \text{ on } \mathbb{R}^n \stackrel{?}{\Rightarrow} f \in \sum \mathbb{R}(\underline{x})^2. \quad \text{(Hilbert's 17th problem).}$$

Remark 2.2.

- (1) Hilbert knew that the answer is NO to the more natural question

$$f \in \mathbb{R}[\underline{x}], f \geq 0 \text{ on } \mathbb{R}^n \Rightarrow f \in \sum \mathbb{R}[\underline{x}]^2 ?$$

- (2) If $n = 1$ then indeed $f \geq 0 \text{ on } \mathbb{R} \Rightarrow f = f_1^2 + f_2^2$.

(3) More generally Hilbert showed that:

Set $P_{d,n} :=$ the set of homogeneous polynomials of degree d in n -variables which are positive semi-definite

and set $\sum_{d,n} :=$ the subset of $P_{d,n}$ consisting of sums of squares.

Then

$$P_{d,n} = \sum_{d,n} \iff n \leq 2 \text{ or } d = 2 \text{ or } (n = 3 \text{ and } d = 4).$$

Note: only d even is interesting because

Lemma 2.3. $0 \neq f \in \sum \mathbb{R}[\underline{x}]^2 \Rightarrow \deg(f)$ is even. More precisely, if $f = \sum_{i=1}^k f_i^2$, with $f_i \in \mathbb{R}[\underline{x}]$ $f_i \neq 0$, then $\deg(f) = 2 \max\{\deg(f_i) : i = 1, \dots, k\}$.

Hilbert knew that $P_{6,3} \setminus \sum_{6,3} \neq \emptyset$.

The first example was given by Motzkin 1967:

$$m(X, Y, Z) = X^6 + Y^4 Z^2 + Y^2 Z^4 - 3X^2 Y^2 Z^2.$$

Theorem 2.4. (Artin, 1927) Let R be a real closed field and $f \in R[\underline{x}]$, $f \geq 0$ on R^n . Then $f \in \sum R(\underline{x})^2$.

Proof. Set $F = R(\underline{x})$ and $T = \sum F^2 = \sum R(\underline{x})^2$. Note that since $R(\underline{x})$ is real, $\sum F^2$ is a proper preordering.

We want to show:

$$f \notin T \Rightarrow \exists \underline{x} \in R^n : f(\underline{x}) < 0.$$

Since $f \in F \setminus T$, by Zorn's Lemma there is a preordering $P \supseteq T$ of F which is maximal for the property that $f \notin P$. Then P is an ordering of F (see proof of Crucial Lemma 2.1 of Lecture 3).

Let \leq_P be the ordering such that (F, \leq_P) is an ordered field extension of the real closed field R (since R is a real closed field, it is uniquely ordered and we know that (F, \leq_P) is an ordered field extension). By construction $f \notin P$ so $f(\underline{x}) < 0$. Consider the system

$$S(\underline{x}) : \left\{ \begin{array}{l} f(\underline{x}) < 0, \\ f(\underline{x}) \in R[\underline{x}]. \end{array} \right.$$

This system has a solution \underline{X} in $F = R(\underline{x})$, namely

$$\underline{X} = (X_1, \dots, X_n) \quad X_i \in R(\underline{x}) = F.$$

thus by T-T-IV $\exists \underline{x} \in R^n$ with $f(\underline{x}) < 0$. □