Inhaltsverzeichnis zur Vorlesung: Reelle algebraische Geometrie I

Prof. Dr. Salma Kuhlmann, Dr. Mickael Matusinski

WS 2009/2010[1]

[1]Die Seitenzahlen in Klammern geben die Seitenzahl fr die Suche mit Adobe Acrobat Reader an (unter dem Men ANZEIGE – GEHE ZU – SEITE).

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (01: 20/10/09)

SALMA KUHLMANN

Contents

Convention: When a new definition is given, the German name appears between brackets.

1. Orderings

Definition 1.1. (*partielle Anordnung*) Let Γ be a non-empty set and let $\leqslant$ be a relation on Γ such that:

(i) $\gamma \leqslant \gamma \quad \forall\, \gamma \in \Gamma$,

(ii) $\gamma_1 \leqslant \gamma_2,\ \gamma_2 \leqslant \gamma_1 \ \Rightarrow\ \gamma_1 = \gamma_2 \quad \forall\, \gamma_1, \gamma_2 \in \Gamma$,

(iii) $\gamma_1 \leqslant \gamma_2,\ \gamma_2 \leqslant \gamma_3 \ \Rightarrow \gamma_1 \leqslant \gamma_3 \quad \forall\, \gamma_1, \gamma_2, \gamma_3 \in \Gamma$.

Then $\leqslant$ is a **partial order** on Γ and $(\Gamma, \leqslant)$ is said to be a **partially ordered set**.

Example 1.2. Let X be a non-empty set. For every $A, B \subseteq X$, the relation

$$A \leqslant B \iff A \subseteq B,$$

is a partial order on the power set $\mathcal{P}(X) = \{A : A \subseteq X\}$.

Definition 1.3. (*totale Anordung*) A partial order $\leqslant$ on a set Γ is said to be **total** if

$$\forall\, \gamma_1, \gamma_2 \in \Gamma \quad \gamma_1 \leqslant \gamma_2 \text{ or } \gamma_2 \leqslant \gamma_1.$$

Notation 1.4. If $(\Gamma, \leqslant)$ is a partially ordered set and $\gamma_1, \gamma_2 \in \Gamma$, then we write:

$\gamma_1 < \gamma_2 \ \Leftrightarrow\ \gamma_1 \leqslant \gamma_2$ and $\gamma_1 \neq \gamma_2$,
$\gamma_1 \geqslant \gamma_2 \ \Leftrightarrow\ \gamma_2 \leqslant \gamma_1$,
$\gamma_1 > \gamma_2 \ \Leftrightarrow\ \gamma_2 \leqslant \gamma_1$ and $\gamma_1 \neq \gamma_2$.

Examples 1.5. Let $\Gamma = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$.

(1) For every $(a_1, b_1), (a_2, b_2) \in \mathbb{R} \times \mathbb{R}$ we can define
$$(a_1, b_1) \leqslant (a_2, b_2) \iff a_1 \leqslant a_2 \text{ and } b_1 \leqslant b_2.$$
Then $(\mathbb{R} \times \mathbb{R}, \leqslant)$ is a partially ordered set.

(2) For every $(a_1, b_1), (a_2, b_2) \in \mathbb{R} \times \mathbb{R}$ we can define
$(a_1, b_1) \leqslant_l (a_2, b_2) \iff [a_1 < a_2]$ or $[a_1 = a_2$ and $b_1 \leqslant b_2]$.
Then $(\mathbb{R} \times \mathbb{R}, \leqslant_l)$ is a totally ordered set. (Remark: the "l" stands for "lexicographic").

2. Ordered fields

Definition 2.1. (*angeordneter Körper*) Let K be a field. Let $\leqslant$ be a total order on K such that:

(i) $x \leqslant y \Rightarrow x + z \leqslant y + z \qquad \forall\, x, y, z \in K,$

(ii) $0 \leqslant x,\ 0 \leqslant y \Rightarrow 0 \leqslant xy \qquad \forall\, x, y \in K.$

Then the pair $(K, \leqslant)$ is said to be an **ordered field**.

Examples 2.2. The field of the rational numbers $(\mathbb{Q}, \leqslant)$ and the field of the real numbers $(\mathbb{R}, \leqslant)$ are ordered fields, where $\leqslant$ denotes the usual order.

Definition 2.3. (*formal reell Körper*) A field K is said to be **(formal) real** if there is an order $\leqslant$ on K such that $(K, \leqslant)$ is an ordered field.

Proposition 2.4. *Let $(K, \leqslant)$ be an ordered field. The following hold:*

- $a \leqslant b \Leftrightarrow 0 \leqslant b - a \qquad \forall\, a, b \in K$
- $0 \leqslant a^2 \qquad \forall\, a \in K$
- $a \leqslant b,\ 0 \leqslant c \Rightarrow ac \leqslant bc \qquad \forall\, a, b, c \in K$
- $0 < a \leqslant b \Rightarrow 0 < 1/b \leqslant 1/a \qquad \forall\, a, b \in K$
- $0 < n \qquad \forall\, n \in \mathbb{N}$

Remark 2.5. If K is a real field then $\mathrm{char}(K) = 0$ and K contains a copy of $\mathbb{Q}$.

Notation 2.6. Let $(K, \leqslant)$ be an ordered field and let $a \in K$.

$$\mathrm{sign}(a) := \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -1 & \text{if } a < 0. \end{cases}$$

$$|a| := \operatorname{sign}(a)a.$$

Fact 2.7. Let $(K, \leqslant)$ be an ordered field and let $a, b \in K$. Then

(*i*) $\operatorname{sign}(ab) = \operatorname{sign}(a)\operatorname{sign}(b)$,

(*ii*) $|\,ab\,| = |\,a\,||\,b\,|$,

(*iii*) $|\,a+b\,| \leqslant |\,a\,| + |\,b\,|$.

3. Archimedean fields

Definition 3.1. (*archimedischer Körper*) Let $(K, \leqslant)$ be a field. We say that K is **Archimedean** if

$$\forall\, a \in K \;\; \exists\, n \in \mathbb{N} \;\text{ such that }\; a < n.$$

Definition 3.2. Let $(\Gamma \leqslant)$ be an ordered set and let $\Delta \subseteq \Gamma$. Then

- Δ is **cofinal** (*kofinal*) in Γ if
$$\forall\, \gamma \in \Gamma \;\; \exists\, \delta \in \Delta \;\text{ such that }\; \gamma \leqslant \delta.$$
- Δ is **coinitial** (*koinitial*) in Γ if
$$\forall\, \gamma \in \Gamma \;\; \exists\, \delta \in \Delta \;\text{ such that }\; \delta \leqslant \gamma.$$
- Δ is **coterminal** (*koterminal*) in Γ if Δ is cofinal and coinitial in Γ.

Example 3.3. Let $(K \leqslant)$ be an Archimedean field. Then $\mathbb{N}$ is cofinal in K, $-\mathbb{N}$ is coinitial in K and $\mathbb{Z} = -\mathbb{N} \cup \mathbb{N}$ is coterminal in K.

Remark 3.4.

- If $(K, \leqslant)$ is an Archimedean field and $Q \subseteq K$ is a subfield, then $(Q, \leqslant)$ is an Archimedean field.

- $(\mathbb{R}, \leqslant)$ is an Archimedean field and therefore also $(\mathbb{Q}, \leqslant)$ is.

Remark 3.5. Let $(K, \leqslant)$ be an ordered field. Then K is Archimedean if and only if $\forall\, a, b \in K^* \;\exists\, n \in \mathbb{N}$ such that

$$|a| \leqslant n|\,b\,| \;\text{ and }\; |\,b\,| \leqslant n|a|.$$

Example 3.6. Let $\mathbb{R}[\mathrm{x}]$ be the ring of the polynomials with coefficients in $\mathbb{R}$. We denote by $ff(\mathbb{R}[\mathrm{x}])$ the field of the rational functions of $\mathbb{R}[\mathrm{x}]$, i.e.

$$ff(\mathbb{R}[\mathrm{x}]) = \mathbb{R}(\mathrm{x}) := \left\{ \frac{f(\mathrm{x})}{g(\mathrm{x})} : f(\mathrm{x}), g(\mathrm{x}) \in \mathbb{R}[\mathrm{x}] \text{ and } g(\mathrm{x}) \neq 0 \right\}.$$

Let $f(\mathrm{x}) = a_n\mathrm{x}^n + a_{n-1}\mathrm{x}^{n-1} + \cdots + a_1\mathrm{x} + a_0 \in \mathbb{R}[\mathrm{x}]$ and let $k \in \mathbb{N}$ the smallest index such that $a_k \neq 0$ (and therefore actually $f(\mathrm{x}) = a_n\mathrm{x}^n + \cdots + a_k\mathrm{x}^k$). We define

$$f(\mathrm{x}) > 0 \;\Leftrightarrow\; a_k > 0$$

and then for every $f(\mathrm{x}), g(\mathrm{x}) \in \mathbb{R}[\mathrm{x}]$ with $g(\mathrm{x}) \neq 0$ we define

$$\frac{f(\mathrm{x})}{g(\mathrm{x})} \geqslant 0 \;\Leftrightarrow\; f(\mathrm{x})g(\mathrm{x}) \geqslant 0.$$

This is a total order on $K = ff(\mathbb{R}[\mathrm{x}])$ which makes $(K, \leqslant)$ an ordered field. We claim that $(K, \leqslant)$ contains

(i) an infinite positive element, i.e.

$$\exists\, A \in K \;\text{ such that }\; A > n \;\; \forall\, n \in \mathbb{N},$$

(ii) an infinitesimal positive element, i.e.

$$\exists\, a \in K \;\text{ such that }\; 0 < a < 1/n \;\; \forall\, n \in \mathbb{N}.$$

For instance the element $\mathrm{x} \in K$ is infinitesimal and the element $1/\mathrm{x} \in K$ is infinite. Therefore $(K, \leqslant)$ is not Archimedean.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (02: 22/10/09)

SALMA KUHLMANN

Contents

1. The field $\mathbb{R}(\mathrm{x})$

Let us consider again the field $\mathbb{R}(\mathrm{x})$ of the rational functions on $\mathbb{R}[\mathrm{x}]$:

Example 1.1. Let $f(\mathrm{x}) = a_n\mathrm{x}^n + a_{n-1}\mathrm{x}^{n-1} + \cdots + a_1\mathrm{x} + a_0 \in \mathbb{R}[\mathrm{x}]$ and let $k \in \mathbb{N}$ the smallest index such that $a_k \neq 0$ (and therefore actually $f(\mathrm{x}) = a_n\mathrm{x}^n + \cdots + a_k\mathrm{x}^k$). We define

$$f(\mathrm{x}) > 0 \;\Leftrightarrow\; a_k > 0$$

and then for every $f(\mathrm{x}), g(\mathrm{x}) \in \mathbb{R}[\mathrm{x}]$ with $g(\mathrm{x}) \neq 0$ we define

$$\frac{f(\mathrm{x})}{g(\mathrm{x})} \geqslant 0 \;\Leftrightarrow\; f(\mathrm{x})g(\mathrm{x}) \geqslant 0.$$

This is a total order on

$$\mathbb{R}(\mathrm{x}) = \left\{ \frac{f(\mathrm{x})}{g(\mathrm{x})} : f(\mathrm{x}), g(\mathrm{x}) \in \mathbb{R}[\mathrm{x}] \text{ and } g(\mathrm{x}) \neq 0 \right\}$$

which makes $(\mathbb{R}(\mathrm{x}), \leqslant)$ an ordered field.

Remark 1.2. By the definition above

$$f(\mathrm{x}) = \mathrm{x} - r < 0 \qquad \forall\, r \in \mathbb{R},\ r > 0.$$

Therefore the element $\mathrm{x} \in \mathbb{R}(\mathrm{x})$ is such that

$$0 < \mathrm{x} < r \quad \forall\, r \in \mathbb{R},\ r > 0.$$

We can see that there is no other ordering on $\mathbb{R}(\mathrm{x})$ which satisfies the above property:

Proposition 1.3. *Let $\leqslant$ be the ordering on $\mathbb{R}(\mathrm{x})$ defined in 1.1. Then $\leqslant$ is the unique ordering on $\mathbb{R}(\mathrm{x})$ such that*

$$0 < \mathrm{x} < r \quad \forall\, r \in \mathbb{R},\ r > 0.$$

Proof. Assume that $\leqslant$ is an ordering on $\mathbb{R}(\mathrm{x})$ such that

$$0 < \mathrm{x} < r \quad \forall\, r \in \mathbb{R},\ r > 0.$$

Then (see Proposition 2.4 of last lecture)

$$0 < \mathrm{x}^m < r \quad \forall\, m \geqslant 1,\ m \in \mathbb{N},\ \forall\, r > 0,\ r \in \mathbb{R}.$$

Let $f(\mathrm{x}) = a_n\mathrm{x}^n + a_{n-1}\mathrm{x}^{n-1} + \cdots + a_k\mathrm{x}^k \in \mathbb{R}[\mathrm{x}]$ with $k \in \mathbb{N}$ the smallest index such that $a_k \neq 0$. We want to prove that $\mathrm{sign}(f) = \mathrm{sign}(a_k)$.

Let $g(\mathrm{x}) = a_n\mathrm{x}^{n-k} + \cdots + a_{k+1}\mathrm{x} + a_k$. Then $f(\mathrm{x}) = \mathrm{x}^k g(\mathrm{x})$.

If $k = 0$, then $f(\mathrm{x}) = g(\mathrm{x})$. Otherwise $f(\mathrm{x}) \neq g(\mathrm{x})$, and since $\mathrm{sign}(f) = \mathrm{sign}(\mathrm{x}^k)\,\mathrm{sign}(g)$ and $\mathrm{sign}(\mathrm{x}^k) = 1$, it follows that $\mathrm{sign}(f) = \mathrm{sign}(g)$. We want $\mathrm{sign}(g) = \mathrm{sign}(a_k)$.

If $g(\mathrm{x}) = a_k$ we are done. Otherwise let $h(\mathrm{x}) = a_n\mathrm{x}^{n-k-1} + \cdots + a_{k+2}\mathrm{x} + a_{k+1}$. Then $g(\mathrm{x}) = a_k + \mathrm{x}h(\mathrm{x})$ and $h(\mathrm{x}) \neq 0$. Since $|\mathrm{x}^m| < 1$ for every $m \in \mathbb{N}$, we get

$$|h(\mathrm{x})| \leqslant |a_n| + \cdots + |a_{k+1}| := c > 0, \qquad c \in \mathbb{R}.$$

Then

$$|\mathrm{x}h(\mathrm{x})| \leqslant c|\mathrm{x}| < |a_k|,$$

otherwise $|\mathrm{x}| \geqslant \frac{|a_k|}{c}$, contradiction.

Therefore $\mathrm{sign}(g) = \mathrm{sign}(a_k + \mathrm{x}h) = \mathrm{sign}(a_k)$, as required (Note that one needs to verify that $|a| > |b| \Rightarrow \mathrm{sign}(a + b) = \mathrm{sign}(a)$).

□

We now want to classify all orderings on $\mathbb{R}(\mathrm{x})$ which make it into an ordered field. For this we need the notion of Dedekind cuts.

2. Dedekind cuts

Notation 2.1. Let $(\Gamma, \leqslant)$ be a totally ordered set and let $L, U \subseteq \Gamma$. If we write

$$L < U$$

we mean that

$$x < y \quad \forall\, x \in L,\ \forall\, y \in U.$$

(Similarly for $L \leqslant U$)

Definition 2.2. (*Dedekindschnitt*) Let $(\Gamma, \leqslant)$ be a totally ordered set. A **Dedekind cut** of $(\Gamma, \leqslant)$ is a pair (L, U) such that $L, U \subseteq \Gamma$, $L \cup U = \Gamma$ and $L < U$.

Remark 2.3. Since $L < U$ it follows that $L \cap U = \varnothing$. Therefore the subsets L, U form a partition of Γ (The letter "L" stands for "lower cut" and the letter "U" for "upper cut").

Example 2.4. Let $(\Gamma, \leqslant)$ be a totally ordered set. For every $\gamma \in \Gamma$ we can consider the following two Dedekind cuts:

$$\gamma_- := (]-\infty, \gamma[, [\gamma, \infty[)$$
$$\gamma_+ := (]-\infty, \gamma],]\gamma, \infty[)$$

Moreover if we take $L, U \in \{\varnothing, \Gamma\}$, then we have two more cuts:

$$-\infty := (\varnothing, \Gamma), \quad +\infty := (\Gamma, \varnothing)$$

Example 2.5. Consider the Dedekind cut (L, U) of $(\mathbb{Q}, \leqslant)$ given by

$$L = \{x \in \mathbb{Q} : x < \sqrt{2}\} \quad \text{and} \quad U = \{x \in \mathbb{R} : x > \sqrt{2}\}.$$

Then there is no $\gamma \in \mathbb{Q}$ such that $(L, U) = \gamma_-$ or $(L, U) = \gamma_+$.

Definition 2.6. (*trivialen und freie Schnitte*) Let (L, U) be a Dedekind cut of a totally ordered set $(\Gamma, \leqslant)$. If $(L, U) = \pm\infty$ or there is some $\gamma \in \Gamma$ such that $(L, U) = \gamma_+$ or $(L, U) = \gamma_-$ (as defined in 2.4), then (L, U) is said to be a **trivial** (or **realized**) Dedekind cut. Otherwise it is said to be a **free** Dedekind cut (or **gap**).

Remark 2.7. A Dedekind cut (L, U) of a totally ordered set $(\Gamma, \leqslant)$ is free if $L \neq \varnothing$, $U \neq \varnothing$, L has no maximum element and U has no least element.

Definition 2.8. (*Dedekindvollständing*) A totally ordered set $(\Gamma, \leqslant)$ is said to be **Dedekind complete** if for every pair (L, U) of subsets of Γ with $L \neq \varnothing$, $U \neq \varnothing$ and $L \leqslant U$, there exists $\gamma \in \Gamma$ such that

$$L \leqslant \gamma \leqslant U.$$

Exercise 2.9. Show that a totally ordered set $(\Gamma, \leqslant)$ is Dedekind complete if and only if $(\Gamma, \leqslant)$ has no free Dedekind cut.

Examples 2.10.

- The ordered set of the reals $(\mathbb{R}, \leqslant)$ is Dedekind complete, i.e. the set of Dedekind cuts of $(\mathbb{R}, \leqslant)$ is $\{a_\pm : a \in \mathbb{R}\} \cup \{-\infty, +\infty\}$.
- We have already seen in 2.5 that $(\mathbb{Q}, \leqslant)$ is not Dedekind complete. We can generalize 2.5: for every $\alpha \in \mathbb{R} - \mathbb{Q}$ we have the gap given by $(\,]-\infty, \alpha[\cap \mathbb{Q},\ ]\,\alpha, \infty\,[\cap \mathbb{Q})$.

3. The orderings on $\mathbb{R}(\mathrm{x})$

Theorem 3.1. *There is a canonical bijection between the set of the orderings on* $\mathbb{R}(\mathrm{x})$ *and the set of the Dedekind cuts of* $\mathbb{R}$.

Proof. Let $\leqslant$ be an ordering on $\mathbb{R}(\mathrm{x})$. Consider the sets $L = \{v \in \mathbb{R} : v < \mathrm{x}\}$ and $U = \{w \in \mathbb{R} : \mathrm{x} < w\}$. Then $\mathcal{C}_{\mathrm{x}}^{\leqslant} := (L, U)$ is a Dedekind cut of $\mathbb{R}$. (Note that if $\leqslant$ is the order defined in 1.1 then $\mathcal{C}_{\mathrm{x}}^{\leqslant} = 0_+$). So we can define a map

$$\begin{array}{ccc} \{\leqslant : \leqslant \text{ is an ordering on } \mathbb{R}(\mathrm{x})\} & \xrightarrow{f} & \{(L,U) : (L,U) \text{ is a Dedekind cut of } \mathbb{R}\} \\ \leqslant & \mapsto & \mathcal{C}_{\mathrm{x}}^{\leqslant} \end{array}$$

We now want to find a map

$$\{(L,U) : (L,U) \text{ is a Dedekind cut of } \mathbb{R}\} \longrightarrow \{\leqslant : \leqslant \text{ is an ordering on } \mathbb{R}(\mathrm{x})\}$$

which is the inverse of f. Every Dedekind cut of $(\mathbb{R}, \leqslant)$ is of the form $-\infty$, a_-, a_+, $+\infty$, with $a \in \mathbb{R}$. With a change of variable, respectively, $\mathrm{y} := -1/\mathrm{x}$, $\mathrm{y} := a - \mathrm{x}$, $\mathrm{y} := \mathrm{x} - a$, $\mathrm{y} := 1/\mathrm{x}$, we obtain an ordering on $\mathbb{R}(\mathrm{y})$ such that

$$0 < \mathrm{y} < r \quad \forall\, r \in \mathbb{R},\ r > 0.$$

We have seen in 1.3 that there is only one ordering with such a property, so we have a well-defined map from the set of the Dedekind cuts of $(\mathbb{R}, \leqslant)$ into the set of orderings of $\mathbb{R}(\mathrm{x})$. It is precisely the inverse of f.

□

4. Order preserving embeddings

Definition 4.1. (*ordungstreue Einbettung*) Let $(K, \leqslant)$ and $(F, \leqslant)$ be ordered fields. An injective homomorphism of fields

$$\varphi \colon K \hookrightarrow F$$

is said to be an **order preserving embedding** if

$$a \leqslant b \ \Rightarrow\ \varphi(a) \leqslant \varphi(b) \qquad \forall\, a, b \in K.$$

Theorem 4.2 (Hölder)**.** *Let $(K, \leqslant)$ be an Archimedean ordered field. Then there is an order preserving embedding*

$$\varphi \colon K \hookrightarrow \mathbb{R}.$$

Proof. Let $a \in K$. Consider the sets

$$I_a := \,]-\infty, a]_K \cap \mathbb{Q} \quad \text{and} \quad F_a := [a, \infty[_K \cap \mathbb{Q}.$$

Then $I_a \leqslant F_a$ and $I_a \cup F_a = \mathbb{Q}$. So we can define

$$\varphi(a) := \sup I_a = \inf F_a \in \mathbb{R}.$$

Since K is Archimedean, φ is well-defined. Note that

$$I_a + I_b = \{x + y : x \in I_a,\, y \in I_b\} \subseteq I_{a+b}$$

and

$$F_a + F_b \subseteq F_{a+b},$$

then $\varphi(a) + \varphi(b) \leqslant \varphi(a+b)$ and $\varphi(a) + \varphi(b) \geqslant \varphi(a+b)$. This proves that φ is additive. Similarly one gets $\varphi(ab) = \varphi(a)\varphi(b)$.

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (03: 27/10/09)

SALMA KUHLMANN

Contents

1. Preorderings and positive cones

Definition 1.1. (*Präordnung*) Let K be a field and let $T \subseteq K$ such that

(*i*) $T + T \subseteq T$,
(*ii*) $TT \subseteq T$,
(*iii*) $a^2 \in T$ for every $a \in K$.

(where $T + T := \{t_1 + t_2 : t_1, t_2 \in T\}$ and $TT := \{t_1 t_2 : t_1, t_2 \in T\}$).
Then T is said to be a **preordering** (or **cone**) of K.

Definition 1.2. (*echte Präordnung*) A preordering T of a field K is said to be **proper** if $-1 \notin T$.

Definition 1.3. (*Positivkegel*) A proper preordering T of a field K is said to be a **positive cone** if $-T \cup T = K$, where $-T := \{-t : t \in T\}$.

Proposition 1.4. *Let $(K, \leqslant)$ be an ordered field. Then the set*

$$P := \{x \in K : x \geqslant 0\}$$

is a positive cone of K. Conversely, if P is a positive cone of a field K, then $\forall\, x, y \in K$

$$x \leqslant y \;\Leftrightarrow\; y - x \in P$$

defines an ordering on K such that $(K, \leqslant)$ is an ordered field.

Therefore for every field K there is a bijection between the set of the orderings on K and the set of the positive cones of K.

Notation 1.5. Let K be a field. We denote by $\sum K^2$ the set

$$\{a_1^2 + \cdots + a_n^2 : n \in \mathbb{N},\, a_i \in K,\, i = 1, \ldots, n\}.$$

Exercise 1.6. Let K be a field. Then

(1) $\sum K^2$ is a preordering of K.

(2) $\sum K^2$ is the smallest preordering of K, i.e. if T is a preordering of K, then $\sum K^2 \subseteq T$.

(3) If K is real then $-1 \notin \sum K^2$ (i.e. $\sum K^2$ is a proper preordering).

(4) If K is algebraically closed then it is not real.

(5) Let (K, P) be an ordered real field, F a field and

$$\varphi : F \longrightarrow K$$

an homomorphism of fields. Then $Q := \varphi^{-1}(P)$ is an ordering of F (Q is said to be the **pullback** of P).

(6) If P, Q are positive cones of K with $P \subseteq Q$, then $P = Q$.

(7) In particular, if $\sum K^2$ is a positive cone (or ordering: see 1.4) of K, then it is the unique ordering of K.

Remark 1.7. Let K be a field with $\mathrm{char}(K) \neq 2$. If $T \subseteq K$ is a preordering which is not proper (i.e. $-1 \in T$), then $T = K$.

Proof. For every $x \in K$,

$$x = \left(\frac{x+1}{2}\right)^2 + (-1)\left(\frac{x-1}{2}\right)^2 \in T.$$

□

Remark 1.8. Let $\mathcal{T} = \{T_i : i \in I\}$ be a family of preorderings of a field K. Then

(*i*)
$$\bigcap_{i \in I} T_i$$
is a preordering of K.

(*ii*) if $\forall\, i, j \in I\ \exists k \in I$ such that $T_i \cup T_j \subseteq T_k$, then
$$\bigcup_{i \in I} T_i$$
is a preordering of K.

2. A crucial Lemma

Lemma 2.1. *Let K be a field and T a proper preordering of K. If $a \in K$ and $a \notin T$, then*

$$T - aT = \{t_1 - at_2 : t_1, t_2 \in T\}$$

is a proper preordering of K.

Proof. Since $K^2 \subseteq T$, also $K^2 \subseteq T - aT$. Clearly $(T - aT) + (T - aT) \subseteq T - aT$. Moreover $\forall\, t_1, t_2, t_3, t_4 \in T$,

$$(t_1 - at_2)(t_3 - at_4) = t_1t_3 + a^2t_2t_4 - a(t_1t_4 + t_2t_3) \ \in \ T - aT,$$

therefore $(T - aT)(T - aT) \subseteq (T - aT)$ and $T - aT$ is a preordering of K.

If $(T - aT)$ is not proper, then $-1 = t_1 - at_2$ for some $t_1, t_2 \in T$ with $t_2 \neq 0$, since T is proper. Therefore

$$a = \frac{1}{t_2^2}(1 + t_1)t_2 \ \in \ T,$$

contradiction. □

3. Several consequences

Corollary 3.1. *Every maximal proper preordering of a field K is an ordering (positive cone: see 1.4) of K.*

Corollary 3.2. *Every proper preordering of a field K is contained in an ordering of K.*

Proof. Let T be a proper preordering. Let

$$\mathcal{T} = \{\, T' : T' \supseteq T,\ T' \text{ is a proper preordering of } K \,\}.$$

$\mathcal{T}$ is non-empty and for every ascending chain of $\mathcal{T}$

$$T_{i_1} \ \subseteq \ T_{i_2} \ \subseteq \ \ldots \ \subseteq \ T_{i_k} \ \subseteq \ \ldots$$

by 1.8(ii) $\bigcup T_{i_j}$ is a proper preordering containing T and Zorn's Lemma applies.

Let P be a maximal element of $\mathcal{T}$. Then P is a maximal preordering of K containing T, and by 3.1 P is an ordering.

□

Corollary 3.3. *Let T be a proper preordering of a field K. Then*

$$T = \bigcap \{P : T \subseteq P,\ P \textit{ positive cone of } K\}.$$

($\subseteq$) It is obvious.

($\supseteq$) Let $a \in K$ such that a is contained in every positive cone containing T. If $a \notin T$, then by Lemma 2.1 $T - aT$ is a proper preordering of K. By Corollary 3.2, $T - aT$ is contained in a positive cone P of K. Then $-a \in P$ and $a \notin P$.

Corollary 3.4. *(Characterization of real fields) Let K be a field. The following are equivalent:*

(1) *K is real (i.e. K has an ordering).*

(2) *K has a proper preordering.*

(3) *$\sum K^2$ is a proper preordering (i.e. $-1 \notin \sum K^2$).*

(4) $\forall\, n \in \mathbb{N}$, $\forall\, a_1, \ldots, a_n \in K$

$$\sum_{i=1}^{n} a_i^2 = 0 \;\Rightarrow\; a_1 = \cdots = a_n = 0.$$

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) obvious. We show now (3) $\Leftrightarrow$ (4).

($\Rightarrow$) Let $\sum_{i=1}^{n} a_i^2 = 0$ and suppose $a_i \neq 0$ for some $1 \leqslant i \leqslant n$. Say $a_n \neq 0$. Then

$$\frac{a_1^2 + \cdots + a_n^2}{a_n^2} \;=\; 0,$$

and

$$\left(\frac{a_1}{a_n}\right)^2 + \cdots + \left(\frac{a_{n-1}}{a_n}\right)^2 + 1 = 0.$$

Therefore $-1 \in \sum K^2$, contradiction.

($\Leftarrow$) Suppose $-1 \in \sum K^2$, so

$$-1 \;=\; b_1^2 + \cdots + b_s^2,$$

for some $s \in \mathbb{N}$ and $b_1, \ldots, b_s \in K$. Then

$$1 + b_1^2 + \cdots + b_s^2 = 0$$

and $1 = 0$, contradiction.

To complete the proof note that if $-1 \notin \sum K^2$ then $\sum K^2$ is a proper preordering, and by Corollary 3.2 K has an ordering. This proves (3) $\Rightarrow$ (1). □

Corollary 3.5. *(Artin) Let K be a real field. Then*

$$\sum K^2 = \bigcap \{P : P \text{ is an ordering of } K\}.$$

In other words, if K is a real field and $a \in K$, then

$$a \geqslant_P 0 \;\text{ for every ordering } P \;\Leftrightarrow\; a \in \sum K^2.$$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (04: 29/10/09)

SALMA KUHLMANN

Contents

1. Ordering extensions

Definition 1.1. Let L/K be a field extension and P an ordering on K.

An ordering Q of L is said to be an **extension** (*Fortsetzung*) of P if $P \subset Q$ (equivalently $Q \cap K = P$).

Definition 1.2. Let L/K be a field extension and P an ordering on K. We define

$$T_L(P) := \{ \sum_{i=1}^{n} p_i y_i^2 : n \in \mathbb{N},\, p_i \in P,\, y_i \in L \}.$$

Remark 1.3. Let L/K be a field extension and P an ordering on K.

Then $T_L(P)$ is the smallest preordering of L containing P.

Corollary 1.4. *Let L/K be a field extension and P an ordering on K.*

Then P has an extension to an ordering Q of L if and only if $T_L(P)$ is a proper preordering (i.e. if and only if $-1 \notin T_L(P)$).

2. Quadratic extensions

Theorem 2.1. *Let K be a field, $a \in K$ and define $L := K(\sqrt{a})$. Then an ordering P of K extends to an ordering Q of L if and only if $a \in P$.*

Proof.

($\Rightarrow$) Assume Q is an extension of P, then $a = (\sqrt{a})^2 \in Q \cap K = P$.

($\Leftarrow$) Let $a \in P$ (without loss of generality we can assume $L \neq K$ and $\sqrt{a} \notin K$). We show that $T_L(P)$ is a proper preordering (and then the thesis follows by Corollary 1.4).

If not, there is $n \in \mathbb{N}$ and there are $x_1, \ldots, x_n, y_1, \ldots, y_n \in K$, $p_1, \ldots, p_n \in P$ such that

$$-1 = \sum_{i=1}^{n} p_i(x_i + y_i\sqrt{a})^2$$
$$= \sum_{i=1}^{n} p_i(x_i^2 + ay_i^2 + 2x_iy_i\sqrt{a}).$$

On the other hand $-1 \in K$, and since every $x \in K(\sqrt{a})$ can be written in a unique way as $x = k_1 + k_2\sqrt{a}$ with $k_1, k_2 \in K$, it follows that

$$-1 = \sum_{i=1}^{n} p_i(x_i^2 + ay_i^2) \ \in P,$$

contradiction.

□

3. Odd degree field extensions

Theorem 3.1. *Let L/K be a field extension such that $[L : K]$ is finite and odd. Then every ordering of K extends to an ordering of L.*

Proof. Otherwise, let $n \in \mathbb{N}$ the minimal odd degree of a field extension for which the theorem fails.

Let L/K be a finite field extension such that $[L : K] = n$ and let P be an ordering of K not extending to an ordering of L.

Since $\mathrm{char}(K) = 0$ Primitive Element Theorem applies and there is some $\alpha \in L \setminus K$ such that

$$L \ = \ K(\alpha) \ \cong \ K[\mathrm{x}]/(f),$$

where f is the minimal polynomial of α over K. Therefore $\deg(f) = n$, $f(\alpha) = 0$ and for every $g(\mathrm{x}) \in K[\mathrm{x}]$ such that $\deg(g) < n$, we have $g(\alpha) \neq 0$.

By Corollary 1.4, $-1 \in T_L(P)$, so

$$1 + \sum_{i=1}^{s} p_i y_i^2 = 0,$$

where $\forall\, i = 1, \ldots, s \ \ p_i \in P$, $p_i \neq 0$, $y_i \in L$, $y_i \neq 0$. Define

$$y_i = g_i(\alpha),$$

where $\forall\, i = 1, \ldots, s \ \ 0 \neq g_i(\mathrm{x}) \in K[\mathrm{x}]$ and $\deg(g) < n$. Since

$$1 + \sum_{i=1}^{s} p_i g_i(\alpha)^2 = 0,$$

it follows that

$$1 + \sum_{i=1}^{s} p_i g_i(\mathrm{x})^2 = f(\mathrm{x})h(\mathrm{x}), \qquad h(\mathrm{x}) \in K[\mathrm{x}].$$

Define $d := \max\{\deg(g_i) : i = 1, \ldots, s\}$. Then $d < n$ and the polynomial $f(\mathrm{x})h(\mathrm{x})$ has degree $2d$. The coefficient of x^{2d} is of the form

$$\sum_{1=1}^{r} p_i b_i^2,$$

with $p_i \in P$ and $b_i \in K$, $b_i \neq 0$, so

$$\sum_{1=1}^{r} p_i b_i^2 \ >_P \ 0.$$

Note that $\deg(h) = 2d - n < n$ (because $d < n$) and $2d - n$ is odd.

Let $h_1(\mathrm{x})$ be an irreducible factor of $h(\mathrm{x})$ of odd degree and suppose β is a root of $h_1(\mathrm{x})$. Then

$$\deg(h_1) = [K(\beta) : K] < [L : K] = n.$$

Since $h_1(\beta) = 0$, also

$$f(\beta)h(\beta) = 1 + \sum_{i=1}^{s} p_i g_i(\beta)^2 = 0.$$

Therefore $\sum_{i=1}^{s} p_i g_i(\beta)^2 = -1 \ \in T_{K(\beta)}(P)$ and by Corollary 1.4 P does not extend to an ordering of $K(\beta)$. This is in contradiction with the minimality of n. □

4. Real closed fields

Definition 4.1. (*reell abgeschloßer Körper*) A field K is said to be **real closed** if

(1) K is real,
(2) K has no proper real algebraic extension.

Proposition 4.2. *(Artin-Schreier, 1926) Let K be a field. The following are equivalent:*

(*i*) *K is real closed.*
(*ii*) *K has an ordering P which does not extend to any proper algebraic extension.*
(*iii*) *K is real, has no proper algebraic extension of odd degree, and*

$$K \ = \ K^2 \ \cup \ -(K^2).$$

Proof. (*i*) $\Rightarrow$ (*ii*). Trivial.

(*ii*) $\Rightarrow$ (*iii*). Let P be an ordering which does not extend to any proper algebraic extension. By Theorem 3.1, it follows that K has no proper algebraic extension of odd degree.

Let $b \in P$. Then $b = a^2$ for some $a \in K$, otherwise by Theorem 2.1 P extends to an ordering of $K(\sqrt{b})$, which is a proper algebraic extension of K.

Since $K = P \cup (-P)$ and $P = \{a^2 : a \in K\}$, we get (iii).

$(iii) \Rightarrow (i)$. Note $\text{char}(K) = 0$ and $\sqrt{-1} \notin K$ since K is real.
Then $K(\sqrt{-1})$ is the only proper quadratic extension of K: if $b \in K$ but $\sqrt{b} \notin K$ (i.e. b is not a square), then $b = -a^2$ for some $a \neq 0, a \in K$, and $K(\sqrt{b}) = K(\sqrt{-1}\sqrt{a^2}) = K(\sqrt{-1})$.

Claim. Every proper algebraic extension of K contains a proper quadratic subextension.

Note that if Claim is established we are done: indeed it follows that no proper extension can be real since -1 is a square in it.

Let L/K a proper algebraic extension. Without loss of generality assume that $[L : K]$ is finite and so even. By Primitive Element Theorem we can further assume that L' is a Galois extension.

Let $G = \text{Gal}(L/K)$, $|G| = [L : K] = 2^a m$, $a \geqslant 1$, m odd. Let S be a 2-Sylow subgroup of G (i.e. $|S| = 2^a$) and let $E := \text{Fix}(S)$. By Galois correspondence we get:

$$[E : K] = [G : S] = m \qquad \text{odd.}$$

Therefore by assumption (iii) we must have $[E : K] = [G : S] = 1$, so $G = S$ is a 2-group ($|G| = 2^a$) and it has a subgroup G_1 of index 2. By Galois correspondence, defining $F_1 := \text{Fix}(G_1)$ we get a quadratic subextension of L/K. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (05: 03/11/09)

SALMA KUHLMANN

Contents

1. Real closed fields

We first recall Artin-Schreier characterization of real closed fields:

Proposition 1.1. *(Artin-Schreier, 1926) Let K be a field. The following are equivalent:*

(*i*) *K is real closed.*
(*ii*) *K has an ordering P which does not extend to any proper algebraic extension.*
(*iii*) *K is real, has no proper algebraic extension of odd degree, and*

$$K = K^2 \cup -(K^2).$$

Corollary 1.2. *If K is a real closed field then*

$$K^2 = \{a^2 : a \in K\}$$

is the unique ordering of K.

Proof. Since K is a real closed field, by (*ii*) it has an ordering P which does not extend to any proper algebraic extension.

Let $b \in P$. Then $b = a^2$ for some $a \in K$, otherwise P extends to an ordering of $K(\sqrt{b})$, which is a proper algebraic extension of K.

Therefore $P = K^2$. □

Remark 1.3. We denote by $\sum K^2$ the unique ordering of a real closed field K, even though we know that $\sum K^2 = K^2$, to avoid any confusion with the cartesian product $K \times K$.

Corollary 1.4. *Let $(K, \leqslant)$ be an ordered field. Then K is real closed if and only if*

(*a*) *every positive element in K has a square root in K, and*
(*b*) *every polynomial of odd degree has a root in K.*

Examples 1.5. $\mathbb{R}$ is real closed and $\mathbb{Q}$ is not.

2. The algebraic closure of a real closed field

Lemma 2.1. *(Hilfslemma) If K is a field such that K^2 is an ordering of K, then every element of $K(\sqrt{-1})$ is a square.*

Proof. Let $x = a + \sqrt{-1}\, b \in K(\sqrt{-1}) := L$, $a, b \in K$, $b \neq 0$. We can suppose $b > 0$. We want to find $y \in L$ such that $x = y^2$.

K^2 is an ordering $\Rightarrow$ $a^2 + b^2 \in K^2$. Let $c \in K$, $c \geqslant 0$ such that

$$a^2 + b^2 = c^2.$$

Since $a^2 \leqslant a^2 + b^2 = c^2$, $|a| \leqslant c$, so $c + a \geqslant 0$, $c - a \geqslant 0$ ($-c \leqslant a \leqslant c$).

Therefore $\frac{1}{2}(c \pm a) \in K^2$. Let $d, e \in K$, $d, e \geqslant 0$ such that

$$\frac{1}{2}(c + a) = d^2$$

$$\frac{1}{2}(c - a) = e^2.$$

So

$$d = \frac{\sqrt{c+a}}{\sqrt{2}} \qquad e = \frac{\sqrt{c-a}}{\sqrt{2}}$$

Now set $y := d + e\sqrt{-1}$. Then

$$\begin{aligned} y^2 &= (d + e\sqrt{-1})^2 \\ &= d^2 + (e\sqrt{-1})^2 + 2de\sqrt{-1} \\ &= \frac{1}{2}(c + a) - \frac{1}{2}(c - a) + 2\frac{1}{2}\sqrt{(c-a)(c+a)}\sqrt{-1} \\ &= \frac{1}{2}a + \frac{1}{2}a + \sqrt{c^2 - a^2}\sqrt{-1} \\ &= a + \sqrt{b^2}\sqrt{-1} \\ &= a + b\sqrt{-1} \\ &= x. \end{aligned}$$

□

Theorem 2.2. *(Fundamental Theorem of Algebra) If K is a real closed field then $K(\sqrt{-1})$ is algebraically closed.*

Proof. Let $L \supseteq K(\sqrt{-1})$ be an algebraic extension of $K(\sqrt{-1})$. We show $L = K(\sqrt{-1})$.

Set $G := \mathrm{Gal}(L/K)$. Then $[L : K] = |G| = 2^a m$, $a \geqslant 1$, m odd.

Let $S < G$ be a 2-Sylow subgroup ($|S| = 2^a$), and $F := \mathrm{Fix}(S)$. We have

$$[F : K] = [G : S] = m \qquad \text{odd.}$$

Since K is real closed, it follows that $m = 1$, so $G = S$ and $|G| = 2^a$. Now

$$[L : K(\sqrt{-1})][K(\sqrt{-1}) : K] = [L : K] = 2^a.$$

Therefore $[L : K(\sqrt{-1})] = 2^{a-1}$. We claim that $a = 1$.

If not, set $G_1 := \mathrm{Gal}(L/K(\sqrt{-1}))$, let S_1 be a subgroup of G_1 of index 2, and $F_1 := \mathrm{Fix}(S_1)$. So

$$[F_1 : K(\sqrt{-1})] = [G_1 : S_1] = 2,$$

and F_1 is a quadratic extension of $K(\sqrt{-1})$. But every element of $K(\sqrt{-1})$ is a square by Lemma 2.1, contradiction. □

Notation. We denote by $\bar{K}$ the algebraic closure of a field K, i.e. the smallest algebraically closed field containing K.

We have just proved that if K is real closed then $\bar{K} = K(\sqrt{-1})$.

3. Factorization in $R[\mathrm{x}]$

Corollary 3.1. *(Irreducible elements in $R[\mathrm{x}]$ and prime factorizaction in $R[\mathrm{x}]$). Let R be a real closed field, $f(\mathrm{x}) \in R[\mathrm{x}]$. Then*

(1) *if $f(\mathrm{x})$ is monic and irreducible then*

$$f(\mathrm{x}) = \mathrm{x} - a \quad \textit{or} \quad f(\mathrm{x}) = (\mathrm{x} - a)^2 + b^2, \quad b \neq 0;$$

(2)

$$f(\mathrm{x}) = d \prod_{i=1}^{n} (\mathrm{x} - a_i) \prod_{j=1}^{m} (\mathrm{x} - d_j)^2 + b_j^2, \quad b_j \neq 0.$$

Proof. Let $f(\mathrm{x}) \in R[\mathrm{x}]$ be monic and irreducible. Then $\deg(f) \leqslant 2$.

Suppose not, and let $\alpha \in \bar{R}$ a root of $f(\mathrm{x})$. Then

$$[R(\alpha) : R] = \deg(f) > 2.$$

On the other hand, by 2.2

$$[R(\alpha) : R] \leqslant [\bar{R} : R] = 2,$$

contradiction.

If $\deg(f) = 1$, then $f(\mathrm{x}) = \mathrm{x} - a$, for some $a \in R$.

If $\deg(f) = 2$, then $f(\mathrm{x}) = \mathrm{x}^2 - 2a\mathrm{x} + c = (\mathrm{x} - a)^2 + (c - a^2)$, for some $a, c \in R$.

We claim that $c - a^2 > 0$. If not,

$$c - a^2 \leqslant 0 \;\Rightarrow\; -(c - a^2) \geqslant 0 \;\Rightarrow\; a^2 - c \geqslant 0,$$

the discriminant $4(a^2 - c) \geqslant 0$, $f(\mathrm{x})$ has a root in R and factors, contradiction.

Therefore $(c - a^2) \in R^2$ and there is $b \in R$ such that $(c - a^2) = b^2 \neq 0$.

□

Corollary 3.2. *(Zwischenwertsatz : Intermediate value Theorem) Let R be a real closed field, $f(\mathrm{x}) \in R[\mathrm{x}]$. Assume $a < b \in R$ with $f(a) < 0 < f(b)$. Then $\exists\, c \in R$, $a < c < b$ such that $f(c) = 0$.*

Proof. By previous Corollary,

$$\begin{aligned} f(\mathrm{x}) &= d \prod_{i=1}^{n} (\mathrm{x} - a_i) \prod_{j=1}^{m} (\mathrm{x} - d_j)^2 + b_j^2 \\ &= d \prod_{i=1}^{n} l_i(\mathrm{x}) q(\mathrm{x}), \end{aligned}$$

where $l_i(\mathrm{x}) := \mathrm{x} - a_i$, $\forall\, i = 1, \ldots, n$ and $q(\mathrm{x}) := \prod_{j=1}^{m} (\mathrm{x} - d_j)^2 + b_j^2$.

We claim that there is some $k \in \{1, \ldots, n\}$ such that $l_k(a) l_k(b) < 0$. Since

$$\operatorname{sign}(f) = \operatorname{sign}(d) \prod_{i=1}^{n} \operatorname{sign}(l_i) \operatorname{sign}(q) \quad \text{and} \quad \operatorname{sign}(q) = 1,$$

if we had that

$$\operatorname{sign}(l_i(a)) = \operatorname{sign}(l_i(b)) \quad \forall\, i \in \{1, \ldots, n\},$$

we would have

$$\operatorname{sign}(f(a)) = \operatorname{sign}(f(b)),$$

in contradiction with $f(a) f(b) < 0$.

For such a k,

$$l_k(a) < 0 < l_k(b),$$

i.e.

$$a - a_k < 0 < b - a_k,$$

and $c := a_k \in\,]a, b[$ is a root of $f(\mathrm{x})$. □

Corollary 3.3. *(Rolle) Let R be a real closed field, $f(\mathrm{x}) \in R[\mathrm{x}]$, Assume that $a, b \in R$, $a < b$ and $f(a) = f(b) = 0$. Then $\exists\, c \in R$, $a < c < b$ such that $f'(c) = 0$.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (06: 05/11/09)

SALMA KUHLMANN

Contents

Let R be a real closed field (for all this lecture).

1. Counting roots in an interval

Definition 1.1. Let $f(\mathrm{x}) \in R[\mathrm{x}]$, $a \in R$,

$$f(\mathrm{x}) = (\mathrm{x} - a)^m h(\mathrm{x})$$

with $m \in \mathbb{N}$, $m \geqslant 1$ and $h(a) \neq 0$ (i.e. $(\mathrm{x} - a)$ is not a factor of $h(\mathrm{x})$).

We say that m is the **multiplicity** (*Vielfachheit*) of f at a.

Corollary 1.2. *(Generalized Intermediate Value Theorem: Verstärkung Zwischenwertsatz). Let $f(\mathrm{x}) \in R[\mathrm{x}]$; $a, b \in R$, $a < b$, $f(a)f(b) < 0$ (i.e. $f(a) < 0 < f(b)$ or $f(b) < 0 < f(a)$). Then the number of roots of $f(\mathrm{x})$ counting multiplicities in the interval $]a, b[\subseteq R$ is odd (in particular, f has a root in $]a, b[$).*

Proof. By Corollary 3.1 of 5th lecture (3/11/09), we can write

$$f(\mathrm{x}) = \prod_{i=1}^{n} (\mathrm{x} - c_i)^{m_i} g(\mathrm{x})$$

with $g(\mathrm{x}) = dq(\mathrm{x})$, where $d \in R$ is the leading coefficient of $f(\mathrm{x})$ and $q(\mathrm{x})$ is the product of the irreducible quadratic factors of $f(\mathrm{x})$.

Note that $g(\mathrm{x})$ has constant sign on R (i.e. $g(r) > 0 \ \forall\, r \in R$ or $g(r) < 0 \ \forall\, r \in R$). Without loss of generality, we can suppose $d = 1$ (and so $g(\mathrm{x})$ is positive everywhere).

Set $\forall\, i = 1, \ldots, n$

$$\begin{cases} L_i(\mathrm{x}) := (\mathrm{x} - c_i)^{m_i} \\ l_i(\mathrm{x}) := \mathrm{x} - c_i. \end{cases}$$

If $l_i(\mathrm{x})$ changes sign in $]a, b[$ we must have $l_i(a) < 0 < l_i(b)$. Note that $L_i(\mathrm{x})$ changes sign in $]a, b[$ if and only if $l_i(\mathrm{x})$ does and m_i is odd.

In particular if $L_i(\mathrm{x})$ changes sign we must have $L_i(a) < 0 < L_i(b)$ as well.

Let us count the number of distinct $i \in \{1, \dots, n\}$ for which $L_i(a) < 0 < L_i(b)$. We claim that this number must be odd. If not, we get an even number of i such that $L_i(a)L_i(b) < 0$, so their product would be positive, in contradiction with the fact that $f(a)f(b) < 0$.

Set

$$|\{i \in \{1, \dots, n\} : L_i(a) < 0 < L_i(b)\}| = M \geqslant 1 \qquad \text{odd.}$$

Say these are $L_1, \dots, L_M$. So the total number of roots of f in $]a, b[$ counting multiplicity is

$$\sum := m_1 + \cdots + m_M.$$

Since m_i is odd $\forall\, i = 1, \dots, M$ and M is odd, it follows that $\sum$ is odd as well.

□

2. Bounding the roots

Corollary 2.1. *Let* $f(\mathrm{x}) \in R[\mathrm{x}]$, $f(\mathrm{x}) = d\mathrm{x}^m + d_{m-1}\mathrm{x}^{m-1} + \cdots + d_0$. *Set*

$$D := 1 + \sum_{i=m-1}^{0} \left| \frac{d_i}{d} \right| \in R.$$

Then

(*i*) $a \in R$, $f(a) = 0 \;\Rightarrow\; |a| < D$;
(*i.e. f has no root in* $]-\infty, -D] \cup [D + \infty[$)

(*ii*) $y \in [D, +\infty[\;\Rightarrow\; \operatorname{sign}(f(y)) = \operatorname{sign}(d)$;

(*iii*) $y \in]-\infty, -D[\;\Rightarrow\; \operatorname{sign}(f(y)) = (-1)^m \operatorname{sign}(d)$.

Proof.

(*i*) For every $i = 0, \dots, m-1$ set $b_i := \frac{d_i}{d}$ and compute for $|y| \geqslant D$:

$$f(y) = dy^m(1 + b_{m-1}y^{-1} + \cdots + b_0 y^{-m}).$$

Now

$$|b_{m-1}y^{-1} + \cdots + b_0 y^{-m}| \leqslant (|b_{m-1}| + \cdots + |b_0|)D^{-1} < 1.$$

(*ii*) If $y \geqslant D$ then $f(y) = d\prod(y - a_i)^{m_i} q(y)$ where $\deg(q)$ is even and $y - a_i > 0$.

(*iii*) If $y \leqslant -D$ then $(y - a_i)^{m_i} < 0$ if and only if m_i is odd. Moreover m is odd if and only if $\sum m_i$ is odd.

□

Corollary 2.2. *(Rolle's Satz) Let* $f(\mathrm{x}) \in R[\mathrm{x}]$, $a < b \in R$ *such that* $f(a) = f(b)$. *Then there is* $c \in R$, $a < c < b$ *such that* $f'(c) = 0$.

Proof. We can suppose $f(a) = f(b) = 0$ (otherwise if $f(a) = f(b) = k \neq 0$, we can consider the polynomial $(f - k)(\mathrm{x})$).

We can also assume that $f(\mathrm{x})$ has no root in $]a, b[$. So

$$f(\mathrm{x}) = (\mathrm{x} - a)^m(\mathrm{x} - b)^n g(\mathrm{x}),$$

where $g(\mathrm{x})$ has no root in $[a, b]$, and by Corollary 1.2 (IVT) $g(\mathrm{x})$ has constant sign in $[a, b]$. Compute

$$f'(\mathrm{x}) = (\mathrm{x} - a)^{m-1}(\mathrm{x} - b)^{n-1} g_1(\mathrm{x}),$$

where

$$g_1(\mathrm{x}) := m(\mathrm{x} - b)g(\mathrm{x}) + n(\mathrm{x} - a)g(\mathrm{x}) + (\mathrm{x} - a)(\mathrm{x} - b)g'(\mathrm{x}).$$

Therefore

$$g_1(a) = m(a - b)g(a)$$
$$g_1(b) = n(b - a)g(b).$$

Since $g_1(a)g_1(b) < 0$, by the Intermediate Value Theorem (1.2) $g_1(\mathrm{x})$ has a root in $]a, b[$ and so does $f'(\mathrm{x})$. □

Corollary 2.3. *(Mittelwertsatz: Mean Value Theorem) Let $f(\mathrm{x}) \in R[\mathrm{x}]$, $a < b \in R$. Then there is $c \in R$, $a < c < b$ such that*

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

Proof. We can apply Rolle's Satz to

$$F(\mathrm{x}) := f(\mathrm{x}) - (\mathrm{x} - a)\frac{f(b) - f(a)}{b - a},$$

since $F(a) = F(b)$. □

Corollary 2.4. *(Monotonicity Theorem). Let $f(\mathrm{x}) \in R[\mathrm{x}]$, $a < b \in R$. If f' is positive (respectively negative) on $]a, b[$, then f is strictly increasing (respectively strictly decreasing) on $[a, b]$.*

Proof. If $a \leqslant a_1 < b_1 \leqslant b$, by the Mean Value Theorem there is some $c \in R$, $a_1 < c < b_1$ such that

$$f'(c) = \frac{f(b_1) - f(a_1)}{b_1 - a_1}.$$

□

3. Changes of sign

Definition 3.1.

(*i*) Let $(c_1, \ldots, c_n)$ a finite sequence in R. An index $i \in \{1, \ldots, n\}$ is a **change of sign** (*Vorzeichenwechsel*) if $c_i c_{i+1} < 0$.

(*ii*) Let $(c_1, \ldots, c_n)$ a finite sequence in R. After we have removed all zero's by the sequence, we define

$$\begin{aligned} \mathrm{Var}(c_1, \ldots, c_n) :&= |\{i \in \{1, \ldots, n\} : i \text{ is a change of sign}\}| \\ &= |\{i \in \{1, \ldots, n\} : c_i c_{i+1} < 0\}|. \end{aligned}$$

Theorem 3.2. *(Lemma von Descartes) Let* $f(\mathrm{x}) = a_n \mathrm{x}^n + \cdots + a_0 \in R[\mathrm{x}]$, $a_n \neq 0$. *Then*

$$|\{a \in R : a > 0 \text{ and } f(a) = 0\}| \ \leqslant \ \mathrm{Var}(a_n, \ldots, a_1, a_0).$$

Proof. By induction on $n = \deg(f)$. The case $n = 1$ is obvious, so suppose $n > 1$.

Let r be the smallest index such that $a_r \neq 0$. By induction applied to

$$f'(\mathrm{x}) = n a_n \mathrm{x}^{n-1} + \cdots + r a_r \mathrm{x}^{r-1},$$

we know that there are $\mathrm{Var}(n a_n, \ldots, r a_r) = \mathrm{Var}(a_n, \ldots, a_r)$ many positive roots of f'. Set $c :=$ the smallest such positive root of f' (by convention $c := +\infty$ if none exists)

Apply Rolle's Theorem: f has at most $1 + \mathrm{Var}(a_n, \ldots, a_r)$ positive roots.

Case 1. If the number of positive roots of f is strictly less than $1 + \mathrm{Var}(a_n, \ldots, a_r)$, then the number of positive roots of f is $\leqslant \mathrm{Var}(a_n, \ldots, a_r) \leqslant \mathrm{Var}(a_n, \ldots, a_r, a_0)$ and we are done.

Case 2. Assume f has exactly $1 + \mathrm{Var}(a_n, \ldots, a_r)$ positive roots. We claim that in this case

$$1 + \mathrm{Var}(a_n, \ldots, a_r) = \mathrm{Var}(a_n, \ldots, a_r, a_0).$$

We observe that f has a root a in $]0, c[$.

For $0 < x \leqslant c$ we have that $\mathrm{sign}(f'(x)) = \mathrm{sign}(a_r) \neq 0$, so f is strictly monotone in the interval $[0, c]$ (Monotonicity Theorem). So

$$\begin{aligned} a_r > 0 \ &\Rightarrow \ a_0 = f(0) < f(a) = 0 \ \Rightarrow \ a_0 < 0, \\ a_r < 0 \ &\Rightarrow \ a_0 = f(0) > f(a) = 0 \ \Rightarrow \ a_0 > 0. \end{aligned}$$

In both cases $a_0 a_r < 0$ and the claim is established. □

Corollary 3.3. *Let* $f(\mathrm{x}) \in R[\mathrm{x}]$ *a polynomial with* m *monomials. Then* f *has at most* $2m - 1$ *roots in* R.

Proof. Consider $f(\mathrm{x})$ and $f(-\mathrm{x})$. By previous Theorem they have both at most $m-1$ strictly positive roots in R. So $f(\mathrm{x})$ has at most $2m-2$ non-zero roots and therefore at most $2m - 1$ roots in R. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (07: 10/11/09)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Sturm's Theorem

Definition 1.1.

(*i*) Let $f \in R[\mathrm{x}]$ be a non-constant polynomial, $\deg(f) \geqslant 1$. The **Sturm sequence** of f is defined recursevely as a sequence $(f_0, \ldots, f_r)$ of polynomials in $R[\mathrm{x}]$ such that:

$$\begin{aligned} f_0 &:= f, \qquad f_1 := f' \qquad \textit{and} \\ f_0 &= f_1 q_1 - f_2 \\ f_1 &= f_2 q_2 - f_3 \\ &\ldots \\ f_{i-1} &= f_i q_i - f_{i+1} \\ &\ldots \\ f_{r-2} &= f_{r-1} q_{r-1} - f_r \\ f_{r-1} &= f_r q_r, \end{aligned}$$

where $f_i, q_i \in R[\mathrm{x}]$, $f_i \neq 0$ and $\deg(f_i) < \deg(f_{i-1})$.

(*ii*) Let $x \in R$. Set

$$V_f(x) := \mathrm{Var}(f_0(x), \ldots, f_r(x)).$$

We recall that after we have removed all zero's by the sequence $(c_1, \ldots, c_n)$, we defined $\mathrm{Var}(c_1, \ldots, c_n)$ as the number of changes of sign in $(c_1, \ldots, c_n)$, i.e.

$$\mathrm{Var}(c_1, \ldots, c_n) = |\{i \in \{1, \ldots, n\} : c_i c_{i+1} < 0\}|.$$

Theorem 1.2. *(Sturm 1829). Let $a, b \in R$, $a < b$, $f(a)f(b) \neq 0$. Then*

$$|\{c : a \leqslant c \leqslant b\,,\ f(c) = 0\}| \ = \ V_f(a) - V_f(b).$$

Proof. For the proof we study the function $V_f(x)$, $x \in R$, locally constant except around finitely many roots for $f_0, \ldots, f_r$.

(1) Suppose $\gcd(f_0, f_1) = 1$.

(2) Hilfslemma $\Rightarrow$ $\exists\, \delta$ such that

$$|x-c| < \delta \;\Rightarrow\; \operatorname{sign}(f_0(x)f_1(x)) = \operatorname{sign}(x-c) = \begin{cases} -1 & \text{if } x < c \\ 0 & \text{if } x = c \\ 1 & \text{if } x > c. \end{cases}$$

(3) $\forall\, i \in \{1, \ldots, r-1\}$: $\gcd(f_{i-1}, f_i) = 1$ and

$$f_{i-1} = q_i f_i - f_{i+1}, \qquad \text{with } f_{i+1} \neq 0.$$

So if $f_i(c) = 0$ then

$$f_{i-1}(c)f_{i+1}(c) < 0.$$

(4) Let $f_i(c) = 0$ for $i \in \{0, \ldots, r-1\}$. Then $f_{i+1}(c) \neq 0$ (so $\operatorname{sign}(f_{i+1}(c)) = \pm 1$).

We shall now compare for $f_i(c) = 0$, $i \in \{0, \ldots, r-1\}$

$$\operatorname{sign}(f_i(x)) \qquad \operatorname{sign}(f_{i+1}(x))$$

for $|x-c| < \delta$ and count.

We first examine the case $i = 0$.

Observe that $\operatorname{sign}(f_1(x)) \neq 0$ $\forall\, x$ such that $|x-c| < \delta$ because of Hilfslemma. So in particular $\operatorname{sign}(f_1(x))$ is constant for $|x-c| < \delta$ and it is equal to $\operatorname{sign}(f_1(c))$:

	$x \to c_-$	$x = c$	$x \to c_+$
$f_0(x)$	$-\operatorname{sign}(f_1(c))$	0	$\operatorname{sign}(f_1(c))$
$f_1(x)$	$\operatorname{sign}(f_1(c))$	$\operatorname{sign}(f_1(c))$	$\operatorname{sign}(f_1(c))$
contribution to $V_f(x)$	1	0	0

Now consider $i \in \{1, \ldots, r-1\}$ and use (2), i.e.

$$f_i(d) = 0 \implies f_{i-1}(d)f_{i+1}(d) < 0:$$

	$x \to d_-$	$x = d$	$x \to d_+$
$f_{i-1}(x)$	$-\operatorname{sign}(f_{i+1}(d))$	$-\operatorname{sign}(f_{i+1}(d))$	$-\operatorname{sign}(f_{i+1}(d))$
$f_i(x)$		0	
$f_{i+1}(x)$	$\operatorname{sign}(f_{i+1}(d))$	$\operatorname{sign}(f_{i+1}(d))$	$\operatorname{sign}(f_{i+1}(d))$
contribution to $V_f(x)$	1	1	1

Therefore for $a < b$, $V_f(a) - V_f(b)$ is the number of roots of f in $]a, b[$.

Let us consider now the general case. Set

$$g_i := f_i / f_r \qquad i = 0, \ldots, r.$$

The sequence of polynomials $(g_0, \ldots, g_r)$ satisfies the previous conditions $(1) - (4)$. We can conclude by noticing that:

(*i*) $\mathrm{Var}(g_0(x), \ldots, g_r(x)) = \mathrm{Var}(f_0(x), \ldots, f_r(x))$ (because $f_i(x) = f_r(x)g_i(x)$),

(*ii*) $f = f_0$ and $g_0 = f/f_r$ have the same zeros ($f_r = \gcd(f, f')$, so $g = f/f_r$ has only simple roots, whereas f has roots with multiplicities.)

□

For $i = 0, \ldots, r$ set $d_i := \deg(f_i)$ and $\varphi_i :=$ the leading coefficient of f_i. Set

$$V_f(-\infty) := \mathrm{Var}((-1)^{d_0}\varphi_0,\ (-1)^{d_1}\varphi_1, \ldots, (-1)^{d_r}\varphi_r)$$
$$V_f(+\infty) := \mathrm{Var}(\varphi_0, \varphi_1, \ldots, \varphi_r).$$

Then we have:

Corollary 1.3. *The number of distinct roots of f is $V_f(-\infty) - V_f(+\infty)$.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (08: 12/11/09)

SALMA KUHLMANN

Contents

1. Real closure

Definition 1.1. Let (K, P) be an ordered field. R is a real closure of (K, P) if

(1) R is real closed,
(2) $R \supseteq K$, $R \,|\, K$ is algebraic,
(3) $P = \sum R^2 \cap K$ (i.e. the order on K is the restriction of the unique order R to K).

Theorem 1.2. *Every ordered field (K, P) has a real closure.*

Proof. Apply Zorn's Lemma to

$$\mathcal{L} := \{(L, Q) : L \,|\, K \text{ algebraic}, \ Q \cap K = P\}.$$

□

Proposition 1.3. *(Corollary to Sturm's Theorem) Let K be a field. Let R_1, R_2 be two real closed fields such that*

$$K \subseteq R_1 \quad \textit{and} \quad K \subseteq R_2$$

with

$$P := K \ \cap \ \sum R_1^2 = K \ \cap \ \sum R_2^2$$

(i.e. R_1 and R_2 induce the same ordering P on K).

Let $f(\mathrm{x}) \in K[\mathrm{x}]$; then the number of roots of $f(\mathrm{x})$ in R_1 is equal to the number of roots of $f(\mathrm{x})$ in R_2.

2. Order preserving extensions

Proposition 2.1. *Let (K, P) be an ordered field. Let R be a real closed field containing (K, P). Let $K \subseteq L \subseteq R$ be such that $[L : K] < \infty$. Let S be a real closed field with*

$$\varphi\colon (K, P) \ \hookrightarrow \ (S, \ \sum S^2)$$

an order preserving embedding. Then φ extends to an order preserving embedding

$$\psi\colon (L, \ \sum R^2 \cap L) \ \hookrightarrow \ (S, \sum S^2).$$

Proof. We recall that if (K, P) and (L, Q) are ordered fields, a field homomorphism $\varphi\colon K \longrightarrow L$ is called **order preserving** with respect to P and Q if $\varphi(P) \subseteq Q$ (equivalently $P = \varphi^{-1}(Q)$).

By the Theorem of the Primitive Element $L = K(\alpha)$.

Consider $f = MinPol(\alpha \,|\, K)$. Since $\alpha \in R$, $\varphi(f)$ has at least one root β in S,

$$L := K(\alpha) \quad \overset{\psi}{\longleftrightarrow} \quad \varphi(K)(\beta),$$

so there is at least one extension of φ from K to L.

Let $\psi_1, \ldots, \psi_r$ all such extensions of φ to $L = K(\alpha)$, and for a contradiction assume that none of them is order preserving with respect to $Q = L \cap \sum R^2$. Then $\exists\, b_1, \ldots, b_r \in L$, $b_i > 0$ (in R) and $\psi_i(b_i) < 0$ (in S) $\forall\, i = 1, \ldots, r$.

Consider $L' := L(\sqrt{b_1}, \ldots, \sqrt{b_r}) \subset R$. Since $[L : K] < \infty$, also $[L', K] < \infty$.

So let τ be an extension of φ from K to L'. In particular $\tau_{|_L}$ is one of the ψ_i's. Say $\tau_{|_L} = \psi_1$.

Now compute for $b_1 \in L$,

$$\psi_1(b_1) = \tau(b_1) = \tau((\sqrt{b_1})^2) = (\tau(\sqrt{b_1}))^2 \in \sum S^2,$$

in contradiction with the fact that $\psi_1(b_1) < 0$.

□

Theorem 2.2. *Let (K, P) be an ordered field and $(R, \sum R^2)$ be a real closure of (K, P). Let $(S, \sum S^2)$ be a real closed field and assume that*

$$\varphi\colon (K, P) \ \hookrightarrow \ (S, \ \sum S^2)$$

is an order preserving embeding. Then φ has a uniquely determined extension

$$\psi\colon (R, \ \sum R^2) \ \hookrightarrow \ (S, \ \sum S^2).$$

Proof. Consider

$$\mathcal{L} := \{(L, \psi) : \ K \subset L \subset R; \ \psi\colon L \hookrightarrow S, \ \psi_{|_K} = \varphi\}.$$

Let (L, ψ) be a maximal element. Then by Proposition 2.1 we must have $L = R$.

Therefore we have an order preserving embedding ψ of R extending φ

$$\psi\colon R \hookrightarrow S.$$

We want to prove that ψ is unique. We show that $\psi(\alpha) \in S$ is uniquely determined for every $\alpha \in R$.

Let $f = PolMin(\alpha \,|\, K)$ and let $\alpha_1 < \cdots < \alpha_r$ all the real roots of f in R. Let $\beta_1 < \cdots < \beta_r$ be all the real roots of f in S. Since $\psi\colon R \hookrightarrow S$ is order preserving, we must have $\psi(\alpha_i) = \beta_i$ for every $i = 1, \ldots, r$. In particular $\alpha = \alpha_j$ for some $1 \leqslant j \leqslant r$ and $\psi(\alpha) = \beta_j \in S$. □

Corollary 2.3. *Let (K, P) be an ordered field, R_1, R_2 two real closures of (K, P). Then exists a unique*

$$\varphi\colon R_1 \longrightarrow R_2$$

K-isomorphism (i.e. with $\varphi_{|_K} = id$).

Corollary 2.4. *Let R be a real closure of (K, P). Then the only K-automorphism of R is the identity.*

Corollary 2.5. *Let R be a real closed field, $K \subseteq R$ a subfield. Set $P := K \cap \sum R^2$ the induced order. Then*

$$K^{ralg} = \{\alpha \in R : \alpha \text{ is algebraic over } K\}$$

is relatively algebraic closed in R and is a real closure of (K, P).

Proof. It is enough to show that K^{ralg} is real closed.

K^{ralg} is real because $Q := K^{ralg} \cap \sum R^2$ is an induced ordering.

Let $a \in Q$, $a = b^2$, $b \in R$. So $p(\mathrm{x}) = \mathrm{x}^2 - a \in K^{ralg}[\mathrm{x}]$ has a root in R.

One can see that b is algebraic over K (so $b \in K^{ralg}$).

Similarly one shows that every odd polynomial with coefficients in K^{ralg} has a root in K^{ralg}. □

Corollary 2.6. *Let (K, P) be an ordered field, S a real closed field and $\varphi\colon (K, P) \hookrightarrow S$ an order preserving embedding. Let $L \,|\, K$ an algebraic extension. Then there is a bijective correspondence*

$$\{\text{extensions } \psi\colon L \to S \text{ of } \varphi\} \longrightarrow \{\text{extensions } Q \text{ of } P \text{ to } L\}$$

$$\psi \mapsto \psi^{-1}(\sum S^2)$$

Proof.

(⇒) Let $\psi\colon L \hookrightarrow S$ an extension of φ. Then indeed $Q := \psi^{-1}(\sum S^2)$ is an ordering on L. Furthermore $\psi^{-1}(\sum S^2) \cap K = \varphi^{-1}(\sum S^2) = P$. So the extension ψ induces the extension Q.

($\Leftarrow$) Conversely assume that Q is an extension of P from K to L ($Q \cap K = P$). Note that if R is a real closure of (L, Q) then R is a real closure of (K, P) as well.

Now apply Theorem 2.2 to extend φ to $\sigma\colon R \to S$. Set $\psi := \sigma_{|_L}$ which is order preserving with respect to Q. So the map is well-defined and surjective. To see that it is also injective, assume

$$\psi_1\colon L \longrightarrow S, \quad \psi_2\colon L \longrightarrow S, \quad \psi_{1_{|_K}} = \psi_{2_{|_K}} = \varphi$$

which induce the same order

$$Q = \psi_1^{-1}(\sum S^2) = \psi_2^{-1}(\sum S^2)$$

on L. Let R be the real closure of (L, Q). Apply Theorem 2.2 to ψ_1 and ψ_2 to get uniquely determined extensions

$$\sigma_1\colon R \longrightarrow S, \quad \sigma_2\colon R \longrightarrow S,$$

of ψ_1 and ψ_2 respectively.

But now $\sigma_{1_{|_K}} = \sigma_{2_{|_K}} = \varphi$. By the uniqueness part of Theorem 2.2 we get $\sigma_1 = \sigma_2$ and a fortiori $\psi_1 = \psi_2$.

□

Corollary 2.7. *Let (K, P) be an ordered field, R a real closure, $[L : K] < \infty$. Let $L = K(\alpha)$, $f = MinPol(\alpha \,|\, K)$. Then there is a bijection*

$$\{\textit{roots of } f \textit{ in } R\} \;\longrightarrow\; \{\textit{extensions } Q \textit{ of } P \textit{ to } L\}.$$

Proof. If β is a root we consider the K-embedding

$$\varphi_\alpha\colon L \hookrightarrow R$$

such that $\varphi_\alpha(\alpha) = \beta$. Set $Q := \varphi^{-1}(\sum R^2)$ ordering on L extending P. □

Example 2.8. $K = \mathbb{Q}(\sqrt{2})$ has 2 orderings $P_1 \neq P_2$, with $\sqrt{2} \in P_1$, $\sqrt{2} \notin P_2$. The Minimum Polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $p(\mathrm{x}) = \mathrm{x}^2 - 2$.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (09: 17/11/09)

SALMA KUHLMANN

Contents

1. Basic version of Tarski-Seidenberg

Basic version: Let $(R, \leqslant)$ be a real closed field. We are interested in a system of equations and inequalities (*Gleichungen und Ungleichungen*) for $\underline{X} = (X_1, \ldots, X_n)$ of the form

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) \lhd_1 0 \\ \quad \vdots \\ f_k(\underline{X}) \lhd_k 0 \end{cases}$$

where $\forall\, i = 1, \ldots, k \;\; \lhd_i \in \{\geqslant, >, =, \neq\}$ and $f_i(\underline{X}) \in \mathbb{Q}[\underline{X}]$ or $f_i(\underline{X}) \in R[\underline{X}]$. We say that $S(\underline{X})$ is a system of polynomial equalities and inequalities with coefficients in $\mathbb{Q}$ (or with coefficients in R) in n variables.

Theorem 1.1. *(Tarski-Seidenberg Theorem: Basic Version) Let $S(\underline{T}; \underline{X})$ be a system with coefficients in $\mathbb{Q}$ in $m+n$ variables, with $\underline{T} = (T_1, \ldots, T_m)$ and $\underline{X} = (X_1, \ldots, X_n)$. Then there exist $S_1(\underline{T}), \ldots, S_l(\underline{T})$ systems in m variables and coefficients in $\mathbb{Q}$ such that:*

for every real closed field R and every $\underline{t} = (t_1, \ldots, t_m) \in R^m$ the system $S(\underline{t}; \underline{X})$ of polynomial equalities and inequalities in n variables and coefficients in R obtained by substituting T_i with t_i in $S(\underline{T}, \underline{X})$ for every $i = 1, \ldots, m$, has a solution $\underline{x} = (x_1, \ldots, x_n) \in R^n$ if and only if $\underline{t} = (t_1, \ldots, t_m) \in R^m$ is a solution in R for one of the systems $S_1(\underline{T}), \ldots, S_l(\underline{T})$.

Example 1.2. Let $m = 3$ and $n = 1$, so $\underline{T} = (T_1, T_2, T_3)$ and $\underline{X} = X$, and

$$S(\underline{T}, \underline{X}) := \Big\{ T_1 X^2 + T_2 X + T_3 = 0$$

Let R be a real closed field and $(t_1, t_2, t_3) \in R^3$. Then $S(\underline{t}; X)$ has a solution X in R if and only if

$$\begin{array}{ccccc} (t_1 \neq 0 \ \wedge \ t_2^2 - 4t_1t_3 \geqslant 0) & \vee & (t_1 = 0 \ \wedge \ t_2 \neq 0) & \vee & (t_1 = t_2 = t_3 = 0) \\ | & & | & & | \\ S_1(T_1, T_2, T_3) & & S_2(T_1, T_2, T_3) & & S_3(T_1, T_2, T_3) \end{array}$$

Concise version:

$$\forall \underline{T} \ [\ (\exists \underline{X} : S(\underline{T}; \underline{X})) \ \Leftrightarrow \ (\bigvee_{i=1}^{l} S_i(\underline{T})) \ ].$$

Remark 1.3. The proof is by induction on n.

The case $n = 1$ is the heart of the proof and we will show it later.

For now, let us just convince ourselves that the induction step is straightforward.

Assume $n > 1$, so

$$S(\underline{T}; X_1, \ldots, X_n) = S(\underline{T}, X_1, \ldots, X_{n-1}; X_n).$$

By case $n = 1$ we have finitely many systems $S_1(\underline{T}, X_1, \ldots, X_{n-1}), \ldots, S_l(\underline{T}, X_1, \ldots, X_{n-1})$ such that

for any real closed field R and any $(t_1, \ldots, t_m, x_1, \ldots, x_{n-1}) \in R^{m+n-1}$ we have

$$\exists X_n : \ S(t_1, \ldots, t_m, x_1, \ldots, x_{n-1}; X_n) \ \longleftrightarrow \ \bigvee_{i=1}^{l} S_i(t_1, \ldots, t_m, x_1, \ldots, x_{n-1}).$$

By induction hypothesis on n:

for every fixed i, $1 \leqslant i \leqslant l$, $\exists$ systems $S_{ij}(\underline{T})$, $j = 1, \ldots, l_i$ such that: for each real closed field R and each $\underline{t} \in R^m$ the system

$$S_i(\underline{t}; X_1, \ldots, X_{n-1})$$

has a solution $(x_1, \ldots, x_{n-1}) \in R^{n-1}$ if and only if $\underline{t}$ is a solution for one of the systems $S_{ij}(\underline{T})$; $j = 1, \ldots, l_i$.

Therefore for any real closed field R and any $\underline{t} \in R^m$

$$S(\underline{t}; X_1, \ldots, X_n) \text{ has a solution } \underline{x} \in R^n \text{ if and only if}$$

$$\underline{t} \text{ is a solution to one of the systems } \Big\{ S_{ij}(\underline{T}); \ i = 1, \ldots, l, \ j = 1, \ldots, l_i$$

2. Tarski Transfer Principle I

Theorem 2.1. *Let $S(\underline{T}, \underline{X})$ be a system with coefficients in $\mathbb{Q}$ in $m + n$ variables. Let $(K, \leqslant)$ be an ordered field. Let R_1, R_2 be two real closed extensions of $(K, \leqslant)$. Then for every $\underline{t} \in K^m$, the system $S(\underline{t}, \underline{X})$ has a solution $\underline{x} \in R_1^n$ if and only if it has a solution $\underline{x} \in R_2^n$.*

Proof. Let $\underline{t} \in K^m \subseteq R_1^m \cap R_2^m$. Then there are systems $S_i(\underline{T})$ $(i = 1, \ldots, l)$ with coefficients in $\mathbb{Q}$ and variables $T_1, \ldots, T_m$ such that

$$\exists\, \underline{x} \in R_1 : S(\underline{t}, \underline{x}) \iff \underline{t} \text{ satisfies } \bigvee_{i=1}^{l} S_i(\underline{T}) \iff \exists\, \underline{x} \in R_2 : S(\underline{t}, \underline{x}).$$

□

3. Tarski Transfer Principle II

Theorem 3.1. *Let $(K, \leqslant)$ be an ordered field, R_1, R_2 two real closed extensions of $(K, \leqslant)$. Then a system of polynomial equations and inequalities of the form*

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) \lhd_1 0 \\ \vdots \\ f_k(\underline{X}) \lhd_k 0 \end{cases}$$

where $\forall\, i = 1, \ldots, k \;\; \lhd_i \in \{\geqslant, >, =, \neq\}$ and $f_i(\underline{X}) \in K[X_1, \ldots, X_n]$,

$$\text{has a solution } \underline{x} \in R_1^n \iff \text{it has a solution } \underline{x} \in R_2^n.$$

Proof. Let $t_1, \ldots, t_m$ be the coefficients of the polynomials $f_1, \ldots, f_k$, listed in some fixed order. Replacing the coefficients $t_1, \ldots, t_m$ by variables $T_1, \ldots, T_m$ yields a system $\sigma(\underline{T}, \underline{X})$ in $m + n$ variables with coefficients in $\mathbb{Q}$ (in fact in $\mathbb{Z}$) for which

$$\sigma(t_1, \ldots, t_m, \underline{X}) = S(\underline{X}).$$

Now we can apply Tarski Transfer I. □

4. Tarski Transfer Principle III

Theorem 4.1. *Suppose that $R \subseteq R_1$ are real closed fields. Then a system of polynomial equations and inequalities with coefficients in R*

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) \lhd_1 0 \\ \vdots \\ f_k(\underline{X}) \lhd_k 0 \end{cases}$$

where $\forall\, i = 1, \ldots, k \;\; \lhd_i \in \{\geqslant, >, =, \neq\}$ and $f_i(\underline{X}) \in R[X_1, \ldots, X_n]$

$$\text{has a solution } \underline{x} \in R_1^n \iff \text{it has a solution } \underline{x} \in R^n.$$

Proof. Apply Tarski Transfer II with $K = R_2 = R$. □

5. Tarski Transfer Principle IV

Theorem 5.1. *Let R be a real closed field and $(F, \leqslant)$ an ordered field extension of R. Then a system of polynomial equations and inequalities of the form*

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) \lhd_1 0 \\ \quad \vdots \\ f_k(\underline{X}) \lhd_k 0 \end{cases}$$

where $\forall\, i = 1, \ldots, k \quad \lhd_i \in \{\geqslant, >, =, \neq\}$ *and* $f_i(\underline{X}) \in R[X_1, \ldots, X_n]$

$$\text{has a solution } \underline{x} \in F^n \iff \text{it has a solution } \underline{x} \in R^n.$$

Proof. Let R_1 be the real closure of the ordered field $(F, \leqslant)$ and apply Tarski Transfer III. □

6. Lang's Homomorphism Theorem

Corollary 6.1. *Suppose R and R_1 are real closed fields, $R \subseteq R_1$. Then a system of polynomial equations of the form*

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) = 0 \\ \quad \vdots \\ f_k(\underline{X}) = 0 \end{cases} \qquad f_i(\underline{x}) \in R[X_1, \ldots, X_n]$$

has a solution $\underline{x} \in R_1^n$ if and only if it has a solution $\underline{x} \in R^n$.

Proof. Apply Tarski Transfer III. □

The previous Corollary is equivalent to the following:

Theorem 6.2. *(Homomorphism Theorem I). Let R and R_1 be real closed fields, $R \subseteq R_1$. For any ideal $I \subseteq R[\underline{X}]$, if there exists an R-algebra homomorphism*

$$\varphi \colon R[\underline{X}]/I \longrightarrow R_1$$

then there exists an R-algebra homomorphism

$$\psi \colon R[\underline{X}]/I \longrightarrow R.$$

Proof. By Hilbert's Basis Theorem, I is finitely generated, say $I = \langle f_1, \ldots, f_k \rangle$, with $f_1, \ldots, f_k \in R[\underline{X}]$. Consider the system

$$S(\underline{X}) := \begin{cases} f_1(\underline{X}) = 0 \\ \quad \vdots \\ f_k(\underline{X}) = 0 \end{cases}$$

Claim. There is a bijection

$$\{\underline{x} \in R_1^n \text{ solution to } S(\underline{X})\} \longleftrightarrow \{\varphi \colon R[\underline{X}]/I \to R_1 \;\; R\text{-algebra homomorphism}\}$$

Proof of the claim:

Let $\underline{x} \in R_1^n$ be a solution to $S(\underline{X})$; then the evaluation homomorphism

$$\begin{array}{rccc} \varphi\colon & R[\underline{X}]/I & \longrightarrow & R_1 \\ & f+I & \mapsto & f(\underline{x}) \end{array}$$

is well-defined and is an R-algebra homomorphism.

Conversely: assume that

$$\varphi\colon R[\underline{X}]/I \longrightarrow R_1$$

is an R-algebra homomorphism. Then for $\underline{e} = (e_1, \ldots, e_n)$ and $f = \sum \underline{a}_e \underline{X}^e = \sum a_{e_1 \ldots e_n} X_1^{e_1} \ldots X_n^{e_n} \in R[\underline{X}]$,

$$\varphi(f+I) = \sum \underline{a}_e \varphi(X_1+I)^{e_1} \cdots \varphi(X_n+I)^{e_n} = f(\varphi(X_1+I), \ldots, \varphi(X_n+I)).$$

In other words set $(x_1, \ldots, x_n) \in R_1^n$ to be defined by $x_1 := \varphi(X_1 + I), \ldots, x_n := \varphi(X_n + I)$, then $(x_1, \ldots, x_n)$ is a solution to $S(\underline{X})$ and the R-algebra homomorphism φ is indeed given by point evaluation at $\underline{x} = (x_1, \ldots, x_n) \in R_1^n$.

Now apply Corollary 6.1. □

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

SALMA KUHLMANN

Contents

1. Homomorphism Theorems

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

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

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

$$\varphi\colon A \longrightarrow R_1$$

then there is an R-algebra homomorphism

$$\psi\colon A \longrightarrow R.$$

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 $\vartheta\colon R[\mathrm{x}_1, \ldots, \mathrm{x}_n] \longrightarrow A$ (for some $n \in \mathbb{N}$).*

Proof.

(⇒) Let A be a finitely generated R-algebra, say with generators $r_1, \ldots, r_n$. Define $\vartheta\colon R[\mathrm{x}_1, \ldots, \mathrm{x}_n] \longrightarrow A$ by setting $\vartheta(\mathrm{x}_i) := r_i$ for every $i = 1, \ldots, n$, and $\vartheta(a) := a$ for every $a \in R$.

(⇐) Given a surjective homomorphism $\vartheta\colon R[\mathrm{x}_1, \ldots, \mathrm{x}_n] \longrightarrow A$ set $r_i := \vartheta(\mathrm{x}_i) \in A$ for every $i = 1, \ldots, n$. Then $\{r_1, \ldots, r_n\}$ generate A over R.

□

So we get $A \cong R[\underline{\mathrm{x}}]/I$ 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*

$$S(\underline{\mathrm{x}}) := \begin{cases} f_1(\underline{\mathrm{x}}) \lhd_1 0 \\ \quad \vdots \\ f_k(\underline{\mathrm{x}}) \lhd_k 0 \end{cases}$$

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

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

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

Proof.

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

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

- Replace each strict inequality

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

- Finally collect all inequalities $f_i \neq 0$, $i = 1, \ldots, t$ 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 $S(\underline{\mathrm{x}})$ be a system with coefficients in R:

$$S(\underline{\mathrm{x}}) := \begin{cases} f_1(\underline{\mathrm{x}}) \lhd_1 0 \\ \quad \vdots \\ f_k(\underline{\mathrm{x}}) \lhd_k 0 \end{cases}$$

Rewrite it as

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

with $f_i(\underline{\mathrm{x}}), g(\underline{\mathrm{x}}) \in R[\mathrm{x}_1, \ldots, \mathrm{x}_n]$.

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

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

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

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

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

□

2. Hilbert's 17^{th} problem

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

We know that

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

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

$$f \geqslant 0 \text{ on } \mathbb{R}^n \ \overset{?}{\Rightarrow}\ f \in \sum \mathbb{R}(\underline{\mathrm{x}})^2. \qquad \textbf{(Hilbert's } 17^{th} \textbf{ problem)}.$$

Remark 2.2.

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

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

(2) If $n = 1$ then indeed $f \geqslant 0$ 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

$P_{d,n} = \sum_{d,n} \iff n \leqslant 2$ or $d = 2$ or $(n = 3$ 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 $\deg(f) = 2\max\{\deg(f_i) : i = 1, \ldots, k\}$.*

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

The first example was given by Motzkin 1967:

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

Theorem 2.4. *(Artin, 1927) Let R be a real closed field and $f \in R[\underline{x}]$, $f \geqslant 0$ 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 $\leqslant_P$ be the ordering such that $(F, \leqslant_P)$ 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 $(F, \leqslant_P)$ is an ordered field extension). By construction $f \notin P$ so $f(\underline{x}) < 0$. Consider the system

$$S(\underline{x}) : \Big\{ f(\underline{x}) < 0, \qquad f(\underline{x}) \in R[\underline{x}].$$

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

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

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

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (11: 24/11/09)

SALMA KUHLMANN

Contents

1. Normal form of semialgebraic sets

Let R be a fixed real closed field and $n \geqslant 1$. We consider 3 operations on subsets of R^n:

(1) finite unions,
(2) finite intersections,
(3) complements.

Definition 1.1.

(*i*) The class of **semialgebraic sets** in R^n is defined to be the smallest class of subsets of R^n closed under operations (1), (2), (3), and which contains all sets of the form

$$\{\underline{x} \in R^n : f(\underline{x}) \lhd 0\},$$

where $f \in R[\underline{x}] = R[x_1, \ldots, x_n]$ and $\lhd \in \{\geqslant, >, =, \neq\}$.

(*ii*) Equivalently a subset $S \subseteq R^n$ is semialgebraic if and only if it is a finite boolean combination of sets of the form

$$\{\underline{x} \in R^n : f(\underline{x}) > 0\},$$

where $f(\underline{x}) \in R[\underline{x}]$.

(*iii*) Consider

$$(*) \quad S(\underline{x}) := \begin{cases} f_1(\underline{x}) \lhd_1 0 \\ \vdots \\ f_k(\underline{x}) \lhd_k 0 \end{cases}$$

with $f_i(\underline{x}) \in R[\underline{x}]$; $\lhd_i \in \{\geqslant, >, =, \neq\}$.
The set of solutions of $S(\underline{x})$ is precisely the semialgebraic set

$$S := \bigcap_{i=1}^{k} \{\underline{x} \in R^n : f_i(\underline{x}) \lhd_i 0\}.$$

The solution set S of a system $(*)$ is called a **basic semialgebraic subset** of R^n.

(*iv*) Let $f_1, \ldots, f_k \in R[\underline{x}] = R[x_1, \ldots, x_n]$. A set of the form

$$Z(f_1, \ldots, f_k) := \{\underline{x} \in R^n : f_1(\underline{x}) = \cdots = f_k(\underline{x}) = 0\}$$

is called an **algebraic set**.

(*v*) A subset of R^n of the form

$$\begin{aligned} \mathcal{U}(f) :&= \{\underline{x} \in R^n : f(\underline{x}) > 0\}, \\ \mathcal{U}(f_1, \ldots, f_k) :&= \{\underline{x} \in R^n : f_1(\underline{x}) > 0, \ldots, f_k(\underline{x}) > 0\} \\ &= \mathcal{U}(f_1) \cap \cdots \cap \mathcal{U}(f_k) \end{aligned}$$

is called a **basic open semialgebraic set**.

(*vi*) A subset of R^n of the form

$$\begin{aligned} \mathcal{K}(f) :&= \{\underline{x} \in R^n : f(\underline{x}) \geqslant 0\}, \\ \mathcal{K}(f_1, \ldots, f_k) &= \mathcal{K}(f_1) \cap \cdots \cap \mathcal{K}(f_k) \end{aligned}$$

is called a **basic closed semialgebraic set**.

Remark 1.2.

(*a*) An algebraic set is in particular a basic semialgebraic set.
(*b*) $Z(f_1, \ldots, f_k) = Z(f)$, where $f = \sum_{i=1}^{k} f_i^2$.

Proposition 1.3.

(1) *A subset of R^n is semialgebraic if and only if it is a finite union of basic semialgebraic sets.*

(2) *A subset is semialgebraic if and only if it is a finite union of basic semialgebraic sets of the form*

$$Z(f) \cap \mathcal{U}(f_1, \ldots, f_k)$$

(normal form).

Proof. (1) ((2) is similar).

($\Leftarrow$) Clear.

($\Rightarrow$) To show that the class of semialgebraic sets is included in the class of finite unions of basic semialgebraic sets it suffices to show that this last class is closed under finitary boolean operations: union, intersection, complement.

The closure by union is by definition.

Intersection:

$$(\cup_i C_i) \cap (\cup_j D_j) = \cup_{i,j} (C_i \cap D_j).$$

Complement: It is enough to show that the complement of

$$\{\underline{x} \in R^n : f(\underline{x}) \lhd 0\} \quad \lhd \in \{\geqslant, >, =, \neq\},$$

is a finite union of basic semialgebraic, since

$$(C \cap D)^c = C^c \cup D^c \quad \text{and} \quad (C \cup D)^c = C^c \cap D^c.$$

Let us consider the possible cases for $\lhd \in \{\geqslant, >, =, \neq\}$:

$$\{\underline{x} \in R^n : f(\underline{x}) \geqslant 0\}^c = \{\underline{x} \in R^n : -f(\underline{x}) > 0\}$$
$$\{\underline{x} \in R^n : f(\underline{x}) > 0\}^c = \{\underline{x} \in R^n : f(\underline{x}) = 0\} \cup \{\underline{x} \in R^n : -f(\underline{x}) > 0\}$$
$$\{\underline{x} \in R^n : f(\underline{x}) = 0\}^c = \{\underline{x} \in R^n : f(\underline{x}) \neq 0\}.$$

□

2. Geometric version of Tarski-Seidenberg

We shall return to a systematic study of the class of semialgebraic sets and its property in the next lectures.

For now we want to derive an important property of this class from Tarski-Seidenberg's theorem:

Theorem 2.1. *(Tarski-Seidenberg geometric version)*
Consider the projection map

$$\pi \colon R^{m+n} = R^m \times R^n \longrightarrow R^m$$
$$(\underline{t}, \underline{x}) \mapsto \underline{t}.$$

Then for any semialgebraic set $A \subseteq R^{m+n}$, $\pi(A)$ is a semialgebraic set in R^m.

Proof. Since

$$\pi(\bigcup_i A_i) = \bigcup_i \pi(A_i),$$

it sufficies to show the result for a basic semialgebraic subset A of R^{m+n}; i.e. show that $\pi(A)$ is semialgebraic in R^m.

Let $\underline{u} := (u_1, \ldots, u_q)$ be the coefficients of all polynomials $f_1(\underline{T}, \underline{X}), \ldots, f_k(\underline{T}, \underline{X}) \in R[T_1, \ldots, T_m, X_1, \ldots, X_n]$ of the system $S(\underline{T}, \underline{X}) = S$ describing A.

So we can view S as a system of polynomial equations and inequalities $S(\underline{U}, \underline{T}, \underline{X})$ with coefficient in $\mathbb{Q}$ such that A is the set of solutions in R^{m+n} of the system $S(\underline{u}, \underline{T}, \underline{X})$, i.e.

$$A = \{(\underline{t}, \underline{x}) \in R^{m+n} : (\underline{t}, \underline{x}) \text{ is solution of } S(\underline{u}, \underline{T}, \underline{X})\}.$$

By Tarski-Seidenberg's theorem, we have systems of polynomial equalities and inequalities with coefficients in $\mathbb{Q}$, say

$$S_1(\underline{u}, \underline{T}), \ldots, S_l(\underline{u}, \underline{T}),$$

such that for any $\underline{t} \in R^m$ the system $S(\underline{u}, \underline{t}, \underline{X})$ has a solution $\underline{x} = (x_1, \ldots, x_n) \in R^n$ if and only if $(\underline{u}, \underline{t})$ is a solution for one of $S_1(\underline{u}, \underline{T}), \ldots, S_l(\underline{u}, \underline{T})$, i.e.

$$\begin{aligned}
\pi(A) &= \{\underline{t} \in R^m : \exists\, \underline{x} \in R^n \text{ with } (\underline{t}, \underline{x}) \in A\} \\
&= \{\underline{t} \in R^m : \exists\, \underline{x} \in R^n \text{ s.t. } (\underline{t}, \underline{x}) \text{ is a solution of } S(\underline{u}, \underline{T}, \underline{X})\} \\
&= \{\underline{t} \in R^m : \text{the system } S(\underline{u}, \underline{t}, \underline{X}) \text{ has a solution } \underline{x} \in R^n\} \\
&= \{\underline{t} \in R^m : \underline{t} \text{ is a solution for one of the } S_i(\underline{u}, \underline{T}), i = 1, \ldots, l\} \\
&= \bigcup_{i=1,\ldots,l} \{\underline{t} \in R^m : \underline{t} \text{ is a solution of } S_i(\underline{u}, \underline{T})\}.
\end{aligned}$$

□

We shall show many important consequences such as the image of a semialgebraic function is semialgebraic and the closure and the interior of a semialgebraic set are semialgebraic.

Definition 2.2. Let $A \subseteq R^m$ and $B \subseteq R^n$. We say that $f\colon A \to B$, is a **semialgebraic map** if A and B are semialgebraic and

$$\Gamma(f) = \{(\underline{x}, \underline{y}) \in R^{m+n} : \underline{x} \in A,\ \underline{y} \in B,\ \underline{y} = f(\underline{x})\}$$

is semialgebraic.

3. Formulas in the language of real closed fields

Definition 3.1. A **first order formula in the language of real closed fields** is obtained as follows recursively:

(1) if $f(\underline{x}) \in \mathbb{Q}[x_1, \ldots, x_n]$, $n \geqslant 1$, then

$$f(\underline{x}) \geqslant 0,\ \ f(\underline{x}) > 0,\ \ f(\underline{x}) = 0,\ \ f(\underline{x}) \neq 0$$

are first order formulas (with free variables $\underline{x} = (x_1, \ldots, x_n)$);

(2) if Φ and Ψ are first order formulas, then

$$\Phi \wedge \Psi, \quad \Phi \vee \Psi, \quad \neg\Phi$$

are also first order formulas (with free variables given by the union of the free variables of Φ and the free variables of Ψ);

(3) if Φ is a first order formula then

$$\exists\, x\, \Phi \quad \text{and} \quad \forall x\, \Phi$$

are first order formulas (with the same free variables as Φ minus $\{x\}$).

The formulas obtained using just (1) and (2) are called **quantifier free**.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (12: 26/11/09)

SALMA KUHLMANN

Contents

1. Quantifier eliminaton for the theory of real closed fields

We recall from last lecture the definition of first order formulas in the language of real closed field:

Definition 1.1. A **first order formula in the language of real closed fields** is obtained as follows recursively:

(1) if $f(\underline{x}) \in \mathbb{Q}[x_1, \ldots, x_n]$, $n \geqslant 1$, then
$$f(\underline{x}) \geqslant 0,\ f(\underline{x}) > 0,\ f(\underline{x}) = 0,\ f(\underline{x}) \neq 0$$
are first order formulas (with free variables $\underline{x} = (x_1, \ldots, x_n)$);

(2) if Φ and Ψ are first order formulas, then
$$\Phi \wedge \Psi, \quad \Phi \vee \Psi, \quad \neg\Phi$$
are also first order formulas (with free variables given by the union of the free variables of Φ and the free variables of Ψ);

(3) if Φ is a first order formula then
$$\exists\, x\, \Phi \quad \text{and} \quad \forall x\, \Phi$$
are first order formulas (with same free variables as Φ minus $\{x\}$).

The formulas obtained using just (1) and (2) are called **quantifier free**.

Definition 1.2. Let $\Phi(x_1, \ldots, x_n)$ and $\Psi(x_1, \ldots, x_n)$ be first order formulas in the language of real closed fields with free variables contained in $\{x_1, \ldots, x_n\}$. We say that $\Phi(\underline{x})$ and $\Psi(\underline{x})$ are **equivalent** if for every real closed field R and every $\underline{r} \in R^n$,
$$\Phi(\underline{r}) \text{ holds in } R \iff \Psi(\underline{r}) \text{ holds in } R.$$

If Φ and Ψ are equivalent, we write $\Phi \sim \Psi$.

Remark 1.3. (Normal form of quantifier free formulas). Every quantifier free formula is equivalent to a finite disjunction of finite conjuctions of formulas obtained using construction (1).

Proof. Like showing that every semialgebraic subset of R^n is a finite union (= finite disjunction) of basic semialgebraic sets (= finite conjuction of formulas of type (1)). □

Theorem 1.4. *(Tarski's quantifier elimination theorem for real closed fields). Every first order formula in the language of real closed fields is equivalent to a quantifier free formula.*

Proof. Since all formulas of type (1) are quantifier free, it suffices to show that

$\mathcal{C} :=$ the set of first order formulas which are equivalent to quantifier free formulas

is closed under constructions of (2) and (3).

Closure under 2. If $\Phi \sim \Phi'$ and $\Psi \sim \Psi'$, then

$$\begin{aligned} \Phi \vee \Psi &\sim \Phi' \vee \Psi' \\ \Phi \wedge \Psi &\sim \Phi' \wedge \Psi' \\ \neg\, \Phi &\sim \neg\, \Phi'. \end{aligned}$$

Closure under 3. It is enough to consider $\exists\, x\, \Phi$, because

$$\forall\, x\, \Phi \;\leftrightarrow\; \neg\, \exists\, x\; (\neg \Phi).$$

We claim that if Φ is equivalent to a quantifier free formula then $\exists\, x\, \Phi$ is equivalent to a quantifier free formula. Since

$$\exists\, x\, (\Phi_1 \vee \cdots \vee \Phi_k) \;\sim\; (\exists\, x\, \Phi_1) \vee \cdots \vee (\exists\, x\, \Phi_k),$$

using the normal form of quantifier free formulas (Remark 1.3), we can assume that Φ is a finite conjunction of polynomial equations and inequalities (i.e. a system $S(\underline{T}, x)$).

Applying Tarski-Seidenberg's Theorem:

$$\exists\, \underline{x}\; S(\underline{T}; \underline{x}) \;\Leftrightarrow\; \bigvee_{i=1}^{l} S_i(\underline{t}),$$

there exist finitely many finite conjunctions of polynomial equalities and inequalities $\vartheta_1, \ldots, \vartheta_l$ (corresponding to the systems $S_1(\underline{t}), \ldots, S_l(\underline{t})$) such that

$$\exists\, \underline{x}\; \Phi \;\sim\; \vartheta_1 \vee \cdots \vee \vartheta_l.$$

□

2. Definable sets

Definition 2.1. Let $\Phi(\underline{T}, \underline{X})$ a first order formula with free variables $T_1, \ldots, T_m, X_1, \ldots, X_n$. Let R be a real closed field and $\underline{t} \in R^m$. Then $\Phi(\underline{t}, \underline{X})$ is a **first order formula with parameters** in R, and $t_1, \ldots, t_m$ are called the parameters.

Definition 2.2. Let R be a real closed field, $n \geqslant 1$. A subset $A \subseteq R^n$ is said to be **definable** (**with parameters** from R) in R if there is a first order formula $\Phi(\underline{t}, \underline{X})$ with parameters $\underline{t} \in R^m$ and free variables $\underline{X} = (X_1, \ldots, X_n)$, such that

$$A = \{\underline{r} \in R^n : \Phi(\underline{t}, \underline{r}) \text{ is true in } R\}.$$

Corollary 2.3. *For any real closed field R the class of definable sets (with parameters) in R coincides with the class of semialgebraic sets.*

(For the second part of the lecture, see file of Lecture 13, from 1.4).

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (12 Continued: 26/11/2009)

SALMA KUHLMANN

THE TARSKI-SEIDENBERG PRINCIPLE

Recall. Let R be a real closed field, $a \in R$. Define

$$sign(a) := \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -1 & \text{if } a < 0. \end{cases}$$

The Tarski-Seidenberg Principle is the following result.

Theorem 1. Let $f_i(\underline{T}, X) = h_{i,m_i}(\underline{T})X^{m_i} + \ldots + h_{i,0}(\underline{T})$ for $i = 1, \ldots, s$ be a sequence of polynomials in n+1 variables ($\underline{T} = (T_1, \ldots, T_n), X$) with coefficients in $\mathbb{Z}$. Let ϵ be a function from $\{1, \ldots, s\}$ to $\{-1, 0, 1\}$. Then there exists a finite boolean combination $B(\underline{T}) := S_1(\underline{T}) \vee \ldots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $T_1, \ldots, T_n$ with coefficients in $\mathbb{Z}$ such that for every real closed field R and for every $\underline{t} \in R^n$, the system

$$\begin{cases} sign(f_1(\underline{t}, X)) = \epsilon(1) \\ \qquad\qquad \vdots \\ sign(f_s(\underline{t}, X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if $B(\underline{t})$ holds true in R.

Notation I. Let $f_1(X), \ldots, f_s(X)$ be a sequence of polynomials in R[X]. Let $x_1 < \ldots < x_N$ be the roots in R of all f_i that are not identically zero.

Set $x_0 := -\infty$, $x_{N+1} := +\infty$

Remark 1. Let $m := max(degf_i, i = 1, \ldots, s)$. Then $N \leq sm$.

Set $I_k :=]x_k, x_{k+1}[$, $k = 0, \ldots, N$

Remark 2. $sign(f_i(x))$ is constant on I_k, for each $i \in 1, \ldots, s$, for each $k \in 0, \ldots, N$.

Set $sign(f_i(I_k)) := sign(f_i(x)),\ x \in I_k$

Notation II. Let $SIGN_R(f_1, \ldots, f_s)$ be the matrix with s rows and $2N+1$ columns whose i^{th} row (for $i = \{1, \ldots, s\}$) is

$$sign\big(f_i(I_0)\big), sign\big(f_i(x_1)\big), sign\big(f_i(I_1)\big), \ldots, sign\big(f_i(x_N)\big), sign\big(f_i(I_N)\big).$$

i.e. $SIGN_R(f_1, \ldots, f_s)$ is an $s \times (2N+1)$ matrix with coefficients in $\{-1, 0, 1\}$ and

$$SIGN_R(f_1, ..., f_s) := \begin{pmatrix} signf_1(I_0) & signf_1(x_1) & \ldots & signf_1(x_N) & signf_1(I_N) \\ signf_2(I_0) & signf_2(x_1) & \ldots & signf_2(x_N) & signf_2(I_N) \\ \vdots & \vdots & & \vdots & \vdots \\ signf_s(I_0) & signf_s(x_1) & \ldots & signf_s(x_N) & signf_s(I_N) \end{pmatrix}$$

Remark 3. Let $f_1, \ldots, f_s \in R[X]$ and $\epsilon : \{1, \ldots, s\} \to \{-1, 0, +1\}$. The system

$$\begin{cases} sign(f_1(X)) = \epsilon(1) \\ \vdots \\ sign(f_s(X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if one column of $SIGN_R(f_1, \ldots, f_s)$ is precisely the matrix $\begin{bmatrix} \epsilon(1) \\ \vdots \\ \epsilon(s) \end{bmatrix}$.

Notation III. Let $M_{P \times Q} :=$ the set of $P \times Q$ matrices with coefficients in $\{-1, 0, +1\}$.

Set $W_{s,m} :=$ the disjoint union of $M_{s \times (2l+1)}$, for $l = 0, \ldots, sm$.

Notation IV. Let $\epsilon : \{1, \ldots, s\} \to \{-1, 0, 1\}$. Set

$$W(\epsilon) = \{M \in W_{s,m} : \textit{one column of } M \textit{ is } \begin{bmatrix} \epsilon(1) \\ \vdots \\ \epsilon(s) \end{bmatrix}\} \subseteq W_{s,m}$$

Lemma 2. (Reformulation of remark 3 using notation IV) Let $\epsilon : \{1, \ldots, s\} \to \{-1, 0, +1\}$, R real closed field and $f_1(X), \ldots, f_s(X) \in R[X]$ of degree $\leq m$. Then the system

$$\begin{cases} sign(f_1(X)) = \epsilon(1) \\ \vdots \\ sign(f_s(X)) = \epsilon(s) \end{cases}$$

has a solution $x \in R$ if and only if $SIGN_R(f_1, \ldots, f_s) \in W(\epsilon)$.

By Lemma 2 (setting $W' = W(\epsilon)$), we see that the proof of Theorem 1 reduces to showing the following proposition:

Main Proposition 3. Let $f_i(\underline{T}, X) := h_{i,m_i}(\underline{T})X^{m_i} + \ldots + h_{i,0}(\underline{T})$ for $i = 1, \ldots, s$ be a sequence of polynomials in n+1 variables with coefficients in $\mathbb{Z}$, and let $m := max\{m_i | i = 1, \ldots, s\}$. Let $W^{'}$ be a subset of $W_{s,m}$. Then there exists a boolean combination $B(\underline{T}) = S_1(\underline{T}) \vee \ldots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $\underline{\mathrm{T}}$ with coefficients in $\mathbb{Z}$, such that, for every real closed field R and every $\underline{t} \in R^n$, we have

$SIGN_R(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X) \in W^{'} \Leftrightarrow B(\underline{t})$ holds true in R.

The proof of the main Proposition will follow by induction from the next main lemma, where we will show that $SIGN_R(f_1, \ldots, f_s)$ is completely determined by the "$SIGN_R$"of a (possibly) longer but simpler sequence of polynomials, i.e. $SIGN_R(f_1, \ldots, f_{s-1}, f_s^{'}, g_1, \ldots, g_s)$, where $f_s^{'}$ = 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.

First we will state and prove the lemma and then prove the proposition.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (13: 01/12/2009)

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

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

$$sign\big(f_s'(\,]-\infty, x_1[\,)\big) = signf_s(x_{i_1}).$$

($\Rightarrow$) We want to show that if $sign\big(f_s'(\,]-\infty, x_1[\,)\big) = signf_s(x_{i_1})$, 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 $signf_s$ must be constant and nonzero on $]-\infty, x_{i_1}]$, so we get $0 \neq signf_s(\,]-\infty, x_1[\,) = signf_s(\,]-\infty, x_{i_1}]\,) = signf_s(x_{i_1}) = signf_s'(\,]-\infty, x_1[\,)$

$\Rightarrow signf_s(\,]-\infty, x_1[\,) = signf_s'(\,]-\infty, x_1[\,)$, a contradiction $\Big[$because on $]-\infty, -D[$: $signf(x) = (-1)^m sign(d)$ for $f = dx^m + \ldots + d_0$ and $signf'(x) = (-1)^{m-1}sign(md)$ for $f' = mdx^{m-1} + \ldots$, see Corollary 2.1 of lecture 6 (05/11/09)$\Big]$.

($\Leftarrow$) Assume that f_s has a root (say) $x \in\,]-\infty, x_{i_1}[$.

Note that $signf_s(x_{i_1}) \neq 0$ $\Big[$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

$$-signf_s(\,]-\infty, x[\,) = signf_s(\,]x, x_{i_1}]\,) = signf_s(x_{i_1}),$$

also (by same argument as before)

$$-signf_s(\,]-\infty, x[\,) = signf_s'(\,]-\infty, x_1[\,),$$

therefore, we get

$$signf_s'(\,]-\infty, x_1[\,) = signf_s(x_{i_1}). \qquad \square \text{ (case 1)}$$

Case 2: Similarly one proves that: f_s has a root in $]x_{i_M}, +\infty[$ (if $M \neq 0$) if and only if

$$sign\big(f_s'(\,]x_N, +\infty[\,)\big)sign\big(g_{\theta(M)}(x_{i_M})\big) = -1,$$

$$\Big(\text{i.e. iff } signf_s'(\,]x_N, +\infty[\,) = -signf_s(x_{i_M}) \neq 0\Big).$$

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

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

(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 $M = 0$. $\square$ (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

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

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

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,

$$SIGN_R(f_1, ..., f_s) := \begin{pmatrix} signf_1(I_0) & signf_1(y_1) & \ldots & signf_1(y_L) & signf_1(I_L) \\ \vdots & \vdots & & \vdots & \vdots \\ signf_{s-1}(I_0) & signf_{s-1}(y_1) & \ldots & signf_{s-1}(y_L) & signf_{s-1}(I_L) \\ signf_s(I_0) & signf_s(y_1) & \ldots & signf_s(y_L) & signf_s(I_L) \end{pmatrix}$$

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 $j = 1, \ldots, s-1$ and $l \in \{0, \ldots, L+1\}$.
Thus one can reconstruct the first $s-1$ rows of $SIGN_R(f_1, ..., f_s)$ from w.

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

- if $l \neq 0$, $\rho(l) = k \Rightarrow$

$$sign\big(f_s(\,]y_l, y_{l+1}[\,)\big) = \begin{cases} sign\big(g_{\theta(k)}(x_{i_k})\big) & \text{if it is } \neq 0, \\ sign\big(f_s'(\,]x_{i_k}, x_{i_{k+1}}[\,)\big) & \text{otherwise.} \end{cases}$$

  $\Big[$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 $]x_{i_k}, x_{i_{k+1}}[$:

$$\begin{cases} f_s' \geq 0 \Rightarrow f_s(x_{i_k}) < f_s(y) \text{ for } y < x_{k+1}, \text{ so } f_s(y) > 0, \\ f_s' \leq 0 \Rightarrow -f_s(x_{i_k}) < -f_s(y) \text{ for } y < x_{k+1}, \text{ so } f_s(y) < 0 \end{cases}$$

  $\big($using lemma (Poizat): In a real closed ordered field, if P is a nonconstant polynomial s.t. $P' \geq 0$ on $[a, b]$, $a < b$, then $P(a) < P(b)\big)$.$\Big]$

- if $l \neq 0$, $\rho(l) = (k, k+1) \Rightarrow sign\big(f_s(\,]y_l, y_{l+1}[\,)\big) = sign\big(f_s'(\,]x_{i_k}, x_{i_{k+1}}[\,)\big)$.

  $\Big[$We argue as follows $\big($noting that $\rho(l) = (k, k+1)$ if $y_l \in]x_{i_k}, x_{i_{k+1}}[\,\big)$:
  $sign\big(f_s(\,]y_l, y_{l+1}[\,)\big)$ 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'.$\Big]$

- if $l = 0 \Rightarrow sign\big(f_s(\,]-\infty, y_1[\,)\big) = sign\big(f_s'(\,]-\infty, x_1[\,)\big)$ (as before). $\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (14: 03/12/2009)

SALMA KUHLMANN

THE TARSKI-SEIDENBERG PRINCIPLE

Main Proposition. Let $f_i(\underline{T}, X) := h_{i,m_i}(\underline{T})X^{m_i} + \ldots + h_{i,0}(\underline{T})$ for $i = 1, \ldots, s$ be a sequence of polynomials in n+1 variables with coefficients in $\mathbb{Z}$, and let $m := max\{m_i | i = 1, \ldots, s\}$. Let W' be a subset of $W_{s,m}$. Then there exists a boolean combination $B(\underline{T}) = S_1(\underline{T}) \vee \ldots \vee S_p(\underline{T})$ of polynomial equations and inequalities in the variables $\underline{\mathrm{T}}$ with coefficients in $\mathbb{Z}$, such that, for every real closed field R and every $\underline{t} \in R^n$, we have

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) \in W' \Leftrightarrow B(\underline{t}) \text{ holds true in R.}$$

Proof. Without loss of generality, we assume that none of $f_1, \ldots, f_s$ is identically zero and that $h_{i,m_i}(\underline{T})$ is not identically zero for $i = 1, \ldots, s$. To every sequence of polynomials $(f_1, \ldots, f_s)$ associate the s-tuple $(m_1, \ldots, m_s)$, where $deg(f_i) = m_i$. We compare these finite sequences by defining a strict order as follows:

$$\sigma := (m_1', \ldots, m_t') \prec \tau := (m_1, \ldots, m_t)$$

if there exists $p \in \mathbb{N}$ such that, for every $q > p$,
-the number of times q appears in σ = the number of times q appears in τ, and
-the number of times p appears in $\sigma <$ the number of times q appears in τ.

This order $\prec$ is a total order [1] on the set of finite sequences.

$\big[$*Example*: let $m = \max(\{m_1, \ldots, m_s\}) = m_s$ (say), σ and τ be the sequence of degrees of the sequences $(f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$ and $(f_1, \ldots, f_{s-1}, f_s)$ respectively, i.e.
$\sigma \rightsquigarrow (f_1, \ldots, f_{s-1}, f_s', g_1, \ldots, g_s)$,
$\tau \rightsquigarrow (f_1, \ldots, f_{s-1}, f_s)$

[1] This was a mistake in the book *Real Algebraic Geometry* of J. Bochnak, M. Coste, M.-F. Roy. For corrected argument, see Appendix I following this proof.

then $\sigma \prec \tau$.]

Let $m = \max\{m_1, \ldots, m_s\}$.

In particular using $p = m$ we have:

$\big(deg(f_1), \ldots, deg(f_{s-1}), deg(f_s^{'}), deg(g_1), \ldots, deg(g_s)\big) \prec \big(deg(f_1), \ldots, deg(f_s)\big)$.

If $\underline{m = 0}$, then there is nothing to show, since $SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) = SIGN_R\big(h_{1,0}(\underline{t}), \ldots, h_{s,0}(\underline{t})\big)$ [the list of signs of "constant terms"].

Suppose that $\underline{m \geq 1}$ and $m_s = m = max\{m_1, \ldots, m_s\}$. Let $W^{''} \subset W_{2s,m}$ be the inverse image of $W^{'} \subset W_{s,m}$ under the mapping φ (as in main lemma). Set $W^{''} = \big\{sign_R(f_1, \ldots, f_{s-1}, f_s^{'}, g_1, \ldots, g_s) \mid sign_R(f_1, \ldots, f_s) \in W^{'}\big\}$.

-Case 1. $h_{i,m_i}(\underline{t}) \neq 0$ for all $i = 1, \ldots, s$
By the main lemma, for every real closed field R and for every $\underline{t} \in R^n$ such that $h_{i,m_i}(\underline{t}) \neq 0$ for $i = 1, \ldots, s$, we have

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_s(\underline{t}, X)\big) \in W^{'}$$

$$\Leftrightarrow$$

$$SIGN_R\big(f_1(\underline{t}, X), \ldots, f_{s-1}(\underline{t}, X), f_s^{'}(\underline{t}, X), g_1(\underline{t}, X), \ldots, g_s(\underline{t}, X)\big) \in W^{''},$$

where $f_s^{'}$ is the derivative of f_s with respect to X, and $g_1, \ldots, g_s$ are the remainders of the euclidean division (with respect to X) of f_s by $f_1, \ldots, f_{s-1}, f_s^{'}$, respectively (multiplied by appropriate even powers of $h_{1,m_1}, \ldots, h_{s,m_s}$, respectively, to clear the denominators).
Now, the sequence of degrees in X of $f_1, \ldots, f_{s-1}, f_s^{'}, g_1, \ldots, g_s$ is smaller than [the sequence of degrees in X of $f_1, \ldots, f_s$ i.e.] $(m_1, \ldots, m_s)$ w.r.t. the order $\prec$.

-Case 2. At least one of $h_{i,m_i}(\underline{t})$ is zero
In this case we can truncate the corresponding polynomial f_i and obtain a sequence of polynomials, whose sequence of degrees in X is smaller than $(m_1, \ldots, m_s)$ w.r.t. the order $\prec$.

This completes the proof of main propostion and also proves the Tarski-Seidenberg principle. □□

APPENDIX I: ORDER ON THE SET OF TUPLES OF INTEGERS

Set $N := \bigcup_{n\in\mathbb{N}} \mathbb{N}^n$

We define on N an equivalence relation $\sim$:
for $\sigma := (n_1, \ldots, n_s)$ and $\tau := (m_1, \ldots, m_t)$ in N, we write $\sigma \sim \tau$ if and only if the following holds:
$s = t$ and there exists a permutation g of $\{1, \ldots, s\}$ such that $m_i = n_{g(i)}$ for all $i \in \{1, \ldots, s\}$.

For any $\sigma \in N$, the equivalence class of σ will be denoted by $[\sigma]$
For any $\sigma \in N$ and $p \in \mathbb{N}$, we set $f_p(\sigma) :=$ (number of occurrences of p in σ).
For any $\sigma,\tau \in N$ and $p \in \mathbb{N}$ we define the property $\mathcal{P}(p, \sigma,\tau)$ by:
$\mathcal{P}(p, \sigma,\tau) \equiv (f_p(\sigma) < f_p(\tau)) \wedge (\forall q > p, f_q(\sigma) = f_q(\tau))$.

Set $M := N/\sim$
Note that if σ', τ' are permutations of σ and τ, then $\mathcal{P}(p, \sigma,\tau)$ is equivalent to $\mathcal{P}(p,\sigma', \tau')$ for all $p \in \mathbb{N}$. This allows us to define a binary relation $<$ on M:

$[\sigma] < [\tau]$ if and only if there exists $p \in \mathbb{N}$ such that $\mathcal{P}(p, \sigma,\tau)$ is satisfied.

Remark 1
`If` $p \in \mathbb{N}$ `satisfies` $\mathcal{P}(p, \sigma,\tau)$`, then for all` $q \geq p$`,` $f_q(\sigma) \leq f_q(\tau)$

Proposition 1
$<$ defines a strict order on M.

Proof. We want to prove that $<$ is antisymmetric and transitive:

antisymmetry: Let $\sigma,\tau \in N$ such that $[\sigma] < [\tau]$; we want to show $[\tau] \not< [\sigma]$

Choose $p \in \mathbb{N}$ satisfying $\mathcal{P}(p, \sigma,\tau)$ and let $q \in \mathbb{N}$.

If $q \geq p$, then by remark 1 we have $f_q(\tau) \not< f_q(\sigma)$ so the first condition of $\mathcal{P}(q, \tau,\sigma)$ fails. Moreover, we have $f_p(\sigma) < f_p(\tau)$, so if $q < p$ the second condition of $\mathcal{P}(q, \tau,\sigma)$ fails.

Thus, $\mathcal{P}(q, \tau,\sigma)$ fails for every $q \in \mathbb{N}$, which proves $[\tau] \not< [\sigma]$.

transitivity: Let $\sigma, \tau, \rho \in N$ such that $[\rho] < [\sigma]$ and $[\sigma] < [\tau]$

Choose $p_1, p_2 \in \mathbb{N}$ such that $\mathcal{P}(p_1, \rho, \sigma)$ and $\mathcal{P}(p_2, \sigma, \tau)$ hold.

Set $p := max(p_1, p_2)$.

If $q > p$, then in particular $q > p_1$ so $f_q(\rho) = f_q(\sigma)$; similarly, we have $q > p_2$ so $f_q(\sigma) = f_q(\tau)$ hence $f_q(\rho) = f_q(\tau)$.

Since $p \geq p_1, p_2$, we have by remark 1: $f_p(\rho) \leq f_p(\sigma) \leq f_p(\tau)$. If $p = p_1$, the first inequality is strict, hence $f_p(\rho) < f_p(\tau)$; if $p = p_2$ then the second inequatlity is strict, which leads to the same conclusion.

This proves that $\mathcal{P}(p, \rho, \tau)$ is satisfied, hence $[\rho] < [\tau]$.

□

Proposition 2
The order $<$ is total on M

Proof. Let $\sigma = (n_1, \ldots, n_s), \tau = (m_1, \ldots, m_t) \in N$ be non-equivalent.
Set $A := \{q \in \{n_1, \ldots, n_s, m_1, \ldots, m_t\} \mid f_q(\sigma) \neq f_q(\tau)\}$.
Note that $A = \varnothing$ if and only if $\sigma \sim \tau$, so by hypothesis we have $A \neq \varnothing$. Thus, we can define $p := maxA$.
By definition of p, we have $f_q(\tau) = f_q(\sigma)$ for all $q > p$.
Moreover, since $p \in A$, we have $f_p(\sigma) \neq f_p(\tau)$.
If $f_p(\sigma) < f_p(\tau)$, then $\mathcal{P}(p, \sigma, \tau)$ is satisfied, so $[\sigma] < [\tau]$; if $f_p(\tau) < f_p(\sigma)$, then $\mathcal{P}(p, \tau, \sigma)$ is satisfied, so $[\tau] < [\sigma]$.

□

Note that we have an algorithm which determines how to order the pair (σ, τ) and gives us an apropriate p:

$p := max\{n_1, \ldots, n_s, m_1, \ldots, m_t\}$.
while $p \geq 0$:
    if $f_p(\sigma) > f_p(\tau)$ return $(\sigma > \tau, p)$
    if $f_p(\sigma) < f_p(\tau)$ return $(\sigma < \tau, p)$
    $p := p - 1$

Proposition 3
$(M, <)$ is well-ordered:

Proof. For any $\sigma = (n_1, \ldots, n_s) \in N$, set $m_\sigma := max(n_1, \ldots, n_s)$. Since m_σ is left unchanged by permutation of σ, so we can define $m_{[\sigma]} := m_\sigma$ unambiguously.
Note that for any $a, b \in M$, $m_a < m_b$ implies $a < b$. Indeed, if $m_a < m_b$, then for any $p > m_b$, we have $f_p(b) = 0 = f_p(a)$; moreover, $f_{m_b}(a) = 0 < f_{m_b}(b)$, which

proves that $\mathcal{P}(m_b, a, b)$ holds.

Let A be a non-empty subset of M and set $m := min\{m_a \mid a \in A\}$
We are going to prove by induction on m that A has a smallest element.

m=0: If $m = 0$, then the set $A_0 := \{[\sigma] \in A \mid \sigma$ only contains zeros $\}$ is non-empty. Let a be the element of A_0 of minimal length; then I claim that a is the smallest element of A.

Indeed: let $b \in A$, $b \neq a$.

If $b \in A_0$, then a and b both only contain zeros, so for all $p > 0$ $f_p(a) = 0 = f_p(b)$; moreover, by choice of a, we have $f_0(a) = length(a) < length(b) = f_0(b)$. This proves that $\mathcal{P}(0, a, b)$ holds, hence $a < b$.

If $b \in A\backslash A_0$, then $m_b > 0 = m_a$ so $b > a$.

$m - 1 \to m$: Assume $m \geq 1$.

Set $B := \{a \in A \mid m_a = m\}$, $n := min\{f_m(a) \mid a \in B\}$ and $C := \{a \in B \mid f_m(a) = n\}$.

I claim that for any $c \in C$ and any $a \in A\backslash C$, $c < a$.

Indeed:

- if $a \in B\backslash C$, then by definition of C we have $f_m(c) < f_m(a)$. Since $a, c \in B$, it follows from the definition of B that m is the maximal element of both a and c, so that $f_p(a) = 0 = f_p(c)$ for all $p > m$. Thus, $\mathcal{P}(m, c, a)$ holds.
- If $a \notin B$, then by definition of B we have $m_a > m = m_c$, hence $a > c$.

Thus, it suffices to prove that C has a smallest element.

For any $c \in C$, we denote by c' the element of M obtained from c by removing every occurrence of m. Set $C' := \{c' \mid c \in C\}$. Since m is the maximal element of every $c \in C$, we have $m_{c'} \leq m - 1$ for every $c' \in C'$, hence $min\{m_{c'} \mid c' \in C'\} \leq m - 1$. By induction hypothesis, C' then has a smallest element c'. c is then the smallest element of C.

□

Note that there is a recursive algorithm which takes a subset of M as an argument and returns its smallest element:

smallest_element(A):
    $m := min\{m_a \mid a \in A\}$

$B := \{a \in A \mid m_a = m\}$
$n = min\{f_m(b) \mid b \in B\}$
$C := \{b \in B \mid f_m(b) = n\}$
if C is a singleton then return its only element
$C' := \{c' \mid c \in C\}$
c':=smallest_element(C')
return the concatenation of c' with $\underbrace{(m, \ldots, m)}_{n \text{ times}}$

Proposition 4
The ordinal type of $(M, <)$ **is** ω^ω

Proof. For any $n \in \mathbb{N}$, set $A_n := \{a \in M \mid m_a = n\}$.

We are going to build an isomorpism from ω^ω to M by induction. More precisely, we are going to build a sequence $(\phi_n)_{n\in\mathbb{N}}$ of maps such that:

- for any $n \in \mathbb{N}$, ϕ_n is an isomorphism from ω^{n+1} to A_n.
- for any $n \in \mathbb{N}$, ϕ_{n+1} extends ϕ_n.

Taking $\phi := \bigcup_{n\in\mathbb{N}} \phi_n$, we obtain an isomorphism ϕ from $\bigcup_{n\in\mathbb{N}} \omega^{n+1} = \omega^\omega$ to $\bigcup_{n\in\mathbb{N}} A_n = M$.

$\underline{n = 0}$ Note that we have $(0) < (0,0) < (0,0,0) < (0,0,0,0) < \ldots$, so an isomorphism from ω to A_0 is given by $n \mapsto \underbrace{(0, 0, \ldots, 0)}_{n+1 \text{ times}}$

$\underline{n \to n+1}$ Assume we have an isomorphism $\phi_n : \omega^{n+1} \to A_n$. Remember that ω^{n+2} is the order type of $(\omega \times \omega^{n+1}, <_{lex})$.

Define: $\phi_{n+1}(\alpha,\beta) := \phi_n(\beta) \wedge \underbrace{(n+1, \ldots, n+1)}_{\alpha \text{ times}}$

(here '$\wedge$' means concatenation). This is an isomorphism from $(\omega \times \omega^{n+1}, <_{lex})$ to A_{n+1}.

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (15: 08/12/09)

SALMA KUHLMANN

Contents

1. Algebraic sets and constructible sets

Definition 1.1. Let K be a field. Let $f_1, \dots, f_k \in K[\underline{\mathrm{x}}] = K[\mathrm{x}_1, \dots, \mathrm{x}_n]$. A set of the form

$$Z(f_1, \dots, f_k) := \{\underline{x} \in K^n : f_1(\underline{x}) = \cdots = f_k(\underline{x}) = 0\}$$

is called an **algebraic set**.

Definition 1.2. A subset $C \subseteq K^n$ is **constructible** if it is a finite Boolean combination of algebraic sets.

Remark 1.3.

(1) A constructible subset of K is either finite or cofinite.

(2) Let $K = \mathbb{R}$ and consider the algebraic set

$$Z = \{(x, y) \in K^2 : x^2 - y = 0\}.$$

Its image under the projection $\pi(x, y) = y$ is $\pi(Z) = [0, \infty[$ which is neither finite nor cofinite.

This shows that in general a Boolean conbination of algebraic sets is not closed under projections.

Definition 1.4. A function $F\colon K^n \to K^m$ is a **polynomial map** if there are polynomials $F_1, \dots, F_m \in K[\mathrm{x}_1, \dots, \mathrm{x}_n]$ such that for every $\underline{x} \in K^n$,

$$F(\underline{x}) = (F_1(\underline{x}), \dots, F_m(\underline{x})) \in K^m.$$

Example 1.5. The projection map

$$\begin{array}{rccc} \prod_n : & K^{n+m} & \longrightarrow & K^n \\ & (x_1, \ldots, x_{n+m}) & \mapsto & (x_1, \ldots, x_n) \end{array}$$

is a polynomial map, where for every i, $1 \leqslant i \leqslant n$,

$$P_i(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}) = x_i$$

and $\prod_n = (P_1, \ldots, P_n)$.

By Chevalley's Theorem (Quantifier elimination for algebraically closed fields), if K is an algebraically closed field, then the image of a constructible set over K under a polynomial map is constructible (in particular under projections).

Let R be now a real closed field.

Remark 1.6.

(1) A semialgebraic subset of R^n is the projection of an algebraic subset of R^{n+m} for some $m \in \mathbb{N}$, e.g. the semialgebraic set

$$\{\underline{x} \in R^n : f_1(\underline{x}) = \cdots = f_l(\underline{x}) = 0, g_1(\underline{x}) > 0, \ldots, g_m(\underline{x}) > 0\}$$

is the projection of the algebraic set

$$\{(\underline{x}, \underline{y}) \in R^{n+m} : f_1(\underline{x}) = \cdots = f_l(\underline{x}) = 0,\ y_1^2 g_1(\underline{x}) = 1, \ldots,\ y_m^2 g_m(\underline{x}) = 1\}.$$

(2) Every semialgebraic subset of R^n is in fact the projection of an algebraic subset of R^{n+1} (Motzkin, The real solution set of a system of algebraic inequalities is the projection of a hypersurface in one more dimension, 1970 Inequalities, II Proc. Second Sympos., U.S. Air Force Acad., Colo., 1967 pp. 251–254 Academic Press, New York).

2. Topology

For $\underline{x} = (x_1, \ldots, x_n) \in R^n$, we have the norm $|| \underline{x} || := \sqrt{x_1^2 + \cdots + x_n^2}$.
Let $r \in R$, $r > 0$.

$$B_n(\underline{x}, r) = \{\underline{y} \in R^n : || \underline{y} - \underline{x} || < r\} \qquad \text{is an open ball.}$$

$$\bar{B}_n(\underline{x}, r) = \{\underline{y} \in R^n : || \underline{y} - \underline{x} || \leqslant r\} \qquad \text{is a closed ball.}$$

$$S^{n-1}(\underline{x}, r) = \{\underline{y} \in R^n : || \underline{y} - \underline{x} || = r\} \qquad \text{is a } n-1\text{-sphere.}$$

$$S^{n-1} = S^{n-1}(\underline{0}, 1) \qquad \underline{0} \in R^n.$$

Exercise 2.1.

– $B_n(\underline{x}, r)$, $\bar{B}_n(\underline{x}, r)$, $S^{n-1}(\underline{x}, r)$ are semialgebraic.

– Polynomials are continuous with respect to the Euclidean topology.

– The open balls form a basis for the Euclidean topology = norm topology = interval topology.

– The closure and the interior of a semialgebraic set are semialgebraic.

Remark 2.2. It is not true that the closure of a semialgebraic set is obtained by relaxing the inequalities! For instance

$$\{x > 0\} \cap \{x < 0\} = \emptyset.$$

3. Semialgebraic functions

Definition 3.1. Let $A \subseteq R^m$, $B \subseteq R^n$ be two semialgebraic sets. A function

$$f\colon A \longrightarrow B$$

is **semialgebraic** if its graph

$$\Gamma_f = \{(\underline{x}, \underline{y}) \in A \times B : \underline{y} = f(\underline{x})\}$$

is a semialgebraic subset of R^{m+n}.

Example 3.2.

(1) Any polynomial mapping $f\colon A \to B$ between semialgebraic sets is semialgebraic.

(2) More generally, any regular rational mapping $f\colon A \to B$ (i.e. all coordinates are rational functions whose denominators do not vanish on A) is semialgebraic.

(3) If A is a semialgebraic set and $f\colon A \to R$, $g\colon A \to R$ are semialgebraic maps, then $|f|$, $\max(f, g)$, $\min(f, g)$ are semialgebraic maps.

(4) If A is a semialgebraic set and $f\colon A \to R$ is a semialgebraic map with $f \geqslant 0$ on A, then $\sqrt{f}$ is a semialgebraic map.

Proposition 3.3.

(1) *The composition $g \circ f$ of semialgebraic maps f and g is semialgebraic.*

(2) *Let $f\colon A \to B$ and $g\colon C \to D$ semialgebraic maps. Then the map*

$$\begin{array}{rccc} f \times g\colon & A \times C & \longrightarrow & B \times D \\ & (\underline{x}, \underline{y}) & \mapsto & (f(\underline{x}), g(\underline{y})) \end{array}$$

is semialgebraic.

(3) *Let $f\colon A \to B$ be semialgebraic.*

(*i*) *$S \subseteq A$ semialgebraic $\Rightarrow$ $f(S)$ is semialgebraic.*
(*ii*) *$T \subseteq B$ semialgebraic $\Rightarrow$ $f^{-1}(T)$ is semialgebraic.*

(4) *Let A be a semialgebraic set. Then*

$$\mathcal{S}(A) = \{f\colon A \to R : f \text{ is semialgebraic}\}$$

is a commutative ring under pointwise addition and pointwise multiplication.

Proposition 3.4. *Let $A \subseteq R^n$ be a non-empty semialgebraic set.*

(*i*) *For every $\underline{x} \in R^n$ the distance between $\underline{x}$ and A:*

$$\operatorname{dist}(\underline{x}, A) := \inf(\{||\underline{x} - \underline{y}|| : \underline{y} \in A\})$$

is well-defined.

(*ii*) *The function*

$$\begin{array}{rccc} \operatorname{dist}\colon & R^n & \longrightarrow & R \\ & \underline{x} & \mapsto & \operatorname{dist}(\underline{x}, A) \end{array}$$

is continuous semialgebraic vanishing on the closure of A and positive elsewhere.

4. Semialgebraic homeomorphisms

We have that every semialgebraic subset of R can be decomposed as the union of finitely many points and open intervals. We shall generalize this to higher dimension:

Definition 4.1. Let A, B be semialgebraic sets and $f\colon A \to B$. We say that f is a **semialgebraic homeomorphism** if

(1) f is a bijection,
(2) f and f^{-1} are continuous and semialgebraic.

Definition 4.2. Let A, B be semialgebraic sets. We say that they are **semialgebraically homeomorphic** if there is a semialgebraic homeomorphism $f\colon A \to B$.

Our aim is to show that every semialgebraic set can be decomposed as the disjoint union of finetely many pieces which are semialgebraically homeomorphic to open hypercubes $(0,1)^d$ (possibly for different $d \in \mathbb{N}$).

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (16: 10/12/09)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Cylindrical algebraic decomposition

Theorem 1.1. *Let $\underline{\mathrm{x}} = (\mathrm{x}_1, \ldots, \mathrm{x}_n)$. Let $f_1(\underline{\mathrm{x}}, \mathrm{y}), \ldots, f_s(\underline{\mathrm{x}}, \mathrm{y})$ be polynomials in $n+1$ variables with coefficients in R. Then there exixts a partition of R^n into a finite number of semialgebraic sets*

$$R^n = A_1 \dot\cup \cdots \dot\cup A_m$$

and for each $i = 1, \ldots, m$ there exists a finite number (possibly 0) of continuous semialgebraic functions $\xi_{i1}, \ldots, \xi_{il_i}$ defined on A_i with

$$\xi_{i1} < \cdots < \xi_{il_i}$$
$$\xi_{ij} \colon A_i \longrightarrow R$$

and $\xi_{ij}(\underline{x}) < \xi_{ij+1}(\underline{x})$ for all $\underline{x} \in A_i$, for all $j = 1, \ldots, l_i$, such that

(*i*) *for each $\underline{x} \in A_i$, $\{\xi_{i1}(\underline{x}), \ldots, \xi_{il_i}(\underline{x})\} = \{$roots of those polynomials among $f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})$ which are not identically zero$\}$;*

(*ii*) *for each $\underline{x} \in A_i$ and $y \in R$, $\mathrm{sign}(f_1(\underline{x}, y)), \ldots, \mathrm{sign}(f_s(\underline{x}, y))$ depend only on $\mathrm{sign}(y - \xi_{i1}), \ldots, \mathrm{sign}(y - \xi_{il_i})$.*

We will prove this Theorem using the following Proposition:

Proposition 1.2. *(Main proposition "with coefficients")*
Let $f_1(\underline{\mathrm{x}}, \mathrm{y}), \ldots, f_s(\underline{\mathrm{x}}, \mathrm{y})$ be polynomials in $n+1$ variables with coefficients in R. Let $q := \max_{i=1,\ldots,s}\{\deg$ in y of $f_i(\underline{\mathrm{x}}, \mathrm{y})\}$ and $w \in W_{s,q}$.

Then there exists a boolean combination $B_w(\underline{\mathrm{x}})$ of polynomial equations and inequalities in the variables $\underline{\mathrm{x}}$ with coefficients in R such that for any $\underline{x} \in R^n$,

$$\mathrm{sign}_R(f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})) = w \;\Leftrightarrow\; B_w(\underline{x}) \text{ is satisfied in } R.$$

Proof. Let $\underline{a} \in R^p$ be the list of coefficients of the polynomials $f_1, \ldots, f_s$. Then for every $k = 1, \ldots, s$,

$$f_k(\underline{\mathrm{x}}, \mathrm{y}) = F_k(\underline{a}, \underline{\mathrm{x}}, \mathrm{y}),$$

where $F_k(\underline{\mathrm{t}}, \underline{\mathrm{x}}, \mathrm{y}) \in \mathbb{Z}[\underline{\mathrm{t}}, \underline{\mathrm{x}}, \mathrm{y}]$ is a polynomial in $p + n + 1$ variables.

Then there is a boolean combination $B^*_w(\underline{\mathrm{t}}, \underline{\mathrm{x}})$ of polynomial equations and inequalities in the variables $(\underline{\mathrm{t}}, \underline{\mathrm{x}})$ with coefficients in $\mathbb{Z}$ such that, for every $(\underline{t}, \underline{x}) \in R^{p+n}$, we have

$$\mathrm{sign}_R(F_1(\underline{t}, \underline{x}, \mathrm{y}), \ldots, F_s(\underline{t}, \underline{x}, \mathrm{y})) = w \;\Leftrightarrow\; B^*_w(\underline{t}, \underline{x}) \text{ holds.}$$

Now set $B_w(\mathrm{x}) = B^*_w(\underline{a}, \underline{\mathrm{x}})$. □

Let us prove now Theorem 1.1:

Proof of the Theorem. Without loss of generality we may assume that the set $\{f_1, \ldots, f_s\}$ is closed under derivation with respect to the variable y (because we can always remove the functions ξ_{ij} that do not give the roots of the polynomials belonging to the initial family, and the conclusions of the theorem still hold with the remaining ξ_{ij}'s).

As in the previous Proposition, let $q := \max_{i=1,\ldots,s}\{\deg \text{ in } y \text{ of } f_i(\underline{x}, y)\}$. Now $W_{s,q}$ is a finite set with

$$|W_{s,q}| = 3^{sq}.$$

For $w \in W_{s,q}$, define:

$$\begin{aligned} A_w :&= \{\underline{x} \in R^n : B_w(\underline{x}) \text{ is satisfied } \} \\ &= \{\underline{x} \in R^n : \mathrm{sign}_R(f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})) = w\}. \end{aligned}$$

Observe that A_w is a semialgebraic set of R^n. Let $A_1, \ldots, A_m$ be the semialgebraic sets among the A_w that are non-empty, i.e.

$$\{A_1, \ldots, A_m\} = \{A_w : w \in W_{s,q} \text{ and } A_w \neq \emptyset\}.$$

Note that by definition of A_w we have that $A_1, \ldots, A_m$ form a partition of R^n (they are all disjoint because $w_1 \neq w_2 \Rightarrow A_{w_1} \cap A_{w_2} = \emptyset$, and for every $\underline{x} \in R^n$, $\underline{x} \in A_w$ with $w = \mathrm{sign}_R(f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y}))$).

Note also that by definition of A_w, $\mathrm{sign}_R(f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})) = w \in W_{q,s}$ is constant on each A_i. In other words by definition of w there is a number $l_i \leqslant sq$ such that, for each $\underline{x} \in A_i$, the polynomials among $f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})$ which are not identically zero have altoghether l_i roots

$$\xi_{i1}(\underline{x}) \;<\; \cdots \;<\; \xi_{il_i}(\underline{x})$$

and moreover for every $k = 1, \ldots, s$ the signs

$$\mathrm{sign}(f_k(\underline{x}, \xi_{ij}(\underline{x}))), \qquad j = 1, \ldots, l_i$$

$$\mathrm{sign}(f_k(\underline{x},]\, \xi_{ij}(\underline{x}), \xi_{ij+1}(\underline{x})\, [)), \qquad j = 0, \ldots, l_i$$

depend only on i and not on $\underline{x} \in A_i$ (with the convention $\xi_{i0} = -\infty$ and $\xi_{il_{i+1}} = +\infty$).

Now it remains to show that each ξ_{ij} is semialgebraic and continuous.

The graph of ξ_{ij} is

$$\Gamma(\xi_{ij}) = \{(\underline{x}, y) \in A_i \times R \ : \exists\, (y_1, \ldots, y_{l_i}) \in R^{l_i} (\prod_k f_k(\underline{x}, y_1) = \cdots = \prod_k f_k(\underline{x}, y_{l_i}) = 0 \text{ and } y_1 < \cdots < y_{l_i} \text{ and } y = y_j)\}$$

(where k ranges over the subscripts of those polynomials $f_k(\underline{x}, \mathrm{y})$ that are not identically zero on A_i), and therefore the function ξ_{ij} is semialgebraic.

To show the continuity of ξ_{ij}, fix $\underline{x}_0 \in A_i$. Then $y_j = \xi_{ij}(\underline{x}_0)$ is a simple root of at least one of $\{f_1(\underline{x}_0, \mathrm{y}), \ldots, f_s(\underline{x}_0, \mathrm{y})\}$ (closure under derivatives of the family), say of $f_1(\underline{x}_0, \mathrm{y})$. For $\varepsilon \in R$ small enough,

$$f_1(\underline{x}_0, y_j - \varepsilon) f_1(\underline{x}_0, y_j + \varepsilon) < 0.$$

Hence, in a neighbourhood U of $\underline{x}_0$ in R^n, we have

$$\forall\, \underline{x} \in U \qquad f_1(\underline{x}, y_j - \varepsilon) f_1(\underline{x}, y_j + \varepsilon) < 0$$

and $f_1(\underline{x}, \mathrm{y})$ has a root between $y_j - \varepsilon$ and $y_j + \varepsilon$ is $\xi_{ij}(\underline{x})$. This proves that ξ_{ij} is continuous. $\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (17: 15/12/09)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Decomposition of semialgebraic sets

In the last lecture we proved the following:

Proposition 1.1. *(Main proposition "with coefficients")*
Let $f_1(\underline{\mathrm{x}}, \mathrm{y}), \ldots, f_s(\underline{\mathrm{x}}, \mathrm{y})$ be polynomials in $n+1$ variables with coefficients in R. Let $q := \max_{i=1,\ldots,s}\{\deg \text{ in } \mathrm{y} \text{ of } f_i(\underline{\mathrm{x}}, \mathrm{y})\}$ and $w \in W_{s,q}$.

Then there exists a boolean combination $B_w(\underline{\mathrm{x}})$ of polynomial equations and inequalities in the variables $\underline{\mathrm{x}}$ with coefficients in R such that for any $\underline{x} \in R^n$,

$$\mathrm{sign}_R(f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})) = w \;\Leftrightarrow\; B_w(\underline{x}) \text{ is satisfied in } R.$$

Theorem 1.2. *Let $\underline{\mathrm{x}} = (\mathrm{x}_1, \ldots, \mathrm{x}_n)$. Let $f_1(\underline{\mathrm{x}}, \mathrm{y}), \ldots, f_s(\underline{\mathrm{x}}, \mathrm{y})$ be polynomials in $n+1$ variables with coefficients in R. Then there exixts a partition of R^n into a finite number of semialgebraic sets*

$$R^n = A_1 \,\dot\cup\, \cdots \,\dot\cup\, A_m$$

and for each $i = 1, \ldots, m$ there exists a finite number (possibly 0) of continuous semialgebraic functions $\xi_{i1}, \ldots, \xi_{il_i}$ defined on A_i with

$$\xi_{i1} < \cdots < \xi_{il_i}$$

$$\xi_{ij} \colon A_i \longrightarrow R$$

and $\xi_{ij}(\underline{x}) < \xi_{ij+1}(\underline{x})$ for all $\underline{x} \in A_i$, for all $j = 1, \ldots, l_i$, such that

(i) *for each $\underline{x} \in A_i$, $\{\xi_{i1}(\underline{x}), \ldots, \xi_{il_i}(\underline{x})\} = \{$roots of those polynomials among $f_1(\underline{x}, \mathrm{y}), \ldots, f_s(\underline{x}, \mathrm{y})$ which are not identically zero$\}$;*

(ii) *for each $\underline{x} \in A_i$ and $y \in R$, $\mathrm{sign}(f_1(\underline{x}, y)), \ldots, \mathrm{sign}(f_s(\underline{x}, y))$ depend only on $\mathrm{sign}(y - \xi_{i1}), \ldots, \mathrm{sign}(y - \xi_{il_i})$.*

Definition 1.3. Let $f_1(\underline{x}, y), \ldots, f_s(\underline{x}, y)$ be polynomials in $n+1$ variables with coefficients in R. A partition of R^n into a finite number of semialgebraic sets

$$R^n = A_1 \dot\cup \cdots \dot\cup A_m$$

together with continuous semialgebraic functions

$$\xi_{i1} < \cdots < \xi_{il_i} \colon A_i \longrightarrow R$$

satisfying properties (i) and (ii) of Theorem 1.2 is called a **slicing** of $f_1, \ldots, f_s$ and is denoted by

$$(A_i \ ; \ (\xi_{ij})_{j=1,\ldots,l_i})_{i\in\{1,\ldots,m\}}$$

If the $A_1, \ldots, A_m$ are given by boolean conbinations on the polynomials $g_1, \ldots, g_t \in R[x_1, \ldots, x_n]$, we say that the $g_1, \ldots, g_t$ **slice** the $f_1, \ldots, f_s$.

Lemma 1.4. *Let $f_1(\underline{x}, y), \ldots, f_s(\underline{x}, y)$ be polynomials in $R[\underline{x}, y]$ and $(A_i \ ; \ (\xi_{ij})_{j=1,\ldots,l_i})_{i\in\{1,\ldots,m\}}$ a slicing of $f_1, \ldots, f_s$. Then for every i, $1 \leqslant i \leqslant m$, and every j, $0 \leqslant j \leqslant l_i$, the slice*

$$]\xi_{ij}, \xi_{ij+1}[:= \{(\underline{x}, y) \in R^{n+1} : \underline{x} \in A_i \text{ and } \xi_{ij}(\underline{x}) < y < \xi_{ij+1}(\underline{x})\}$$

is semialgebraic and semialgebraically homeomorphic to $A_i \times]0,1[$ (with the convention $\xi_{i0} = -\infty$ and $\xi_{il_{i+1}} = +\infty$).

Proof. Each slice is semialgebraic, since A_i and the functions ξ_{ij}, $j = 1, \ldots, l_i$ are semialgebraic. We now give explicity the semialgebraic homeomorphism

$$h \colon]\xi_{ij}, \xi_{ij+1}[\longrightarrow A_i \times]0,1[.$$

For $j = 1, \ldots, l_i - 1$ define:

$$h(\underline{x}, y) = (\underline{x}, \ (y - \xi_{ij}(\underline{x}))/(\xi_{ij+1}(\underline{x}) - \xi_{ij}(\underline{x}))).$$

For $j = 0$, $\xi_{i0} = -\infty$, define (if $l_i \neq 0$):

$$h(\underline{x}, y) = (\underline{x}, \ (1 + \xi_{i,1}(\underline{x}) - y)^{-1}).$$

For $j = l_i \neq 0$, $\xi_{il_{i+1}} = +\infty$, define:

$$h(\underline{x}, y) = (\underline{x}, \ (y - \xi_{i,l_i}(\underline{x}) + 1)^{-1}).$$

If $l_i = 0$, $\xi_0 = -\infty$ and $\xi_1 = +\infty$, define:

$$h(\underline{x}, y) = (\underline{x}, \ (y + \sqrt{1+y^2})/2\sqrt{1+y^2}).$$

□

Theorem 1.5. *Every semialgebraic subset of R^n is the disjoint union of a finite number of semialgebraic sets, each of them semialgebraically homeomorphic to an open hypercube $]0,1[^d \subset R^d$, for some $d \in \mathbb{N}$ (where $]0,1[^0$ is a point).*

Proof. By induction on n.

For $n = 1$, we already know that every semialgebraic subset of R is the union of a finite number of points and open intervals. Open intervals are semialgebraically homeomorphic to $]0,1[$ and a point is semialgebraically homeomorphic to $]0,1[^0$.

We now assume that the result holds for n. Let S be a semialgebraic subset of R^{n+1}, given by a boolean combination of sign conditions on the polynomials $f_1, \ldots, f_s$, and let $(A_i \ ; \ (\xi_{ij})_{j=1,\ldots,l_i})_{i\in\{1,\ldots,m\}}$ be a slicing of $f_1, \ldots, f_s$.

By induction, all A_i are semialgebraically homeomorphic to open hypercubes. Moreover, S is the union of a finite number of semialgebraic sets that are either the graph of a function ξ_{ij}, or a slice $]\xi_{ij}, \xi_{ij+1}[$ as in Lemma 1.4.

The graph of ξ_{ij} is semialgebraically homeomorphic to A_i, while, by Lemma 1.4, the slice $]\xi_{ij}, \xi_{ij+1}[$ is semialgebraically homeomorphic to $A_i \times]0,1[$. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (18: 17/12/09)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Semialgebraic connectedness

In the last lecture we showed:

Theorem 1.1. *Every semialgebraic subset of R^n is the disjoint union of a finite number of semialgebraic sets, each of them semialgebraically homeomorphic to an open hypercube $]0,1[^d \subset R^d$, for some $d \in \mathbb{N}$ (where $]0,1[^0$ is a point).*

Question 1.2. Are the $]0,1[^d$ connected? (equivalently is R^d connected?)

If $R = \mathbb{R}$ yes, but in general no, because if $R \neq \mathbb{R}$ then R is not Dedekind complete and therefore is disconnected.

So what is a reasonable notion of connectedness for semialgebraic sets?

Definition 1.3. Let $A \subset R^n$ be a semialgebraic set. We say that A is **semialgebraic connected** (*semialgebraisch zusammenhängend*) if the following equivalent conditions hold:

(1) A is not the disjoint union of two non-empty semialgebraic open (relatively to A) subsets of A.

(2) There are no semialgebraic open sets U_1, U_2 of R^n such that

$$U_1 \cap A \neq \emptyset \qquad U_2 \cap A \neq \emptyset$$
$$U_1 \cap U_2 \cap A = \emptyset \quad \text{and} \quad (U_1 \cup U_2) \cap A = A.$$

(3) If A_1, A_2 are disjoint semialgebraic subsets of A with $A = A_1 \cup A_2$ and A_1, A_2 are open in A, then

$$\text{either } A_1 = \emptyset \quad \text{or } A_2 = \emptyset.$$

(4) Whenever $F_1 \subseteq A$, $F_2 \subseteq A$ are semialgebraic and closed in A with $F_1 \dot\cup F_2 = A$, then

$$F_1 = A \quad \text{or} \quad F_2 = A.$$

Remark 1.4.

(*i*) A subset $A \subseteq R^n$ is connected if it is not the disjoint union of two nonempty open (relatively to A) subsets of A. So for any semialgebraic set A,

$$A \text{ connected } \Rightarrow \ A \text{ semialgebraic connected.}$$

(*ii*) Every interval in R is semialgebraic connected, so

$$A \text{ semialgebraic connected } \not\Rightarrow \ A \text{ connected.}$$

(*iii*) The property of being semialgebraic connected (as the property of being connected) is preserved under semialgebraic homeomorphisms.

Theorem 1.5.

(*a*) *Assume A, $B \subset R^n$ semialgebraic connected with $A \cap \bar{B} \neq \emptyset$. Then $A \cup B$ is semialgebraic connected.*

(*a′*) *If A and B are semialgebraic, with $A \subseteq B \subseteq \bar{A}$,*

$$A \text{ semialgebraic connected } \Rightarrow \ B \text{ semialgebraic connected.}$$

(*b*) *$A \subseteq R^m$, $B \subseteq R^n$ semialgebraic connected $\Rightarrow$ $A \times B \subseteq R^{n+m}$ semialgebraic connected.*

(*c*) *If $A \subseteq R^m$ semialgebraic connected and $f\colon A \to R^n$ a continuous semialgebraic map, then $f(A) \subseteq R^n$ is semialgebraic connected.*

Proof.

(*a*) Let $A \cup B = U \dot\cup V$ with U, V semialgebraic and open in $A \cup B$. Assume for a contradiction U, $V \neq \emptyset$, say without loss of generality $A \cap U \neq \emptyset$. Since A is semialgebraic connected, we must have $A \subseteq U$. Therefore $A \cap V = \emptyset$, $V \subseteq B$ and B semialgebraic connected $\Rightarrow$ $V = B$ and $U = A$. So A, B are open in $A \cup B$ and disjoint. Therefore $A \cap \bar{B} = \emptyset$, contradiction.

(*a′*) Exercise.

(*b*) Let $A \times B = U \dot\cup V$ with U, V semialgebraic and open in $A \times B$. Set

$$A_1 := \{x \in A : \{x\} \times B \subseteq U\}.$$
$$A_2 := \{x \in A : \{x\} \times B \subseteq V\}.$$

Since B is semialgebraic connected, $A = A_1 \dot\cup A_2$. Now $A - A_1 = \pi_1(V)$ is open in A. Therefore A_1 is closed in A, A_2 is closed in A. But A_1, A_2 semialgebraic and A semialgebraic connected $\Rightarrow$ $A_1 = \emptyset$ or $A_2 = \emptyset$, so $U = \emptyset$ or $V = \emptyset$.

(*c*) Exercise.

□

2. Semialgebraic connected components

Proposition 2.1. *Let $A \subseteq R^n$ be non-empty semialgebraic. There are finitely many pairwise disjoint $A_1, \ldots, A_r$ semialgebraic connected, semialgebraic subsets of A which are all open (therefore all closed) in A with*

$$A = A_1 \dot\cup \cdots \dot\cup A_r$$

and this decomposition is unique (up to permutation).

Proof. We know $A = C_1 \dot\cup \cdots \dot\cup C_m$ with $C_i \approx R^d$ semialgebraic, semialgebraic connected $C_i \neq \emptyset$. We proceed by induction on m.

- $m = 1$. It is clear.
- $m > 1$. If C_1 is open and closed in A, we can use induction on $C_2 \cup \cdots \cup C_m$. Otherwise $\exists\, i \in \{2, \ldots, m\}$ such that $\bar{C_1} \cap C_i \neq \emptyset$ or $C_1 \cap \bar{C_i} \neq \emptyset$. In both cases we get $C_1 \cup C_i$ semialgebraic connected (by 1.5(1.4)(*a*)) and we are done by induction again.

Uniqueness: Suppose $A = A_1 \dot\cup \cdots \dot\cup A_r = A'_1 \dot\cup \cdots \dot\cup A'_q$ with each A_i and each A'_j open and closed in A and semialgebraic connected. Then each A_i is contained in exactly one A'_j and viceversa every A'_j is contained in exactly one A_i (Exercise).

□

Definition 2.2. The $A_1, \ldots, A_r$ are called the **semialgebraic connected components** of the semialgebraic set $A \subset R^n$.

Remark 2.3. A semialgebraic subset of $\mathbb{R}^n$ is semialgebraic connected if and only if it is connected, so every semialgebraic subset of $\mathbb{R}^n$ has a finite number of connected components which are semialgebraic.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (19: 22/12/09)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Motivation

Theorem 1.1. *(**Curve-selection Lemma**: Kurvenauswahllemma) Let A be a semialgebraic subset of R^n, $x \in R^n$, $x \in \bar{A} = \mathrm{clos}(A)$. Then there exists a continuous semialgebraic map $f\colon [\,0,1\,] \to R^n$ such that $f(0) = x$ and $f(]\,0,1\,]) \subset A$.*

This has important consequences such as

(1) The image of a closed and bounded semialgebraic set under a continuous semialgebraic map is a closed and bounded semialgebraic set.

(2) A semialgebraic set is semialgebraic connected if and only if it is semialgebraic **path connected** (*wegzusammenhängend*).

2. Closed and bounded semialgebraic sets

Definition 2.1. A subset $A \subseteq R^n$ is **bounded** if $\exists\, r \in R$ such that $||a|| < r$ $\forall\, a \in A$.

We have seen that for $R \neq \mathbb{R}$ we have to replace the notion of "connected" by "semialgebraic connected".

Similarly the notion of compactness is problematic for $R \neq \mathbb{R}$. In fact, closed and bounded subsets of R need not be compact.

Example 2.2. Let $R = \mathbb{R}_{alg} = \{\text{real algebraic numbers}\} = \text{the real closure of } \mathbb{Q} \text{ in } \mathbb{R}$. The interval $[0,1] \subseteq R$ is not compact. For example the set

$$\mathcal{U} = \{\, [0,r[\subset R \;: r < \pi/4 \,\} \cup \{\,]s,1] \subset R \;: s > \pi/4 \,\}$$

is an open cover of $[0,1]$ by semialgebraic subsets of R and it is not possible to extract from it a finite subcover!

This example shows that, unlike the notion of semialgebraic connectness, a notion of of semialgebraic compactness given just with semialgebraic open coverings is not appropriate. Instead, we shall suffice ourselves with studying "closed and bounded" semialgebraic sets and bounded semialgebraic functions.

Definition 2.3. A function $f\colon A \to R$ is **bounded** if $\forall\, a \in A\ \exists\, r \in R$ with $||f(a)|| < r$.

Proposition 2.4. *Let $r \in R$, $r > 0$ and $\varphi\colon]0, r] \to R$ a continuous bounded semialgebraic function. Then φ extends to a continuous function on $[0, r]$.*

For the proof we need the following lemma:

Lemma 2.5. *Let $A \subseteq R$ be a semialgebraic set and $\varphi\colon A \to R$ a semialgebraic function. Then there exists a non-zero polynomial $f \in R[\mathrm{x}, \mathrm{y}]$ such that f vanishes on $\Gamma(\varphi)$, i.e.*

$$\forall\, x \in A \quad f(x, \varphi(x)) = 0.$$

(For its proof see Lemma 1.1 of Lecture 21)

Proof of Proposition 2.4. Assuming Lemma 2.5, let $f \in R[\mathrm{x}, \mathrm{y}]$ be a non-zero polynomial such that f vanishes on $\Gamma(\varphi)$. We shall proceed by induction on $d = \deg f$ in y.

Suppost first $d = 1$. We write

$$f = Q_1(\mathrm{x})\mathrm{y} + Q_0(\mathrm{x}), \quad Q_0, Q_1 \in R[\mathrm{x}], \quad Q_1 \not\equiv 0.$$

We have that

$$f(x, \varphi(x)) = 0 \ \Rightarrow\ Q_1(x)\varphi(x) + Q_0(x) = 0 \qquad \forall x \in\,]0, r].$$

We may assume that $Q_1(\mathrm{x})$, $Q_0(\mathrm{x}) \in R[\mathrm{x}]$ are relatively prime (otherwise we divide by the common factor). So we get that

$$\varphi(x) = \frac{-Q_0(x)}{Q_1(x)}$$

(we may assume that $Q_1(x) \neq 0$ for all $x \in\,]0, r]$, otherwise we take an opportune subinterval $]0, r'] \subset\,]0, r]$).

Note that $Q_1(x)$ does not have a zero at $x = 0$ (i.e. x does not divide $Q_1(\mathrm{x})$), otherwise by continuity

$$\lim_{x \to 0^+} \varphi(x) = \pm\infty$$

which contradicts our assumptions that $\exists\, M \in R$ such that $|\varphi(x)| < M$ for all $x \in\,]0, r]$. So we can set

$$\varphi(0) := \frac{-Q_0(0)}{Q_1(0)}$$

and with this new definition the map

$$\varphi\colon [0, r] \ \longrightarrow\ R$$

is continuous.

Let now $d > 1$ and assume the result to be true for $\deg_{\mathrm{y}} f(\mathrm{x},\mathrm{y}) < d$. Without loss of generality we may assume that $f(\mathrm{x},\mathrm{y})$ is not divisible by x. Otherwise, if

$$f(\mathrm{x},\mathrm{y}) = \mathrm{x} f_1(\mathrm{x},\mathrm{y}),$$

we have

$$f(x,\varphi(x)) = x f_1(x,\varphi(x)) = 0 \qquad \forall x \in]0,r],$$

therefore

$$f_1(x,\varphi(x)) = 0 \qquad \forall x \in]0,r]$$

and we can replace f by f_1 if necessary.
Let

$$f' = \frac{\partial f}{\partial \mathrm{y}} \not\equiv 0$$

and let

$$(A_i\ ; \{\xi_{ij}\}_{j=1,\dots,l_i})_{i\in I}$$

be a slicing of $\{f, f'\}$. So A_i is a partition of R in intervals and points. We may assume without loss of generality that $A_1 =]0,r]$ and $\varphi = \xi_{1,j_0}$ (for some r' small enough, i.e. replacing r by r' if necessary).

We have to consider two cases:

- If for $x \in A_1$ $\varphi(x)$ is also a root of $f'(x,\mathrm{y})$ (i.e. f' vanishes on $\Gamma(\varphi)$), then we are done by induction hypothesis, since
$$\deg_{\mathrm{y}} f'(\mathrm{x},\mathrm{y}) < d.$$
- If not, say $\operatorname{sign}(f'(x,\xi_{1j_0}(x))) = \operatorname{sign}(f'(x,\varphi(x))) > 0$ for $x \in]0,r]$.

  <u>*Claim*</u>: There are two continuous semialgebraic functions ρ and θ such that $\rho,\theta\colon [0,r] \to R$ and
  $$\forall\, x \in]0,r] \qquad \rho(x) < \varphi(x) < \theta(x)$$
  and $\operatorname{sign}(f'(x,y))$ is positive for all $y \in]\,\rho(x),\theta(x)\,[\qquad (*)$.

  Proof of Claim. We can take
  $$\rho := \xi_{1j_0-1} \ \text{ and } \ \theta = \xi_{1j_0+1}.$$
  If $\varphi = \xi_{1j_0} = \xi_{11}$ then we can take ρ to be the constant function $-(M+1)$, where M is the bound for φ.
  If $j_0 = l_1$ we can take θ to be the constant function $M+1$.

  Note that these functions are roots of the derivative f', and $\deg f' < d$ in y, so by induction hypothesis the continuous semialgebraic maps ρ and θ can be extended to $[0,r]$ since f' vanishes on $\Gamma(\rho)$ and $\Gamma(\theta)$). □

Now consider $\rho(0)$ and $\theta(0)$: by continuity we have $\rho(0) \leqslant \theta(0)$.

- If $\rho(0) = \theta(0)$, set $\varphi(0) = \rho(0)$. This gives a continuous extension of φ to $[0, r]$.

- Otherwise $\rho(0) < \theta(0)$. Consider the function $f'(0, y)$: it is non-negative for every $y \in [\rho(0), \theta(0)]$ (by continuity together with $(*)$ of Claim).

  Now if $f(0, y)$ is constant, it would be identically zero because we have

$$f(0, \rho(0)) \ \leqslant \ 0 \ \leqslant \ f(0, \theta(0))$$

  but this is impossible since x is not a factor of f.

  So we must have $f'(0, y) > 0$ and the function $f(0, y)$ is strictly increasing and has a unique root $y_0 \in [\rho(0), \theta(0)]$. Set

$$\varphi(0) := y_0.$$

  It remains to show that with this definition φ is continuous at 0 (i.e. that $\lim_{x \to 0^+} \varphi(x) = y_0$).

  Case 1. $\rho(0) < y_0 < \theta(0)$.

  Then for $\varepsilon \in R$, $\varepsilon > 0$ small enough, $f(0, y_0 - \varepsilon) < 0$, $f(0, y_0 + \varepsilon) > 0$, $\rho(0) < y_0 - \varepsilon < y_0 < y_0 + \varepsilon < \theta(0)$. Hence there exists $\eta \in R$, $\eta > 0$ such that for every $x \in]0, \eta[$:

$$\begin{cases} f(x, y_0 - \varepsilon) < 0 \\ f(x, y_0 + \varepsilon) > 0 \\ \rho(x) < y_0 - \varepsilon \\ y_0 + \varepsilon < \theta(x) \end{cases}$$

  Therefore $\varphi(x) \in]y_0 - \varepsilon, y_0 + \varepsilon[$ for every $x \in]0, \eta[$.

  Case 2. $\rho(0) = y_0$.

  We have $f(0, y_0 + \varepsilon) > 0$ for every $\varepsilon \in R$, $\varepsilon > 0$ small enough. Then there exists $\eta \in R$, $\eta > 0$ such that for every $x \in]0, \eta[$:

$$\begin{cases} f(x, y_0 + \varepsilon) > 0 \\ y_0 - \varepsilon < \rho(x) < y_0 - \varepsilon \end{cases}$$

  Again these imply that $\varphi(x) \in]y_0 - \varepsilon, y_0 + \varepsilon[$ for every $x \in]0, \eta[$.

  Case 3. $\theta(0) = y_0$. Analogous.

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (20: 07/01/10)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Recall and plan

During the last lecture we proved that:

Proposition 1.1. *Let $\varphi\colon]0,r[\to R$ be a continuous bounded semialgebraic function defined on an interval $]0,r[\subset R$. Then φ can be continuously extended to 0.*

This was done assuming the following Lemma that we did not yet prove:

Lemma 1.2. *Let $A \subseteq R$ be a semialgebraic set, $\varphi\colon A \to R$ a semialgebraic function. Then there exists a nonzero polynomial $f \in R[\mathrm{x},\mathrm{y}]$ such that for every $x \in A$, $f(x,\varphi(x)) = 0$.*

We shall postpone the proof of the previous Lemma to next lecture, since we want to focus today on the proof of the Curve Selection Lemma. For this we shall further assume Thom's Lemma:

Proposition 1.3. *(Thom's Lemma) Let $f_1,\dots,f_s$ be a family of polynomials in $R[\mathrm{x}]$ closed under derivation. Let $\varepsilon\colon \{1,\dots,s\} \to \{-1,0,1\}$ be a sign condition. Set*

$$A_\varepsilon := \bigcap_{k=1}^{s} \{x \in R : \mathrm{sign}(f_k(x)) = \varepsilon(k)\}.$$

Denote by $A_{\bar\varepsilon}$ the semialgebraic subset of R obtained by relaxing the strict inequalities in A_ε, i.e. :

$$A_{\bar\varepsilon} := \bigcap_{k=1}^{s} \{x \in R : \mathrm{sign}(f_k(x)) = \overline{\varepsilon(k)}\}.$$

where $\bar\varepsilon$ is defined as follows:

$$\bar 0 = \{0\} \qquad \overline{-1} = \{-1,0\} \qquad \bar 1 = \{0,1\}$$

Then

(*i*) *either A_ε is empty, or A_ε is a point, or A_ε is an open interval;*
(*ii*) *if A_ε is nonempty then its closure is $A_{\bar{\varepsilon}}$;*
(*iii*) *if A_ε is empty then $A_{\bar{\varepsilon}}$ is either empty or a point.*

Using Prop 1.1 (proved last time) and Thom's Lemma (to be proved next time) our goal today is to prove the following:

Theorem 1.4. *(**Curve Selection Lemma**) Let A be a semialgebraic subset of R^n, $x \in R^n$, $x \in \bar{A} = \mathrm{clos}(A)$. Then there exists a continuous semialgebraic map $f\colon [\,0,1\,] \to R^n$ such that $f(0) = x$ and $f(]\,0,1\,]) \subset A$.*

Lemma 1.5. *Let $f_1, \ldots, f_s \in R[\mathrm{x}_1, \ldots, \mathrm{x}_n; \mathrm{y}]$ be **quasi-monic** with respect to* y *(i.e. $f_k = a_{d_k}\mathrm{y}^{d_k} + g_{d_k}(\mathrm{x}_1, \ldots, \mathrm{x}_n)\mathrm{y}^{d_k-1} + \cdots + g_0(\mathrm{x}_1, \ldots, \mathrm{x}_n)$ and $a_{d_k} \in R$ is constant). Assume that the set $\{f_1, \ldots, f_s\}$ is closed under derivation with respect to* y.

Let $(A_i \ ; \ (\xi_{ij})_{j=1,\ldots,l_i})_{i=1,\ldots,m}$ be a slicing of $\{f_1, \ldots, f_s\}$. Then every function ξ_{ij} can be continuously extended to the closure of A_i.

We shall prove the CSL and Lemma 1.5 simultaneously by induction on n in the following way. We shall show that:

(*i*) CSL is true for $n = 1$.
(*ii*) CSL for n implies Lemma 1.5 for n.
(*iii*) CSL and Lemma 1.5 for n imply CSL for $n + 1$.

(Clearly once $(i), (ii), (iii)$ are established, CSL and Lemma 1.5 will follow by induction).

2. Proof of the Curve Selection Lemma

(*i*) $n = 1$. Let $x \in \bar{A}$. We may assume $x \notin A$ (otherwise take f to be the constant map $f\colon [0,1] \to R^n$, $f(r) = x \ \forall\, r$).

(By o-minimality) we know that $A \subset R$ semialgebraic is a finite union of intervals and points. So the result is clear in this case (if $x \in \bar{A}$, say x is the endpoint of a (half) open interval I of the form $(x, b] \subset A$ or $(x, b) \subset A$ or $[a, x) \subset A$ or (a, x), in all cases one can define continuous semialgebraic $f\colon [0,1] \to I$ with $f(0) = x$).

(*ii*) Assume CSL holds for n. We show that Lemma 1.5 holds for n.

For fixed i, j and $\underline{x} \in A_i$, we set

$$\varepsilon(k) := \mathrm{sign}(f_k(\underline{x}, \xi_{ij}(\underline{x}))),$$

with $k = 1, \ldots, s$. This is well-defined since $\mathrm{sign}(f_k(x, \xi_{ij}(x)))$ does not depend on $\underline{x} \in A_i$.

Let $\underline{x}' \in \mathrm{clos}(A_i)$. We show that ξ_{ij} can be continuously extended to the semialgebraic set $A_i \cup \{\underline{x}'\}$.

By CSL for n there is $f\colon [0,1] \to R^n$ countinuous and semialgebraic such that $f(0) = \underline{x}'$ and $f(]0,1]) \subset (A_i \cap \bar{B}_n(\underline{x}', 1)) = A$, where $\bar{B}_n(\underline{x}', 1)$ is the n-dimensional closed ball with center $\underline{x}'$ and radius 1, i.e.

$$\bar{B}_n(\underline{x}', 1)) = \{\underline{a} \in R^n \mid \|\underline{a} - \underline{x}'\| \leqslant 1\},$$

which is a closed and bounded semialgebraic set.

Define $\varphi\colon]0,1] \to R$, $\varphi := (\xi_{ij} \circ f_{]0,1]})$. Then φ is continuous and semialgebraic. We want to show that φ is bounded in order to apply Prop 1.1.

Now let $k \in \{1, \dots, s\}$ be such that for $\underline{x} \in A_i$:

$$\xi_{ij}(\underline{x}) \text{ is a root of } f_k(\underline{x}, \mathrm{y}),$$

i.e. say for $\underline{x} \in A_i$, $\xi_{ij}(\underline{x})$ is a root of

$$f_k(\underline{x}, \mathrm{y}) = a_d \mathrm{y}^d + g_{d-1}(\underline{x})\mathrm{y}^{d-1} + \cdots + g_0(\underline{x})$$

By Corollary 2.1 of Lecture 6 we have for $\underline{x} \in A_i$:

$$|\xi_{ij}(\underline{x})| \leqslant 1 + |\frac{g_{d-1}(\underline{x})}{a_d}| + \cdots + |\frac{g_0(\underline{x})}{a_d}|$$

Consider now $\underline{x}$ in the bounded set $A_i \cap \bar{B}_n(\underline{x}', 1))$.

Each polynomial $g_0, \dots, g_{d-1}$ is bounded on this set.

So let $a \in R$ be such that for every $\underline{x} \in A_i \cap \bar{B}_n(\underline{x}', 1))$ we have

$$|g_l(\underline{x})| \leqslant a \qquad \forall\, l = 0, \dots, d-1.$$

Therefore φ is a bounded function. Indeed let $t \in]0,1[$ and compute

$$|\varphi(t)| = |\xi_{ij}(f(t))| \qquad \text{with } \underline{x} = f(t) \in A_i \cap \bar{B}_n(\underline{x}', 1))$$

so

$$|\xi_{ij}(f(t))| \leqslant 1 + |g_{d-1}(f(t))| + \cdots + |g_0(f(t))| \leqslant 1 + \frac{a}{|a_d|} + \cdots + \frac{a}{|a_d|} = 1 + \frac{da}{|a_d|}.$$

We apply Proposition 1.1 to the bounded continuous semialgebraic function φ to extend φ continuously to 0 and we define now

$$\xi_{ij}(\underline{x}') := \varphi(0).$$

Claim. ξ_{ij} is continuous at x'.
We argue by contradiction. If not $\exists\, \mu > 0$, $\mu \in R$ such that

$$\forall\, \eta \in R\ \exists\, \underline{x} \in A_i \ \text{ such that } \ \|\underline{x} - \underline{x}'\| < \eta \ \text{ but } \ |\xi_{ij}(\underline{x}) - \varphi(0)| \geqslant \mu.$$

Consider

$$C_\mu = \{\underline{x} \in A_i \mid |\xi_{ij}(\underline{x}) - \varphi(0)| \geqslant \mu\} \cap \bar{B}_n(\underline{x}', 1)$$

Since $\underline{x}' \in \mathrm{clos}(C_\mu) \subset R^n$, we can apply CSL to have a continuous semialgebraic function

$$g\colon [0,1] \longrightarrow R^n$$

with $g(0) = \underline{x}'$ and $g(]0,1]) \subset C_\mu$. We now consider

$$\psi\colon]0,1] \to R, \quad \psi := (\xi_{ij} \circ g_{]0,1]}).$$

As before ψ can be continuously extended to 0.

Subclaim.

(•) $|\varphi(0) - \psi(0)| \geqslant \mu$.

(••) For every $k = 1, \ldots, s$

$$\operatorname{sign} f_k(\underline{x}', \varphi(0)) \in \overline{\varepsilon(k)}$$

$$\operatorname{sign} f_k(\underline{x}', \psi(0)) \in \overline{\varepsilon(k)}.$$

Proof of the Subclaim.

(•) For every $t \in]0, 1]$, $\psi(t) = \xi_{ij}(g(t)) = \xi_{ij}(\underline{x})$ for some $\underline{x} \in C_\mu$. Therefore $|\varphi(t) - \psi(0)| \geqslant \mu$ for every $t \in]0, 1]$ and by continuity of ψ, $|\varphi(0) - \psi(0)| \geqslant \mu$.

(••) Let $k \in \{1, \ldots, s\}$.

If $\varepsilon(k) = 0$, then $f_k(\underline{x}, \xi_{ij}(\underline{x})) = 0$ for all $\underline{x} \in A_i$, so by continuity

$$\begin{cases} f_k(\underline{x}', \varphi(0)) = 0 & \text{and} \\ \\ f_k(\underline{x}', \psi(0)) = 0. \end{cases}$$

Similarly if $\varepsilon(k) = -1$, then $f_k(\underline{x}, \xi_{ij}(\underline{x})) < 0$ for all $\underline{x} \in A_i$, so by continuity

$$\begin{cases} f_k(\underline{x}', \varphi(0)) \geqslant 0 & \text{and} \\ \\ f_k(\underline{x}', \psi(0)) \geqslant 0. \end{cases}$$

and finally if $\varepsilon(k) = 1$, then $f_k(\underline{x}, \xi_{ij}(\underline{x})) > 0$ for all $\underline{x} \in A_i$ and

$$\begin{cases} f_k(\underline{x}', \varphi(0)) \geqslant 0 & \text{and} \\ \\ f_k(\underline{x}', \psi(0)) \geqslant 0. \end{cases}$$

□

Consider now the set

$$\{y \in R \,|\, \operatorname{sign}(f_k(\underline{x}', y)) \in \bar{\varepsilon}(k),\ k = 1, \ldots, s\}.$$

By Thom's Lemma this set is either empty or reduces to a point. On the other hand $\varphi(0) \neq \psi(0)$ and bot $\varphi(0)$, $\psi(0)$ belong to this set by the subclaim, contradiction. Therefore ξ_{ij} is continuous at $\underline{x}'$.

(*iii*) We assume CSL and Lemma 1.5 to be true for n and show that CSL is true for $n + 1$.

Let $A \subseteq R^{n+1}$ semialgebraic given by a boolean combination of sign conditions on $f_1, \ldots, f_s \in R[\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{y}]$.

Claim. We may assume that $f_1, \ldots, f_s$ are quasi-monic and that the family is closed under derivation, so that $f_1, \ldots, f_s$ satisfy the conditions of Lemma 1.5.

Let $(A_i \,; \{\xi_{ij}\}_{j=1,\ldots,l_i})_{i=1,\ldots m}$ be a slicing of $f_1, \ldots, f_s$. So $A_i \subset R^n$ for every $i = 1, \ldots, m$ and the set A is the union of the graphs of some functions ξ_{ij} and some slices $]\xi_{ij},\, \xi_{ij+1}[$.

Let $(\underline{x}, y) \in \mathrm{clos}(A) \subseteq R^{n+1}$. We have to consider the following cases:

(1) $(\underline{x}, y) \in \mathrm{clos}(\Gamma(\xi_{ij}))$, $\xi_{ij} \colon A_i \to R$.

(2) $(\underline{x}, y) \in \mathrm{clos}(\,]\xi_{ij},\, \xi_{ij+1}[\,)$, where $1 < j < l_i$.

(3) $(\underline{x}, y) \in \mathrm{clos}(\,]\xi_{ij},\, \xi_{ij+1}[\,)$, where $j = 1$ or $j = l_i$.

Case 1. Let $(\underline{x}, y) \in \mathrm{clos}(\Gamma(\xi_{ij}))$, $\xi_{ij} \colon A_i \to R$, with $\Gamma(\xi_{ij}) \subseteq A$. Applying the CSL, let $\varphi \colon [0,1] \to R^n$ be a continuous and semialgebraic map such that $\varphi(0) = \underline{x}$ and $\varphi(]0,1]) \subseteq A_i$.

We can use Lemma 1.5 for n to extend ξ_{ij} at $\underline{x}$ continuously. So we must have $\xi_{ij}(\underline{x}) = y$.

Now set

$$\psi \colon [0,\, 1] \;\xrightarrow{\;\varphi\;}\; A_i \cup \{\underline{x}\} \;\xrightarrow{\;\xi_{ij}\;}\; R$$

and $f := (\varphi, \psi)$. f is continuous semialgebraic, $f(0) = (\varphi(0), \psi(0)) = (\underline{x}, y)$ and $f(]0,\, 1]) \subseteq A$.

Case 2. $(\underline{x}, y) \in \mathrm{clos}(\,]\xi_{ij},\, \xi_{ij+1}[\,)$, where $1 < j < l_i$, with $]\xi_{ij},\, \xi_{ij+1}[\subseteq A \subseteq R^{n+1}$, $\xi_{ij}, \xi_{ij+1} \colon A_i \to R$.

By CSL for n let $\varphi \colon [0,\, 1] \to R^n$ be a continuous semialgebraic map with $\varphi(0) = \underline{x}$ and $\varphi(]0,1]) \subseteq A_i$.

By Lemma 1.5 for n extend the function ξ_{ij} and ξ_{ij+1} continuously to $\underline{x}$:

$$\begin{aligned} \xi_{ij} \colon A_i \cup \{\underline{x}\} &\longrightarrow R \qquad \xi_{ij}(\underline{x}) \in R \\ \xi_{ij+1} \colon A_i \cup \{\underline{x}\} &\longrightarrow R \qquad \xi_{ij+1}(\underline{x}) \in R \end{aligned}$$

Set

$$t := \begin{cases} 1/2 & \text{if } \xi_{ij}(\underline{x}) = \xi_{ij+1}(\underline{x}) \\ \\ \frac{y - \xi_{ij}(\underline{x})}{\xi_{ij+1}(\underline{x}) - \xi_{ij}(\underline{x})} & \text{if } \xi_{ij}(\underline{x}) \neq \xi_{ij+1}(\underline{x}) \end{cases}$$

and $\psi\colon [(1-t)\xi_{ij} + t(\xi_{ij+1})] \circ \varphi$. Then ψ is continuous semialgebraic and $\psi(0) = y$. Set $f := (\varphi, \psi)$. f is continuous and semialgebraic, with $f(0) = (\varphi(0), \psi(0)) = (\underline{x}, y)$ and $f(]0,\, 1]) \subseteq A$.

Case 3. Exercise.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (21: 12/01/10)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Thom's Lemma

Lemma 1.1. *Let $A \subset R$ be a semialgebraic set and $\varphi\colon A \to R$ a semialgebraic function. Then exists $f \in R[\mathrm{x}, \mathrm{y}]$, $f \neq 0$, such that*

$$\forall\, x \in A \qquad f(x, \varphi(x)) = 0 \qquad (f \text{ vanishes on the graph of } \varphi).$$

Proof. The graph of φ $\Gamma(\varphi) = \{(x, \varphi(x)) : x \in A\} \subset R^2$ is a semialgebraic set, so it is a finite union of sets of the form

$$\{(x, y) \in R^2 : f_i(x, y) = 0,\ i = 1, \ldots, l\ g_j(x, y) > 0,\ j = 1, \ldots, m\}$$

with at least one among the $f_i \neq 0$, otherwise $\Gamma(\varphi)$ would contain an open subset of R^2, contradiction.

Now take f to be the product of these nonzero polynomials. □

Proposition 1.2. *(Thom's Lemma) Let $\{f_1, \ldots, f_s\}$ be a family of non-zero polynomials in $R[X]$ closed under derivation. Let $\varepsilon\colon \{1, \ldots, s\} \to \{-1, 0, 1\}$ be a sign function. Set*

$$A_\varepsilon := \{x \in R : \mathrm{sign}(f_k(x)) = \varepsilon(k),\ k = 1, \ldots, s\}.$$

Denote by $A_{\bar{\varepsilon}}$ the semialgebraic subset of R obtained by relaxing the strict inequalities in A_ε, i.e. :

$$A_{\bar{\varepsilon}} := \bigcap_{k=1}^{s} \{x \in R : \mathrm{sign}(f_k(x)) \in \bar{\varepsilon}(k)\}.$$

where $\bar{\varepsilon}$ is defined as follows:

$$\bar{0} = \{0\} \qquad -\bar{1} = \{-1, 0\} \qquad \bar{1} = \{0, 1\}.$$

Then

(*i*) *either A_ε is empty, or A_ε is a point, or A_ε is a non-empty open interval (if A_ε is empty or a point, then $\varepsilon(k) = 0$ for some k; if A_ε is a non-empty open interval then $\varepsilon(k) = \pm 1$ for every k);*

(*ii*) *if A_ε is non-empty then its closure is $A_{\bar{\varepsilon}}$ (which is either a point or a closed interval different from a point and the interior of this interval is A_ε);*

(*iii*) *if A_ε is empty then $A_{\bar{\varepsilon}}$ is either empty or a point.*

Proof. By induction on s. The Lemma holds trivially for $s = 0$. Let $f_1, \ldots, f_s, f_{s+1} \in R[\mathrm{x}] \setminus \{0\}$ be polynomials such that if $f_k' \neq 0$, then $f_k' \in \{f_1, \ldots, f_{s+1}\}$. Without loss of generality we assume that $\deg(f_{s+1}) = \max\{\deg(f_k) : 1 \leqslant k \leqslant s+1\}$.

Let $\varepsilon' \colon \{1, \ldots, s, s+1\} \to \{-1, 0, 1\}$ and $\varepsilon \colon \{1, \ldots, s, \} \to \{-1, 0, 1\}$ the restriction.

Note that

$$A_{\varepsilon'} = A_\varepsilon \cap \{x \in R : \mathrm{sign}(f_{s+1}(x)) = \varepsilon'(s+1)\}.$$

By induction A_ε is empty, a point, or an interval.

If A_ε is empty or a point, then obviously so is $A_{\varepsilon'}$ and the other property follows immediately by induction hypothesis on A_ε.

Assume A_ε is an interval. Now $f_{s+1}' = 0$ or $f_{s+1}' \in \{f_1, \ldots, f_s\}$. So by definition of A_ε, f_{s+1}' has constant sign on A_ε. Therefore f_{s+1} is either strictly increasing, or strictly decreasing or constant on A_ε.

Consider $A_\varepsilon = (a, b)$ There are three cases depending on $\varepsilon'(s+1)$:

Case 1. $A_{\varepsilon'} = \{x \in (a, b) : f_{s+1}(x) > 0\}$.

Case 2. $A_{\varepsilon'} = \{x \in (a, b) : f_{s+1}(x) < 0\}$.

Case 3. $A_{\varepsilon'} = \{x \in (a, b) : f_{s+1}(x) = 0\}$.

If $A_{\varepsilon'} = \emptyset$ there is nothing to prove.

Assume $A_{\varepsilon'} \neq \emptyset$. If f_{s+1} is constant on A_ε then f_{s+1} is a constant polynomial $f_{s+1}(x) = c \neq 0$. So $A_{\varepsilon'}$ is empty or $A_{\varepsilon'} = (a, b)$ depending on whether $\mathrm{sign}(c) = \varepsilon'(s+1)$.

Assume now f_{s+1} strictly increasing on A_ε and $A_{\varepsilon'} = \{x \in (a, b) : f_{s+1}(x) > 0\} \neq \emptyset$. Let $x_0 = \inf\{x \in (a, b) : f_{s+1}(x) > 0\}$. Since f_{s+1} is strictly increasing it follows that $f_{s+1}(x) > 0 \ \forall\, x \in (a, b)$ with $x > x_0$. So $A_{\varepsilon'} = (x_0, b)$ and its closure is $[x_0, b] = A_{\bar{\varepsilon'}}$. The other cases are treated similarly. □

2. Semialgebraic path connectedness

Definition 2.1. Let $A \subseteq R^n$ be a semialgebraic set.

(1) A **semialgebraic path** in A is a continuous semialgebraic map

$$\alpha\colon I \longrightarrow A,$$

where I is either $[0,1]$ or $]0,1[$.

(2) Let $x, y \in A$. We say that x is semialgebraic path connected to y if there exists a semialgebraic path in A

$$\alpha\colon [0,1] \longrightarrow A$$

with $\alpha(0) = x$ and $\alpha(1) = y$.

Remark 2.2. Note that "x is semialgebraic path connected to y" is an equivalence relation on A:

To see simmetry observe that if α is a path from x to y then

$$\alpha^*(t) := \alpha(1-t)$$

defines a path from y to x.

To see transitivity observe that if α is a path from x to y and β is a path from y to z, then

$$\gamma(t) := \begin{cases} \alpha(2t) & 0 \leqslant t \leqslant 1/2 \\ \beta(2t-1) & 1/2 \leqslant t \leqslant 1 \end{cases}$$

is a path from x to z.

(3) A is **semialgebraic path connected** if any two points in A are semialgebraic path connected.

Proposition 2.3. *Let A be a semialgebraic set. Then*

A is semialgebraic connected $\iff$ A is semialgebraic path connected.

Proof.

($\Rightarrow$) Suppose A is a semialgebraic connected set and let

$$A = \bigcup_{i=1}^{n} C_i$$

a semialgebraic cell decomposition of A (so each C_i is semialgebraic path connected). Then we have seen that there is an equivalence relation on $\{C_i : i = 1, \ldots, n\}$ given by:

$$\begin{aligned} C_i \sim C_j \Leftrightarrow \exists\, C_{i_0}, \ldots, C_{i_q} \text{ such that } C_{i_0} = C_i,\ C_{i_q} = C_j \text{ and} \\ C_{i_k} \cap \bar{C}_{i_{k+1}} \neq \emptyset \text{ or } \bar{C}_{i_k} \cap C_{i_{k+1}} \neq \emptyset \ \ \forall\, 0 \leqslant k < q, \end{aligned}$$

such that the equivalence classes with respect to this equivalence relation are the semialgebraic connected component of S. Since A is semialgebraic connected there is only one equivalence class.

Claim 1. If C is a semialgebraic path connected set, also the closure $\bar{C}$ of C is semialgebraic path connected (it is an immediate

consequence of the Curve Selection Lemma).

Claim 2. If $A_1, A_2 \subseteq R^n$ are semialgebraic path connected with $A_1 \cap A_2 \neq \emptyset$, then $A_1 \cup A_2$ is semialgebraic path connected.

So let $x, y \in A$. We want to find a semialgebraic path in A joining x and y. Let $x \in C_i$ and $y \in C_j$ and $C_{i_0}, \ldots, C_{i_q}$ as above. For every $0 \leqslant k < q$, let $a_k \in C_{i_k} \cap \bar{C}_{i_{k+1}}$ or $a_k \in \bar{C}_{i_k} \cap C_{i_{k+1}}$. By Claim 1 and Claim 2 we can find semialgebraic paths joining a_k with a_{k+1} for every $0 \leqslant k < q$ and conclude joining x with a_0 (since $C_i = C_{i_0}$ is semialgebraic path connected) and a_{q-1} with y (since $C_j = C_{i_q}$ is semialgebraic path connected).

($\Leftarrow$) **Claim.** If A is path connected then A is connected.

Suppose for a contradiction that A is a disjoint union of non-empty open sets A_1 and A_2. Take $x \in A_1$, $y \in A_2$ and $\varphi : [0,1] \to A$ a continuous function such that $\varphi(x) = 0$ and $\varphi(y) = y$ (it exists because A is path connected).

Now consider $X_1 := [0,1] \cap \varphi^{-1}(A_1)$ and $X_2 := [0,1] \cap \varphi^{-1}(A_2)$. Then X_1 and X_2 disconnect $[0,1]$, contradiction.

So we have:

A semialg. path conn. $\Rightarrow$ A path conn. $\Rightarrow$ A conn. $\Rightarrow$ A semialg. conn.

□

The semialgebraic assumption is essential to prove ($\Rightarrow$), as the following example shows:

Example 2.4. Let $\Gamma = \{(x,\ \sin(1/x) : x > 0\} \subset \mathbb{R}^2$ and consider $A = \{(0,0)\} \cup \Gamma$. Note that $(0,0)$ is in the closure $\bar{\Gamma}$ of Γ. Then A is connected but it is not path connected: there is no continuous function inside A joining $\{(0,0)\}$ with a point of Γ.

3. Semialgebraic compactness

Definition 3.1. A semialgebraic set $A \subset R^n$ is **semialgebraic compact** if for every semialgebraic path $\alpha\colon]0,1[\longrightarrow A$,

$$\exists \lim_{t \to 0^+} \alpha(t) \in A.$$

Theorem 3.2. *Let $A \subseteq R^n$ be a semialgebraic set. Then*

A is semialgebraic compact $\iff$ *A is closed and bounded.*

Proof.

($\Leftarrow$) Let $A \subseteq R^n$ be closed and bounded and $\alpha\colon]0,1[\to A$ a semialgebraic path.

Since A is bounded, α can be continuously extended to 0, so

$$\exists \lim_{t\to 0^+} \alpha(t) = x \in R^n$$

and $x = \alpha(0)$.

But A is closed, then $\alpha(0) \in A$.

($\Rightarrow$) Assume A is semialgebraic compact and suppose for a contradiction that A is not closed.

Let $x \in \bar{A}$, $x \notin A$. By the Curve Selection Lemma there is a semialgebraic continuous function $f\colon [0,1] \to R^n$ such that $f(]0,1]) \subset A$ and $f(0) = x$. Therefore

$$x = \lim_{t\to 0^+} f(t),$$

and $x \in A$, since A is semialgebraic compact. Contradiction.

To show that A is bounded we use the following corollary to the Curve Selection Lemma:

Corollary 3.3. *Let $A \subseteq R^n$ be an unbounded semialgebraic set. Then there is a semialgebraic path $\alpha\colon]0,1[\to A$ with*

$$\lim_{t\to 0} |\alpha(t)| = \infty.$$

□

The following Theorem and its Corollory is a particular indication that the notion of "semialgebraic compactness" is the correct analogue to usual compactness, adapted to the semialgebraic setting:

Theorem 3.4. *Let A, B semialgebraic sets and $f\colon A \to B$ a semialgebraic continuous map. Then*

$$A \text{ semialgebraic compact } \Rightarrow \ f(A) \text{ semialgebraic compact }.$$

Proof. We assume the following Lemma:

Lemma 3.5. *Let $f\colon A \to B$ be a semialgebraic map with A, B semialgebraic sets. Let $\beta\colon]0,1[\to B$ be a semialgebraic path in B with $\beta(]0,1[) \subseteq f(A)$. Then there is $0 < c \leqslant 1$ and a semialgebraic continuous function $\alpha\colon]0,c[\to A$ such that $\beta(t) = f(\alpha(t))$ for every $0 < t < c$.*

Let $\beta\colon]0,1[\to f(A)$ be a semialgebraic path. We want to show that

$$\exists \lim_{t\to 0^+} \beta(t) \in f(A).$$

By Lemma 3.5, there is $0 < c \leqslant 1$ and a semialgebraic continuous function $\alpha\colon]0,c[\to A$ such that $\beta(t) = f(\alpha(t))$ for every $0 < t < c$. Since A is semialgebraic compact

$$\exists \lim_{t\to 0^+} \alpha(t) = x \in A.$$

So $\lim_{t\to 0^+} \beta(t) = f(x) \in f(A)$, as required. □

Corollary 3.6. *If A is a semialgebraic compact set then any semialgebraic continuous function $f\colon A \to R$ takes maximum and minimum.*

Proof. By Thereom above $f(A)$ is semialgebraic compact, so by 3.2 it is closed and bounded. So $f(A)$ is a union of finitely many intervals $[a_i, b_i]$ (with $a_i \leqslant b_i \in R$). □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (22: 14/01/10)

SALMA KUHLMANN

Contents

Let R be a real closed field.

1. Semialgebraic dimension

Theorem 1.1. *Let $S \subset R^n$ be a semialgebraic set and $T_1, \dots, T_q$ finitely many semialgebraic subsets of S. Then*

$$S = \dot{\bigcup_{k=1,\dots,r}} \Sigma_k, \qquad \textit{where}$$

(*i*) *every Σ_k is semialgebraic homeomorphic to an open hypercube $(0,1)^{d_k}$;*

(*ii*) *the closure of Σ_k in S is the union of Σ_k and some Σ_j with $j \neq k$ and $d_j < d_k$;*

(*iii*) *the closure $\bar{\Sigma}_k$ of Σ_k is the union of Σ_k and finitely many semialgebraic sets S_i semialgebraic homeomorphic to an open hypercube $(0,1)^{d_i}$, with $d_i < d_k$;*

(*iv*) *every T_i is the union of some Σ_k.*

Such a decomposition $S = \bigcup_k \Sigma_k$ is said to be a ***stratification*** *of S and the $\Sigma_1, \dots, \Sigma_r$ are called* ***strata****.*

Proposition 1.2. *Let $S \subset R^n$ be a semialgebraic set. Let*

$$S = \bigcup_{i=1}^{p} C_i \qquad S = \bigcup_{j=1}^{q} D_j$$

be two decompositions of S into a disjoint union of semialgebraic sets, with

$$C_i \quad \textit{semialgebraic isomorphic to } (0,1)^{d_i} \quad \forall\, i = 1, \dots, p,$$

$$D_j \quad \textit{semialgebraic isomorphic to } (0,1)^{d_j} \quad \forall\, j = 1, \dots, q.$$

Then $\max_{i=1,\dots,p}\{d_i\} = \max_{j=1,\dots,q}\{d_j\} = d$.

We define the ***dimension*** *of S such a d. We write* $\dim S = d$.

Proof. We can apply Theorem 1.1 taking the semialgebraic subsets $T_{ij} = C_i \cap D_j$, for $i = 1, \dots, p$ and $j = 1, \dots, q$, and we find a stratification

$$S = \bigcup_{k=1}^{r} \Sigma_k$$

which is a common refinement of the two decomposition, i.e. each C_i and each D_j is a finite union of some Σ_k and each Σ_k is semialgebraic homeomorphic to $(0,1)^{d_k}$.

We want to show that $\max_{i=1,\dots,p}\{d_i\} = \max_{j=1,\dots,q}\{d_j\} = \max_{k=1,\dots,r}\{d_k\}$.

Set $\bar{d}_i := \max_{i=1,\dots,p}\{d_i\}$ and $\bar{d}_k := \max_{k=1,\dots,r}\{d_k\}$.
Since every Σ_k is contained in some C_i, of course $\bar{d}_k \leqslant \bar{d}_i$.

Let now Σ_k a stratum semialgebraic homeomorphic to $(0,1)^{\bar{d}_k}$ and suppose that $\Sigma_k \subset C_i$. We claim that Σ_k is open in C_i (equivalently, $C_i \setminus \Sigma_k$ is closed in C_i): by Theorem 1.1(ii), if Σ_s is a stratum in $C_i \setminus \Sigma_k$ then the closure of Σ_s in C_i contains only Σ_s and strata Σ_a with $d_a < d_s \leqslant \bar{d}_k$. Therefore the closure of $C_i \setminus \Sigma_k$ in C_i is disjoint from Σ_k and this shows that $C_i \setminus \Sigma_k$ is closed in C_i (and Σ_k is open in C_i). We conclude assuming the following fact:

Fact 1.3.

- $A \subset X$, X homeomorphic to $(0,1)^d$, A open in $X \;\Rightarrow$ A locally homeomorphic to $(0,1)^d$ (i.e. for every $x \in A$ there is an open neighborhood of x homeomorphic to $(0,1)^d$).

- $(0,1)^{d_1}$ is homeomorphic to $(0,1)^{d_2} \;\Leftrightarrow\; d_1 = d_2$.

Therefore $\bar{d}_k = \bar{d}_i$, and $\bar{d}_k = \bar{d}_j$ is similar. □

Remark 1.4. Let A, $B \subset R^n$ be semialgebraic sets. Then

(1) $\dim(A \cup B) = \max\{\dim A, \dim B\}$.

(2) $\dim(A \times B) = \dim A + \dim B$.

We see now that the dimension of a semialgebraic set behaves well with respect to the topological closure:

Proposition 1.5. *Let $S \subset R^n$ be semialgebraic. Then*

(i) $\dim \bar{S} = \dim S$.

(ii) $\dim(\bar{S} \setminus S) < \dim S$.

Proof. Let us observe that by 1.4(1), (ii) $\Rightarrow$ (i).
We claim that if

$$S = \dot{\bigcup_{k=1,\dots,r}} \Sigma_k$$

is a stratification of S as in Theorem 1.1, then

$$\bar{S} = \bigcup_{k=1}^{r} \bar{\Sigma}_k :$$

($\subseteq$) $\bigcup_{k=1}^{r} \bar{\Sigma}_k$ is a finite union of closed set, so it is closed. It contains S, so it contains also the closure $\bar{S}$ of S.

($\supseteq$) For every $k = 1, \ldots, r$, $\Sigma_k \subseteq S$. Then $\bar{\Sigma}_k \subseteq \bar{S}$ and $\bigcup_{k=1}^{r} \bar{\Sigma}_k \subseteq \bar{S}$.

Therefore $\dim(\bar{S} \setminus S) \leqslant \max\{\dim(\bar{\Sigma}_k \setminus \Sigma_k) : 1 \leqslant k \leqslant r\}$ and by Theorem 1.1(*iii*) this is stricly less than $\max\{\dim \Sigma_k : 1 \leqslant k \leqslant r\} = \dim S$. □

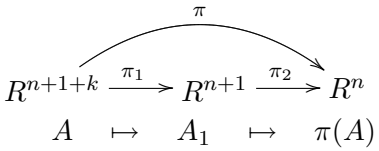
Now we see that the dimension of a semialgebraic set is invariant by semialgebraic bijections (not necessarily continuous!):

Lemma 1.6. *Let $A \subset R^{n+k}$ be a semialgebraic set, $\pi\colon R^{n+k} \to R^n$ the projection on the first n coordinates. Then $\dim \pi(A) \leqslant \dim A$. Moreover if $\pi_{|A}\colon A \to R^n$ is injective, then $\dim \pi(A) = \dim A$.*

Proof. By induction on k.

- $k = 1$. Write A as a disjoint union of cells.

- $k \Rightarrow k+1$. Consider the projection $\pi\colon R^{n+k+1} \to R^n$ on the first n coordinates as the composition of the projection $\pi_1\colon R^{n+k+1} \to R^{n+1}$ on the first $n+1$ coordinates and the projection $\pi_2\colon R^{n+1} \to R^n$ on the first n coordinates:



Then by induction $\dim A \geqslant \dim \pi_1(A) = A_1 \geqslant \dim \pi_2(A_1) = \pi(A)$.

Moreover

$$\pi_{|A} \text{ is injective} \iff \pi_{1|A} \text{ and } \pi_{2|A_1} \text{ are injective.}$$

□

Theorem 1.7. *Let $S \subset R^n$ be semialgebraic, $f\colon S \to R^k$ a semialgebraic map (not necessarily continuous). Then $\dim f(S) \leqslant \dim S$. If f is injective then $\dim f(S) = \dim S$.*

Proof. Let $A \subset R^{n+k}$ be the graph of f:

$$A = \Gamma(f) = \{(\underline{x}, f(\underline{x})) : \underline{x} \in S\}.$$

Let $\pi_1\colon R^{n+k} \to R^n$ be the projection on the first n coordinates. Then $\pi_{1|A}$ is injective and $\pi_1(A) = S$. Therefore, by Lemma 1.6, $\dim S = \dim A$.

Let now $\pi_2\colon R^{n+k} \to R^k$ be the projection on the last k coordinates. Then $\pi_2(A) = f(S)$. Again by Lemma 1.6 $\dim f(S) \leqslant \dim A = \dim S$.

If f is injective then $\dim f(S) = \dim A$. □

2. Algebraic dimension

Consider the ring of polynomials $R[\underline{x}] := R[x_1, \ldots, x_n]$ in n variables and coefficients in R.

An algebraic set $V \subset R^n$ is by definition the common zeroset of all polynomials belonging to a subset $A \subset R[\underline{x}]$:

$$V = \mathcal{Z}(A) := \{\underline{x} \in R^n : p(\underline{x}) = 0 \ \forall\, p \in A\}.$$

Then we can consider the set of polynomials which vanish on V (which of course contains A):

$$\mathcal{I}(V) := \{p \in R[\underline{x}] : p(\underline{x}) = 0 \ \forall\, \underline{x} \in V\}.$$

We take the ring of polynomal functions on V, i.e. the quotient of $R[\underline{x}]$ by $\mathcal{I}(V)$:

$$\mathcal{P}(V) := \frac{R[\underline{x}]}{\mathcal{I}(V)}.$$

And now we are ready to define the algebraic dimension of V:

Definition 2.1. The **dimension** of an algebraic set V is by definition the Krull dimension of $\mathcal{P}(V)$, i.e. the maximal $d \in \mathbb{N}$ such that

$$\exists\ P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d,$$

where P_i is a prime ideal of $\mathcal{P}(V)\ \forall\ i = 1, \ldots, d$.

We recall that an ideal P is said to be **prime** if for every pair of ideals A and B,

$$AB \subset P \ \Rightarrow\ A \subset P \text{ or } B \subset P.$$

In general, given a subset $S \subset R^n$, $\mathcal{Z}(\mathcal{I}(S))$ is the smallest algebraic subset of R^n containing S. It is said to be the **Zariski closure** of S and it is denoted by $\bar{S}^Z$.

In fact, the algebraic subsets of R^n are the closed sets of the **Zariski topology**, and $\bar{S}^Z$ is the closure of S with respect to this topology.

The Zariski topology is coarser than the Euclidean topology, i.e. each algebraic set is closed in the Euclidean topology, but the converse is not true.

Theorem 2.2. *Let $S \subset R^n$ be a semialgebraic set. Then its dimension as a semialgebraic set is equal to the dimension, as an algebraic set, of its Zariski closure $\bar{S}^Z$. In particular, if $V \subset R^n$ is an algebraic set, then its dimension as a semialgebraic set is equal to its dimension as an algebraic set (i.e. the Krull dimension of $\mathcal{P}(V)$).*

Dimension will be investigated more during next term.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (23: 19/01/10)

SALMA KUHLMANN

Contents

PART III
Konvexe Bewertungen und reelle Stellen auf angeordnete Körper

1. Valued Z-modules and valued Q-vector spaces

All modules M considered are left Z-modules for a fixed ring Z with 1 (we are mainly interested in $Z = \mathbb{Z}$, i.e. in valued abelian groups).

Definition 1.1. Let Γ be a totally ordered set and ∞ an element greater than aech element of Γ (Notation: $\infty > \Gamma$). A surjective map

$$v\colon M \longrightarrow \Gamma \cup \{\infty\}$$

is a **valuation** on M (and (M, v) is a **valued module**) if $\forall\, x, y \in M$ and $\forall\, r \in Z$:

(i) $v(x) = \infty \Leftrightarrow x = 0$;

(ii) $v(rx) = v(x)$, if $r \neq 0$ (value preserving scalar multiplication);

(iii) $v(x - y) \geqslant \min\{v(x), v(y)\}$ (ultrametric Δ-inequality).

Remark 1.2. $(i) + (ii) \Rightarrow M$ is torsion-free.

Remark 1.3. Consequences of the ultrametric:

- $v(x) \neq v(y) \Rightarrow v(x + y) = \min\{v(x), v(y)\}$;
- $v(x + y) > v(x) \Rightarrow v(x) = v(y)$.

Definition 1.4. $v(M) := \Gamma = \{v(x) : 0 \neq x \in M\}$ is the **value set** of M.

Definition 1.5.

(*i*) Let (M_1, v_1), (M_2, v_2) two valued modules with value sets Γ_1 and Γ_2 respectively. Let

$$h\colon M_1 \longrightarrow M_2$$

be an isomorphism of Z-modules. We say that h **preserves the valuation** if there is an isomorphism of ordered sets

$$\varphi\colon \Gamma_1 \longrightarrow \Gamma_2$$

such that $\forall\, x \in M_1 :\ \varphi(v_1(x)) = v_2(h(x))$.

(*ii*) Two valuations v_1, v_2 on M are **equivalent** if the identity map on M preserves the valuation.

Definition 1.6.

(1) An **ordered system of Z-modules** is denoted by:

$$[\,\Gamma,\ \{B(\gamma) : \gamma \in \Gamma\}\,]$$

where $\{B(\gamma) : \gamma \in \Gamma\}$ is a family of modules indexed by a totally ordered set Γ.

(2) Two systems

$$S_i = [\,\Gamma_i,\ \{B_i(\gamma) : \gamma \in \Gamma_i\}\,] \qquad i = 1, 2$$

are **isomorphic** (we write $S_1 \cong S_2$) if and only if there are an isomorphism

$$\varphi\colon \Gamma_1 \longrightarrow \Gamma_2$$

of totally ordered sets, and $\forall\, \gamma \in \Gamma_1$ an isomorphism of modules

$$\varphi_\gamma\colon B_1(\gamma) \longrightarrow B_2(\varphi(\gamma)).$$

(3) Let (M, v) be a valued module, $\Gamma := v(M)$. For $\gamma \in \Gamma$ set

$$M^\gamma := \{x \in M : v(x) \geqslant \gamma\}$$
$$M_\gamma := \{x \in M : v(x) > \gamma\}.$$

Then $M_\gamma \subsetneq M^\gamma \subsetneq M$. Set

$$B(M, \gamma) := M^\gamma / M_\gamma.$$

$B(M, \gamma)$ is **the (homogeneous) component corresponding to** γ. **The skeleton** (*das skelett*) of the valued module (M, v) is the ordered system

$$S(M) := [\,v(M),\ \{B(M, \gamma) : \gamma \in v(M)\}\,].$$

We write $B(\gamma)$ for $B(M, \gamma)$ if the context is clear.

(4) For every $\gamma \in \Gamma$, the **coefficient map** (*Koeffizient Abbildung*)

$$\begin{aligned} \pi^M(\gamma, -)\colon M^\gamma &\longrightarrow B(\gamma) \\ x &\mapsto x + M_\gamma \end{aligned}$$

is the canonical projection.

We write $\pi(\gamma, -)$ instead of $\pi^M(\gamma, -)$ if the context is clear.

Lemma 1.7. *The skeleton is an isomorphism invariant, i.e.*

$$\begin{aligned} \textit{if} \quad & (M_1, v_1) \cong (M_2, v_2), \\ \textit{then} \quad & S(M_1) \cong S(M_2). \end{aligned}$$

Proof. Let $h\colon M_1 \to M_2$ be an isomorphism which preserves the valuation. Then

$$\tilde{h}\colon v(M_1) \longrightarrow v(M_2)$$

defined by

$$\tilde{h}(v_1(x)) := v_2(h(x))$$

is a well defined map and an isomorphism of totally ordered sets.

For $\gamma \in v(M_1)$ the map

$$h_\gamma\colon B_1(\gamma) \longrightarrow B_2(\tilde{h}(\gamma))$$

defined by

$$\pi^{M_1}(\gamma, x) \mapsto \pi^{M_2}(\tilde{h}(\gamma), h(x))$$

is well defined and an isomorphism of modules. □

2. Hahn valued modules

A system $[\,\Gamma,\ \{B(\gamma) : \gamma \in \Gamma\}\,]$ of torsion-free modules can be realized as the skeleton of a valued module through the following canonical construction:

Consider $\prod_{\gamma\in\Gamma} B(\gamma)$ the product module. For $s \in \prod_{\gamma\in\Gamma} B(\gamma)$ define

$$\operatorname{support}(s) = \{\gamma \in \Gamma : s(\gamma) \neq 0\}.$$

The **Hahn sum** $\bigsqcup_{\gamma\in\Gamma} B(\gamma)$ is the submodule of $\prod_{\gamma\in\Gamma} B(\gamma)$ consisting of elements with finite support (i.e. $\bigoplus_{\gamma\in\Gamma} B$) endowed with the valuation:

$$\begin{aligned} v_{\min}\colon \bigsqcup_{\gamma\in\Gamma} B(\gamma) &\longrightarrow \Gamma \cup \{\infty\} \\ v_{\min}(s) &= \min \operatorname{support}(s). \end{aligned}$$

(convention: $\min \emptyset = \infty$).

The **Hann product** $\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma)$ is the submodule of $\prod_{\gamma\in\Gamma} B(\gamma)$ consisting of the elements with well-ordered support equipped with $v_{\min}$.

We recall that a totally ordered set Γ is **well-ordered** if every non-empty subset of Γ has a least, or equivalently if every descending sequence of elements from Γ is finite.

3. Hahn Sandwich Proposition

Lemma 3.1.

(i) $\bigsqcup_{\gamma\in\Gamma} B(\gamma)) \subseteq \mathrm{H}_{\gamma\in\Gamma}\, B(\gamma)$.

(ii)

$$\begin{aligned} S(\bigsqcup_{\gamma\in\Gamma} B(\gamma)) &\cong [\,\Gamma, \{B(\gamma) : \gamma\in\Gamma\}\,] \\ &\cong S(\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma)). \end{aligned}$$

We shall show that if $Z = Q$ is a field and (V, v) is a valued Q-vector space with skeleton $S(V) = [\,\Gamma, B(\gamma)\,]$, then

$$(\bigsqcup B(\gamma), v_{\min}) \hookrightarrow (V, v) \hookrightarrow (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma), v_{\min}).$$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (24: 21/01/10)

SALMA KUHLMANN

Contents

1. Hahn Sandwich Proposition

From now, let $Z = Q$ be a field and (V, v) a valued Q-vector space with skeleton $S(V) = [\,\Gamma, B(\gamma)\,]$. We want to show

$$(\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}) \ \hookrightarrow\ (V, v) \ \hookrightarrow\ (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma),\ v_{\min}).$$

2. Immediate extensions

Definition 2.1. Let (V_i, v_i) be valued Q-vector spaces $(i = 1, 2)$.

(1) Let $V_1 \subseteq V_2$ Q-subspace with $v_1(V_1) \subseteq v_2(V_2)$. We say that (V_2, v_2) is an **extension** of (V_1, v_1), and we write

$$(V_1, v_1) \ \subseteq\ (V_2, v_2),$$

if $v_{2|_{V_1}} = v_1$.

(2) If $(V_1, v_1) \subseteq (V_2, v_2)$, for $\gamma \in v_1(V_1)$ the map

$$\begin{aligned} B_1(\gamma) &\longrightarrow B_2(\gamma) \\ x + (V_1)_\gamma &\mapsto x + (V_2)_\gamma \end{aligned}$$

is a natural identification of $B_1(\gamma)$ as a Q-subspace of $B_2(\gamma)$. The extension $(V_1, v_1) \subseteq (V_2, v_2)$ is **immediate** if $\Gamma := v_1(V_1) = v_2(V_2)$ and $\forall\, \gamma \in v_1(V_1)$

$$B_1(\gamma) = B_2(\gamma).$$

Equivalently, $(V_1, v_1) \subseteq (V_2, v_2)$ is immediate if $S(V_1, v_1) = S(V_2, v_2)$.

Lemma 2.2. *(Characterization of immediate extensions)*
The extension $(V_1, v_1) \subseteq (V_2, v_2)$ is immediate if and only if

$$\forall\, x \in V_2,\ x \neq 0,\ \exists\, y \in V_1 \ \text{ such that } \ v_2(x-y) > v_2(x).$$

Proof. We show that in a valued Q-vector space (V, v), for every $x, y \in V$

$$v(x-y) > v(x) \iff \begin{cases} (i) & \gamma = v(x) = v(y) \ \text{ and} \\ (ii) & \pi(\gamma, x) = \pi(\gamma, y). \end{cases}$$

($\Leftarrow$) Assume (i) and (ii). So $x, y \in V^\gamma$ and $x - y \in V_\gamma$.
Then $v(x-y) > v(x) = \gamma$.

($\Rightarrow$) Assume $v(x-y) > v(x)$. We show (i) and (ii).
If $v(x) \neq v(y)$, then $v(x-y) = \min\{v(x), v(y)\}$. In both cases $\min\{v(x), v(y)\} = v(x)$ and $\min\{v(x), v(y)\} = v(y)$ we have a contradiction. (ii) is analogue.

□

Example 2.3. $(\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}) \ \subseteq\ (\mathrm{H}_{\gamma\in\Gamma} B(\gamma),\ v_{\min})$
is an immediate extension.

Proof. Given $x \in \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$, $x \neq 0$, set

$$\gamma_0 := \min \mathrm{support}(x) \qquad \text{and} \qquad x(\gamma_0) := b_0 \in B(\gamma_0).$$

Let $y \in \bigsqcup_{\gamma\in\Gamma} B(\gamma)$ such that

$$y(\gamma) = \begin{cases} 0 & \text{if } \gamma \neq \gamma_0 \\ b_0 & \text{if } \gamma = \gamma_0. \end{cases}$$

Namely $y = b_0 \chi_{\gamma_0}$, where

$$\chi_{\gamma_0} \colon \Gamma \ \longrightarrow\ Q$$

$$\chi_{\gamma_0}(\gamma) = \begin{cases} 1 & \text{if } \gamma = \gamma_0 \\ 0 & \text{if } \gamma \neq \gamma_0. \end{cases}$$

Then $v_{\min}(x-y) > \gamma_0 = v_{\min}(x)$ (because $(x-y)(\gamma_0) = x(\gamma_0) - y(\gamma_0) = b_0 - b_0 = 0$).

□

3. Valuation independence

Definition 3.1. $\mathcal{B} = \{x_i : i \in I\} \subseteq V \setminus \{0\}$ is **Q-valuation independent** if for $q_i \in Q$ with $q_i = 0$ for all but finitely many $i \in I$, we have

$$v(\sum_{i\in I} q_i x_i) = \min_{i\in I, q_i\neq 0} \{v(x_i)\}.$$

Remark 3.2. $\mathcal{B} \subseteq V\setminus\{0\}$ Q-valuation independent $\Rightarrow$ Q-linear independent.
(Otherwise $\exists\ q_i \neq 0$ with $\sum q_i x_i = 0$ and $v(\sum q_i x_i) = \infty$).

Proposition 3.3. *(Characterization of valuation independence)*
Let $\mathcal{B} \subseteq V \setminus \{0\}$. Then $\mathcal{B}$ is Q-valuation independent if and only if $\forall\, n \in \mathbb{N}$, $\forall\, b_1, \ldots, b_n \in \mathcal{B}$ pairwise distinct with $v(b_1) = \cdots = v(b_n) = \gamma$, the coefficients

$$\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n) \in B(\gamma)$$

are Q-linear independent in $B(\gamma)$.

Proof.

($\Rightarrow$) Let $b_1, \ldots, b_n \in \mathcal{B}$ with $v(b_1) = \cdots = v(b_n) = \gamma$ and suppose for a contradiction that

$$\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n) \in B(\gamma)$$

are not Q-linear independent. So there are $q_1, \ldots, q_n \in Q$ non-zero such that $\pi(\gamma, \sum q_i b_i) = 0$ and $v(\sum q_i b_i) > \gamma$, contradiction.

($\Leftarrow$) We show that

$$v(\sum q_i b_i) = \min\{v(b_i)\} = \gamma.$$

Since $\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n)$ are Q-linear independent in $B(\gamma)$, also

$$\pi(\gamma, \sum_{i=0}^{n} q_i b_i) \neq 0,$$

i.e. $v(\sum q_i b_i) \leqslant \gamma$.
On the other hand $v(\sum q_i b_i) \geqslant \gamma$, so $v(\sum q_i b_i) = \gamma = \min\{v(b_i)\}$.
□

4. Maximal valuation independence

By Zorn's lemma, maximal valuation independent sets exist:

Corollary 4.1. *(Characterization of maximal valuation independent sets)*
$\mathcal{B} \subseteq V \setminus \{0\}$ is maximal valuation independent if and only if $\forall\, \gamma \in v(V)$

$$\mathcal{B}_\gamma := \{\pi(\gamma, b) : b \in \mathcal{B}; v(b) = \gamma\}$$

is a Q-vector space basis of $B(V, \gamma)$.

Corollary 4.2. *Let $\mathcal{B} \subseteq V \setminus \{0\}$ be valuation independent in (V, v). Then $\mathcal{B}$ is maximal valuation independent if and only if the extension*

$$\langle\, \mathcal{B} \,\rangle := (V_0, v_{|V_0}) \ \subseteq\ (V, v)$$

is an immediate extension.

Proof.

($\Rightarrow$) Assume $\mathcal{B} \subseteq V$ is maximal valuation independent. We show $V_0 \subseteq V$ is immediate.

If not $\exists\, x \in V$, $x \neq 0$ such that

$$\forall\, y \in V_0 :\ v(x-y) \leqslant v(x).$$

We will show that in this case $\mathcal{B} \cup \{x\}$ is valuation independent (which will contradict our maximality assumption).

Consider $v(y_0 + qx)$, $q \in Q$, $q \neq 0$, $y_0 \in V_0$. Set

$$y := -y_0/q.$$

We claim that $v(y_0 + qx) = v(x-y) = \min\{v(x), v(y)\}$

Fact.

$$v(x-y) \leqslant v(x) \iff v(x-y) = \min\{v(x), v(y)\}.$$

Proof of the fact. ($\Leftarrow$) is clear. To see ($\Rightarrow$), assume that $v(x-y) > \min\{v(x), v(y)\}$. If $\min\{v(x), v(y)\} = v(x)$, then we have a contradiction. If $\min\{v(x), v(y)\} = v(y) < v(x)$, then $v(x-y) = v(y) > v(y)$, again a contradiction.

($\Leftarrow$) Now assume $(V_0, v) \subseteq (V, v)$ is immediate. We show that $\mathcal{B}$ is maximal valuation independent.

If not, there is $\gamma \in v(V)$ such that B_γ is not a basis for $B(V, \gamma)$.

Let $b \in B(V, \gamma)$, $b \notin \langle \mathcal{B}_\gamma \rangle$.

$$b \in V^\gamma / V_\gamma \implies b = x + V_\gamma,$$

with $x \in V$, $v(x) = \gamma$.

Claim: $\forall\, y \in V_0\ v(x-y) \leqslant v(x)$ (contradicting that the extension is immediate). This follows by Characterization of immediate extensions (Lemma 2.2).

□

5. Valuation basis

Definition 5.1. $\mathcal{B}$ is a **Q-valuation basis** of (V, v) if

(1) $\mathcal{B}$ is a Q-basis,
(2) $\mathcal{B}$ is Q-valuation independent.

Remark 5.2. $\mathcal{B}$ Q-valuation basis $\Rightarrow$ $\mathcal{B}$ is maximal valuation independent.

Example 5.3. $(\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min})$ admits a valuation basis.

Proof. Let $\mathcal{B}_\gamma$ be a Q-basis of $B(\gamma)$ for $\gamma \in \Gamma$ and consider

$$\mathcal{B} := \bigcup_{\gamma\in\Gamma} \{b\chi_{\{\gamma\}};\ b \in \mathcal{B}_\gamma\},$$

where $\forall\, \gamma \in \Gamma$

$$\chi_\gamma \colon \Gamma \longrightarrow Q$$

$$\chi_\gamma(\gamma') = \begin{cases} 1 & \text{if } \gamma = \gamma' \\ 0 & \text{if } \gamma \neq \gamma'. \end{cases}$$

□

Corollary 5.4. *(V, v) with skeleton $S(V) = [\,\Gamma, B(\gamma)\,]$ admits a valuation basis if and only if*

$$(V, v) \;\cong\; (\bigsqcup_{\gamma\in\Gamma} B(\gamma),\; v_{\min}).$$

Proof.

($\Leftarrow$) Clear.

($\Rightarrow$) Let $\mathcal{B}$ be a valuation basis for (V, v). Then $\mathcal{B} = \{b_i : i \in I\}$ is maximal valuation independent. For every $b_i \in \mathcal{B}, v(b_i) = \gamma$, define

$$h(b_i) = \pi(\gamma, b_i)\chi_\gamma$$

and extend it to V by linearity (note that $v(b_i) = v_{\min}(h(b_i))$).

□

Corollary 5.5. *Assume $S(V) = [\,\Gamma, B(\gamma)\,]$. Then*

$$(\bigsqcup_{\gamma\in\Gamma} B(\gamma),\; v_{\min}) \;\hookrightarrow\; (V, v).$$

Proof. By Zorn's lemma, let $\mathcal{B} \subset V \setminus \{0\}$ be maximal valuation independent. Set

$$V_0 := {}_Q\langle\, \mathcal{B}\,\rangle.$$

Then $\mathcal{B}$ is a valuation basis for V_0 and $V_0 \subseteq V$ (immediate), so $S(V_0) = S(V) = [\,\Gamma, B(\gamma)\,]$ and

$$(V_0, v) \;\cong\; (\bigsqcup_{\gamma\in\Gamma} B(\gamma),\; v_{\min}).$$

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (25: 26/01/10)

SALMA KUHLMANN

Contents

1. Introduction

Our aim for this and next lecture is to complete the proof of Hahn's embedding Theorem:

Let (V, v) be a Q-valued vector space with $S(V) = [\,\Gamma, B(\gamma)\,]$.
Let $\{x_i : i \in I\} \subset V$ be maximal valuation independent and

$$h\colon V_0 = (\langle\{x_i : i \in I\}\rangle,\ v) \ \xrightarrow{\sim}\ (\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}).$$

Then h extends to a valuation preserving embedding (i.e. an isomorphism onto a valued subspace)

$$\tilde{h}\colon (V, v) \ \hookrightarrow\ (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma),\ v_{\min}).$$

The picture is the following:

$$\begin{array}{ccc} (V,\, v) & \xhookrightarrow{\ \tilde{h}\ } & (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma),\ v_{\min}) \\ \text{immediate}\ \big| & & \big|\ \text{immediate} \\ (V_0,\, v) & \xrightarrow[\sim]{\ h\ } & (\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}) \end{array}$$

2. Pseudo-convergence and maximality

Definition 2.1. A valued Q-vector space (V, v) is said to be **maximally valued** if it admits no proper immediate extension.

Definition 2.2. A well ordered set $S = \{a_\rho : \rho \in \lambda\} \subset V$ without a last element is said to be **pseudo-convergent** (or **pseudo-Cauchy**) if for every $\rho < \sigma < \tau$ we have

$$v(a_\sigma - a_\rho) \ < \ v(a_\tau - a_\sigma).$$

Example 2.3.

(*a*) Let $V = (\mathrm{H}_{\mathbb{N}_0}\mathbb{R}, v_{\min})$, where $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. An element $s \in V$ can be viewed as a function $s\colon \mathbb{N}_0 \to \mathbb{R}$. Consider

$$\begin{aligned} a_0 &= (1, 0, 0, 0, 0 \dots) \\ a_1 &= (1, 1, 0, 0, 0 \dots) \\ a_2 &= (1, 1, 1, 0, 0 \dots) \\ &\vdots \end{aligned}$$

The sequence $\{a_n : n \in \mathbb{N}_0\} \subset V$ is pseudo-Cauchy.

(*b*) Take V as above and $s \in V$ with

$$\mathrm{support}(s) = \mathbb{N}_0,$$

i.e. $s_i := s(i) \neq 0 \ \forall\, i \in \mathbb{N}_0$. Define the sequence

$$\begin{aligned} b_0 &= (s_0, 0, 0, 0, 0 \dots) \\ b_1 &= (s_0, s_1, 0, 0, 0 \dots) \\ b_2 &= (s_0, s_1, s_2, 0, 0 \dots) \\ &\vdots \end{aligned}$$

For every $l < m < n \in \mathbb{N}_0$, we have

$$l + 1 = v_{\min}(b_m - b_l) < v_{\min}(b_n - b_m) = m + 1.$$

Therefore $\{b_n : n \in \mathbb{N}_0\} \subset V$ is pseudo-Cauchy.

Lemma 2.4. *If $S = \{a_\rho\}_{\rho\in\lambda}$ is pseudo-convergent then*

(*i*) *either $v(a_\rho) < v(a_\sigma)$ for all $\rho < \sigma \in \lambda$,*

(*ii*) *or $\exists\, \rho_0 \in \lambda$ such that $v(a_\rho) = v(a_\sigma) \ \forall\, \rho, \sigma \geqslant \rho_0$.*

Proof. Assume (*i*) does not hold, i.e. $v(a_\rho) \geqslant v(a_\sigma)$ for some $\rho < \sigma$. Then we claim that

$$v(a_\tau) = v(a_\sigma) \qquad \forall\, \tau > \sigma.$$

Otherwise, $v(a_\tau - a_\sigma) = \min\{v(a_\tau), v(a_\sigma)\} \leqslant v(a_\sigma)$.
But $v(a_\sigma - a_\rho) \geqslant v(a_\sigma)$, contradicting 2.2. □

Notation 2.5. In case (*ii*) define

$$\mathrm{Ult}\, S := v(a_{\rho_0}) = v(a_\rho) \qquad \forall \rho \geqslant \rho_0.$$

Lemma 2.6. *If $\{a_\rho\}$ is pseudo-convergent then for all $\rho < \sigma$ we have*

$$v(a_\sigma - a_\rho) = v(a_{\rho+1} - a_\rho).$$

Proof. We may assume $\sigma > \rho + 1$ (so $\rho < \rho + 1 < \sigma$). From

$$v(a_{\rho+1} - a_\rho) < v(a_\sigma - a_{\rho+1})$$

and the identity

$$a_\sigma - a_\rho = (a_\sigma - a_{\rho+1}) + (a_{\rho+1} - a_\rho),$$

we deduce that

$$\begin{aligned} v(a_\sigma - a_\rho) &= \min(v(a_\sigma - a_{\rho+1}), v(a_{\rho+1} - a_\rho)) \\ &= v(a_{\rho+1} - a_\rho). \end{aligned}$$

□

Notation 2.7.

$$\begin{aligned} \gamma_\rho :&= v(a_{\rho+1} - a_\rho) \\ &= v(a_\sigma - a_\rho) \qquad \forall\, \sigma > \rho. \end{aligned}$$

Remark 2.8. Since $\rho < \rho + 1 < \rho + 2$, we have $\gamma_\rho < \gamma_{\rho+1}$ for all ρ.

3. Pseudo-limits

Definition 3.1. Let $S = \{a_\rho\}$ be a pseudo-convergent set. We say that $x \in V$ is a **pseudo-limit** of S if

$$v(x - a_\rho) = \gamma_\rho \qquad \text{for all } \rho.$$

Remark 3.2.

(*i*) If $v(a_\rho) < v(a_\sigma)$ for $\rho < \sigma$, then $x = 0$ is a pseudo-limit.

(*ii*) If 0 is not a pseudo-limit and x is a pseudo-limit, then $v(x) = \operatorname{Ult} S$.

Example 3.3.

(*a*) In Example 2.3(*a*), the costant function 1:

$$a = (1, 1, \dots)$$

is a pseudo-limit of the sequence $\{a_n\}_{n\in\mathbb{N}_0}$.

(*b*) In Example 2.3(*b*), s is a pseudo-limit of $\{b_n\}_{n\in\mathbb{N}_0}$.

Definition 3.4. (V, v) is **pseudo-complete** if every pseudo-convergent sequence has a pseudo-limit in V.

Definition 3.5. Let $S = \{a_\rho\}$ be pseudo-convergent. The **breadth** (*Breite*) B of S is defined to be the following subset of V:

$$B(S) = \{y \in V : v(y) > \gamma_\rho \ \forall\, \rho\}.$$

Lemma 3.6. *Let $\{a_\rho\}$ be pseudo-convergent with breadth B and let $x \in V$ be a pseudo-limit. Then an element of V is a pseudo-limit of $\{a_\rho\}$ if and only if it is of the form $x + y$ with $y \in B$.*

Proof.

($\Rightarrow$) Let z be another pseudo-limit of $\{a_\rho\}$. It follows from

$$x - z = (x - a_\rho) - (z - a_\rho)$$

that

$$v(x - z) \geqslant \min\{v(x - a_\rho), v(z - a_\rho)\} = \gamma_\rho \qquad \forall\, \rho.$$

Since γ_ρ is increasing, it follows that $v(x - z) > \gamma_\rho$ for all ρ. So $z \in B$ as required.

($\Leftarrow$) If $y \in B$ then $v(y) > \gamma_\rho = v(x - a_\rho)$ for all ρ. Then

$$v(x + y - a_\rho) = v(x - a_\rho + y) = \min\{v(x - a_\rho), v(y)\} = \gamma_\rho \qquad \forall\, \rho.$$

□

4. Cofinal subsets

Definition 4.1. Let Γ be a totally ordered set. A subset $A \subset \Gamma$ is cofinal in Γ if

$$\forall\, \gamma \in \Gamma\ \exists\, a \in A \text{ with } \gamma \leqslant a.$$

Example 4.2. If $\Gamma = [0, 1] \subset R$, then for instance $A = \{1\}$ is cofinal in Γ.

Lemma 4.3. *Let Γ be a totally ordered set. Then there is a well ordered cofinal subset $A \subset \Gamma$. Moreover if Γ has no last element, then also A has no last element.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (26: 28/01/10)

SALMA KUHLMANN

Contents

1. Pseudo-completeness

Let (V, v) be a valued Q-vector space. We recall that

- (V, v) is said to be **maximally valued** if it admits no proper immediate extension.
- (V, v) is **pseudo-complete** if every pseudo-convergent sequence in V has a pseudo-limit in V.

Theorem 1.1. *(V, v) is maximally valued if and only if (V, v) is pseudo-complete.*

We prove only one implication:

(V, v) pseudo-complete $\Rightarrow$ (V, v) maximally valued.

This implication follows from the following:

Proposition 1.2. *Let (V, v) be an immediate extension of (V_0, v). Then any element in V which is not in V_0 is a pseudo-limit of a pseudo-Cauchy sequence of elements of V_0, without a pseudo-limit in V_0.*

Proof. Let $z \in V \setminus V_0$. Consider the set

$$X = \{v(z - a) : a \in V_0\}.$$

Since $z \notin V_0$, $\infty \notin X$.

We show that X cannot have a maximal element. Otherwise, assume $a_0 \in V_0$ and $v(z - a_0)$ maximal in X. Since the extension is immediate, by Lemma 2.2 of Lecture 24 there is $a_1 \in V_0$ such that $v(z-a_0-a_1) > v(z-a_0)$. So $a_0 + a_1 \in V_0$ and $v(z - (a_0 + a_1)) > v(z - a_0)$, contradiction. Then X has no greatest element.

Select from X a well ordered cofinal subset $\{\alpha_\rho\}_{\rho\in\lambda}$. Since the set X has no greatest member, also $\{\alpha_\rho\}_{\rho\in\lambda}$ does not have a last term (see Lemma 4.3 of Lecture 25).

For every $\rho \in \lambda$ choose an element $a_\rho \in V_0$ with

$$v(z - a_\rho) = \alpha_\rho.$$

The identity

$$a_\sigma - a_\rho = (z - a_\rho) - (z - a_\sigma)$$

together with the inequality

$$v(z - a_\rho) < v(z - a_\sigma) \qquad (\forall\, \rho < \sigma \in \lambda)$$

imply

$$(*) \qquad v(a_\sigma - a_\rho) = v(z - a_\rho).$$

Then $\{a_\rho\}_{\rho\in\lambda}$ is pseudo-convergent with z as a pseudo-limit.
Suppose now that $\{a_\rho\}_{\rho\in\lambda}$ had a further limit $z_1 \in V_0$.
Then by Lemma 3.6 of Lecture 25 we have

$$v(z - z_1) > v(a_\sigma - a_\rho).$$

Combining this with $(*)$ we get

$$v(z - z_1) > v(z - a_\rho) = \alpha_\rho \qquad \forall\, \rho \in \lambda$$

and this is a contradiction, since $\{\alpha_\rho\}_{\rho\in\lambda}$ is cofinal in X. □

Theorem 1.3. *Suppose that*

(*i*) *V_i and V_i' are Q-valued vector spaces and V_i' is an immediate extension of V_i, for $i = 1, 2$.*

(*ii*) *h is an isomorphism of valued vector spaces of V_1 onto V_2.*

(*iii*) *V_2' is pseudo-complete.*

Then there exists an embedding h' of valued vector spaces of V_1' in V_2' such that h' extends h.

Moreover h' is an isomorphism of valued vector spaces of V_1' onto V_2' if and only if V_1' is pseudo-complete.

Proof. The picture is the following:

$$\begin{array}{ccc} V_1' & \xhookrightarrow{h'} & V_2' \\ \text{immediate}\,\big| & & \big|\,\text{immediate} \\ V_1 & \xrightarrow[\sim]{h} & V_2 \end{array}$$

By Zorn's Lemma, let

$$V_1 \subseteq M_1 \subseteq V_1',$$
$$V_2 \subseteq M_2 \subseteq V_2'$$

and g a valuation isomorphism of M_1 onto M_2 extending h. We shall show how to extend g to V_1'.

Let $y_1 \in V_1' \setminus M_1$. Since V_1' is an immediate extension of M_1 there exists a pseudo-convergent sequence

$$S = \{a_\rho\}_{\rho\in\lambda}$$

of M_1 without a pseudo-limit in M_1 but with a pseudo-limit $y_1 \in V_1'$.
Consider

$$g(S) = \{g(a_\rho)\}_{\rho\in\lambda}$$

Since g is a valuation preserving isomorphism, $g(S)$ is a pseudo-convergent sequence of M_2 without a pseudo-limit in M_2 but with pseudo-limit $y_2 \in V_2'$, because V_2' is pseudo-complete.
Let $M_i' = \langle M_i, y_i\rangle$, for $i = 1, 2$, and denote by g' the unique Q-vector space isomorphism of the linear space M_1' onto the linear space M_2' extending g and such that $g'(y_1) = y_2$.
We show that g' is valuation preserving: let

$$y = x + qy_1 \qquad x \in M_1 \qquad q \in Q \setminus \{0\}$$

be an arbitrary element of $M_1' \setminus V_1$. The set

$$S(y) = \{x + qa_\rho\}_{\rho\in\lambda}$$

is a pseudo-convergent sequence in M_1 with pseudo-limit $y \in M_1'$ and 0 is not a pseudo-limit (otherwise $-x/q \in M_1$ would be a pseudo-limit of S).
It follows that (since $y = x+qy_1$ is a pseudo-limit for the sequence $x+qa_\rho$ which does not have 0 as a pseudo-limit)

$$v(y) = \operatorname{Ult} S(y)$$

similarly

$$v(g'(y)) = \operatorname{Ult} S(g'(y))$$

where

$$S(g'(y)) = \{g'(x) + qg'(a_\rho)\}_{\rho\in\lambda}$$

is a pseudo-convergent sequence of M_2 with limit $g'(y) \in M_2'$.
Now $g'_{|M_1} = g$ is valuation preserving from M_1 to M_2. So we have

$$\operatorname{Ult}(S(y)) = \operatorname{Ult}(S(g'(y)))$$

hence

$$v(y) = v(g'(y))$$

as required. □

Proposition 1.4. $\mathrm{H}_{\gamma\in\Gamma} B(\gamma)$ *is pseudo-complete.*

Proof. Let $\{a_\rho\}_{\rho\in\lambda}$ be pseudo-Cauchy. Recall that

$$\gamma_\rho = v(a_\rho - a_{\rho+1})$$

is strictly increasing. Define $x \in \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$ by

$$x(\gamma) = \begin{cases} a_\rho(\gamma) & \text{if } \gamma < \gamma_\rho \\ 0 & \text{otherwise.} \end{cases}$$

It is well defined because if $\rho_1 < \rho_2$, $\gamma < \gamma_{\rho_1}$ and $\gamma < \gamma_{\rho_2}$, then

$$v(a_{\rho_1} - a_{\rho_2}) = \gamma_{\rho_1}$$

and then

$$a_{\rho_1}(\gamma) = a_{\rho_2}(\gamma).$$

We show now that support(x) is well ordered.

Let $A \subseteq \text{support}(x)$, $A \neq \emptyset$ and $\gamma_0 \in A$. Then $\exists\, \rho$ such that $\gamma_0 < \gamma_\rho$ and $x(\gamma_0) = a_\rho(\gamma_0)$ with $\gamma_0 \in \text{support}(a_\rho)$.

Consider

$$A_0 := \{\gamma \in A : \gamma \leqslant \gamma_0\}.$$

Note that since $x(\gamma) = a_\rho(\gamma)$ for $\gamma \leqslant \gamma_0$ it follows that $A_0 \subseteq \text{support}(a_\rho)$ which is well ordered, so $\min A_0$ exists in A_0 and it is the least element of A.

We now conclude by showing that x is a pseudo-limit. From definition of x we have

$$v(x - a_\rho) \geqslant \gamma_\rho = v(a_{\rho+1} - a_\rho) \quad \forall\, \rho.$$

If $v(x - a_\rho) > v(a_\rho - a_{\rho+1})$, then

$$v(x - a_{\rho+1}) = v(x - a_\rho + a_\rho - a_{\rho+1}) = v(a_\rho - a_{\rho+1}) = \gamma_\rho$$

but

$$v(x - a_{\rho+1}) \geqslant \gamma_{\rho+1} > \gamma_\rho,$$

contradiction. □

As a corollary to the general embedding theorem and this proposition we get Hahn's embedding's theorem.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (27: 02/02/10)

SALMA KUHLMANN

Contents

1. Ordered abelian groups

Definition 1.1. $(G, +, 0, <)$ is an **ordered abelian group** if $(G, +, 0)$ is an abelian group and $<$ is a total order on G such that for every $a, b, c \in G$

$$a \leqslant b \;\Rightarrow\; a + c \leqslant b + c.$$

Definition 1.2. A subgroup C of an ordered abelian group G is **convex** if $\forall\, c_1, c_2 \in C$ and $\forall\, x \in G$

$$c_1 < x < c_2 \;\Rightarrow\; x \in C.$$

Examples 1.3. $C = \{0\}$ and $C = G$ are convex subgroups.

Definition 1.4. Let G be an abelian ordered group, $x \in G$, $x \neq 0$.
We define:

$$C_x := \bigcap \{C : C \text{ is a convex subgroup of } G \text{ and } x \in C\}.$$

$$D_x := \bigcup \{D : D \text{ is a convex subgroup of } G \text{ and } x \notin D\}.$$

A convex subgroup C of G is said to be **principal** if there is some $x \in G$ such that $C = C_x$.

Proposition 1.5.

(1) *D_x is a proper convex subgroup of C_x.*

(2) *D_x is the largest proper convex subgroup of C_x, i.e. if C is a convex subgroup such that*

$$D_x \subseteq C \subseteq C_x$$

then $C = D_x$ or $C = C_x$.

(3) *It follows that the ordered abelian group C_x/D_x has no non-trivial proper convex subgroup.*

2. Archimedean groups

Definition 2.1. Let $(A, +, 0, <)$ be an ordered abelian group. We say that A is **archimedean** if for all non-zero $a_1, a_2 \in A$:

$$\exists\, n \in \mathbb{N}: \quad n|a_1| > |a_2| \ \text{ and } \ n|a_2| > |a_1|,$$

where for every $a \in A$, $|a| := \max\{a, -a\}$.

Proposition 2.2. *(Hölder) Every archimedean group is isomorphic to a subgroup of $(\mathbb{R}, +, 0, <)$.*

Proposition 2.3. *A is archimedean if and only if A has no non-trivial proper convex subgroup.*

Therefore if G is an ordered group and $x \in G$ with $x \neq 0$, the quotient C_x/D_x is archimedean (by 2.3) and can be embedded in $(\mathbb{R}, +, 0, <)$ (by 2.2).

Definition 2.4. Let G be an ordered group, $x \in G$, $x \neq 0$. We say that

$$B_x := C_x/D_x$$

is **the archimedean component** of x in G.

3. Archimedean equivalence

Definition 3.1. An abelian group G is **divisible** if for every $x \in G$ and for every $n \in \mathbb{N}$ there is $y \in G$ such that $x = ny$.

Remark 3.2. Any ordered divisible abelian group G is a $\mathbb{Q}$-vector space and G can be viewed as a valued $\mathbb{Q}$-vector space in a natural way.

Definition 3.3. (archimedean equivalence) For every $x, y \in G$ we define

$$\begin{aligned} x \ \sim^+ \ y \quad &\Leftrightarrow \quad \exists\, n \in \mathbb{N} \quad n|x| \geqslant |y| \ \text{ and } \ n|y| \geqslant |x|. \\ x \ <<^+ \ y \quad &\Leftrightarrow \quad \forall\, n \in \mathbb{N} \quad n|x| < |y|. \end{aligned}$$

Proposition 3.4.

(1) $\sim^+$ *is an equivalence relation.*

(2) $\sim^+$ *is compatible with* $<<^+$*:*

$$\begin{aligned} x <<^+ y \quad \textit{and} \quad x \sim^+ z \quad &\Rightarrow \quad z <<^+ y, \\ x <<^+ y \quad \textit{and} \quad y \sim^+ z \quad &\Rightarrow \quad x <<^+ z. \end{aligned}$$

Because of the last proposition we can define an order $<_\Gamma$ on $\Gamma := G/\sim^+ = \{[x] : x \in G\}$ as follows:

$$[y] <_\Gamma [x] \quad \Leftrightarrow \quad x <<^+ y.$$

Proposition 3.5.

(1) Γ *is a totally ordered set under* $<_\Gamma$*.*

(2) *The map*

$$\begin{aligned} v\colon G &\longrightarrow \Gamma \cup \{\infty\} \\ 0 &\mapsto \infty \\ x &\mapsto [x] \quad (\textit{if } x \neq 0) \end{aligned}$$

is a valuation on G *as a* $\mathbb{Z}$*-module:*

For every $x, y \in G$*:*

- $v(x) = \infty \quad \textit{iff} \quad x = 0$,
- $v(nx) = v(x) \quad \forall\, n \in \mathbb{Z},\ n \neq 0$,
- $v(x+y) \geqslant \min\{v(x), v(y)\}$.

(3) *if* $x \in G$, $x \neq 0$, $v(x) = \gamma$, *then*

$$\begin{aligned} G^\gamma &:= \{a \in G : v(a) \geqslant \gamma\} = C_x. \\ G_\gamma &:= \{a \in G : v(a) > \gamma\} = D_x. \end{aligned}$$

So

$$B_x = C_x/D_x = G^\gamma/G_\gamma = B(\gamma)$$

is the archimedean component associated to γ*.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (28: 04/02/10)

SALMA KUHLMANN

Contents

1. Examples

If G is a Hahn group, namely a Hahn sum

$$G = \bigsqcup_{\gamma\in\Gamma} B(\gamma)$$

or a Hahn product

$$G = \mathrm{H}_{\gamma\in\Gamma}\, B(\gamma)$$

as in section 2 of Lecture 23, then the valued $\mathbb{Q}$-vector space $(G, v_{\min})$ is isomorphic to (G, v), where v is the natural valuation explained in the last lecture (Lecture 27, section 3). Namely

$$\forall\, x, y \in G \qquad v(x) = v(y) \;\Leftrightarrow\; v_{\min}(x) = v_{\min}(y).$$

2. Valued fields

Definition 2.1. Let K be a field, G an ordered abelian group and ∞ an element greater than every element of G. A surjective map

$$w\colon K \longrightarrow G \cup \{\infty\}$$

is a **valuation** if and only if $\forall\, a, b \in K$:

(i) $w(a) = \infty \;\Leftrightarrow\; a = 0.$

(ii) $w(ab) = w(a) + w(b).$

(iii) $w(a - b) \geqslant \min\{w(a), w(b)\}.$

Immediate consequences are:

- $w(a) = w(-a)$,
- $w(a^{-1}) = -w(a)$ if $a \neq 0$,
- $w(a) \neq w(b) \;\Rightarrow\; w(a+b) = \min\{w(a), w(b)\}$.

Definition 2.2.

$$R_w := \{a \in K : w(a) \geqslant 0\} \text{ is the } \textbf{valuation ring}.$$
$$I_w := \{a \in K : w(a) > 0\} \text{ is the } \textbf{valuation ideal}.$$

Lemma 2.3. *I_w is an ideal of the ring R_w and it is maximal proper.*

Thus R_w/I_w is a field denoted by K_w and called the **residue field**.
The **residue map** is the canonical surjection:

$$\begin{array}{ccc} R_w & \longrightarrow & R_w/I_w \\ b & \mapsto & b + I_w := b_w \end{array}$$

The **group of units** of the valuation ring R_w is given by

$$\mathcal{U}_w = \{a \in K : w(a) = 0\}$$

and it is a subgroup of the multiplicative group of R_w.
The **group of 1-units** is the multiplicative subgroup of $\mathcal{U}_w$ given by

$$1 + I_w = \{a \in K : w(a-1) > 0\}.$$

3. The natural valuation of an ordered field

Let $(K, +, \cdot, 0, 1, <)$ be a totally ordered field.

Remark 3.1. $(K, +, 0, <)$ is a totally ordered divisible abelian group.

So we have the natural valuation v on K as a $\mathbb{Q}$-vector space. Setting $G := v(K \setminus \{0\})$, we have:

$$\begin{array}{rcl} v\colon K & \longrightarrow & G \cup \{\infty\} \\ 0 \neq a & \mapsto & v(a) := [a] \\ 0 & \mapsto & \infty \end{array}$$

We shall show now that we can endow the totally ordered value set $(G, <)$ with a group operation $+$ such that $(G, +, <)$ is a totally ordered abelian group. For every $a, b \in K \setminus \{0\}$ define

$$[a] + [b] := [ab].$$

Lemma 3.2. *This addition is well defined and $(G, +, <)$ is a totally ordered abelian group.*

4. The field of power series

Let K be a field and G a totally ordered abelian group.

The field of formal power series with coefficients in K and exponent in G is the set of formal objects

$$K((G)) := \{s = \sum_{g \in G} s(g)t^g : s(g) \in K \text{ and } \operatorname{support}(s) = \{g \in G : s(g) \neq 0\} \text{ is well ordered in G}\}$$

with the following addition and multiplication:

$$(\sum_{g \in G} s(g)t^g) + (\sum_{g \in G} r(g)t^g) := \sum_{g \in G} (s(g) + r(g))\, t^g.$$

$$(\sum_{g \in G} s(g)t^g) \cdot (\sum_{g \in G} r(g)t^g) := \sum_{g \in G} (\sum_{g' \in G} r(g')s(g - g'))\, t^g.$$

Lemma 4.1. *This multiplication is well defined:*

(1) *the sum is finite.*
(2) $\operatorname{support}(rs)$ *is well ordered.*

To see that $K((G))$ is a field, we compute the inversion function. Let $s \in K((G))$ with $\min \operatorname{support}(s) = g_0$. We can write

$$s = s(g_0)t^{g_0}(1 + \varepsilon),$$

and then

$$s^{-1} = \frac{1}{s(g_0)} t^{-g_0}(1 + \varepsilon)^{-1},$$

with

$$(1 + \varepsilon)^{-1} = \sum_{i \in \mathbb{N}} a_i \varepsilon^i.$$

Example 4.2. If $G = \mathbb{Z}$ and $K = \mathbb{R}$, $K((G)) = \mathbb{R}((\mathbb{Z}))$ is the field of Laurent series with coefficients in $\mathbb{R}$:

$$s = \sum_{n=-m}^{\infty} s(n)t^n \qquad s(n) \in \mathbb{R}.$$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (29: 09/02/10)

SALMA KUHLMANN

Contents

1. Hardy fields

Definition 1.1. (Hardy field) Consider the set of all real valued functions defined on positive half lines:

$$\mathcal{F} := \{f \mid f\colon [a,\infty) \to \mathbb{R} \text{ or } f\colon (a,\infty) \to \mathbb{R},\ a \in \mathbb{R}\}.$$

For every $f, g \in \mathcal{F}$ we define

$$f \sim g \ \Leftrightarrow\ \exists\, N \in \mathbb{N} \text{ s.t. } f(x) = g(x)\ \forall\, x \geqslant N.$$

When $f \sim g$ we say that f and g **have the same germ at** ∞.
We identify $f \in \mathcal{F}$ with its germ $[f]$.

We denote by $\mathcal{G}$ the set of all germs. Note that $\mathcal{G}$ is a commutative ring with 1 by:

$$[f] + [g] := [f+g]$$
$$[f] \cdot [g] := [f \cdot g]$$

A subring H of $\mathcal{G}$ is a **Hardy field** if it is a field with respect to the operations above and it is closed under differentiation, i.e.

$$f \in H \ \Rightarrow\ f' \in H.$$

Remark 1.2. (defininig a total order on a Hardy field). Let H be a Hardy field and $f \in H$, $f \neq 0$.

Since $1/f \in H$, $f(x) \neq 0$ ultimately. Moreover since $f' \in H$, f is ultimately differentiable and thus ultimately continuous.

It follows that $\operatorname{sign}(f)$ is constant ultimately (i.e. f is strictly positive on some interval (N,∞) or f is strictly negative on some interval (N,∞)).

This key property allows us to define a total order on H:

Definition 1.3. Let H be a Hardy field. For every f, g we define

$$f > g \;\Leftrightarrow\; f - g \text{ is ultimately positive.}$$

Lemma 1.4. *$>$ above is an ordering on H.*

Examples 1.5.

(1) $\mathbb{Q}$ and $\mathbb{R}$ are Hardy fields consisting of just constant germs. They are archimedean Hardy fields.

(2) Let x denote the germ of the identity function. Then $\mathrm{x} > \mathbb{R}$ and $\mathbb{R}(\mathrm{x})$ is a non-archimedean Hardy field.

Lemma 1.6. *(Monotonicity) Let H be a Hardy field and $f \in H$, $f' \neq 0$. Since f' is ultimately positive or negative, it follows that f is ultimately increasing or decreasing. Therefore*

$$\exists \lim_{x\to\infty} f(x) \in \mathbb{R} \cup \{-\infty, +\infty\}.$$

2. The natural valuation of a Hardy field

Definition 2.1. (Valuation on H). Let H be a Hardy field. Define for $f, g \neq 0$

$$f \sim g \;\Leftrightarrow\; \lim_{x\to\infty} \frac{f(x)}{g(x)} = r \in \mathbb{R} \setminus \{0\}.$$

This is an equivalence relation. Denote the equivalence class of f by $v(f)$. Define

$$v(f) + v(g) := v(fg),$$

and

$$v(f) > v(g) \;\Leftrightarrow\; \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Lemma 2.2. *The map*

$$\begin{array}{rcl} H & \longrightarrow & H/\sim \cup \{\infty\} \\ 0 \neq f & \mapsto & v(f) \\ 0 & \mapsto & \infty \end{array}$$

is a valuation and it is equivalent to the natural valuation.

Remark 2.3.

$$R_v = \{f : \lim_{x\to\infty} f(x) \in \mathbb{R}\}.$$

$$I_v = \{f : \lim_{x\to\infty} f(x) = 0\}.$$

$$\mathcal{U}_v = \{f : \lim_{x\to\infty} f(x) \in \mathbb{R} \setminus \{0\}\}.$$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (30: 11/02/10)

SALMA KUHLMANN

Contents

1. Convex valuations

Let K be a non-archimedean ordered field. Let v be its non-trivial natural valuation with valuation ring R_v and valuation ideal I_v.

Remark 1.1.

(1) R_v/I_v is archimedean.

(2) R_v is the convex hull of $\mathbb{Q}$ in K.

Let w be any valuation of K with valuation ring R_w, valuation ideal I_w and residue field $K_w := R_w/I_w$.

Definition 1.2. We say that w **is compatible with the order** if $\forall\, a, b \in K$

$$0 < a \leqslant b \;\Rightarrow\; w(a) \geqslant w(b).$$

Compatible valuations are also called **convex valuations**.

Example 1.3. The natural valuation is compatible with the order.

Remark 1.4. We recall that a subset C of a totally ordered set X is said to be **convex** if $\forall\, c_1, c_2 \in C$ and $x \in X$:

$$c_1 < x < c_2 \;\Rightarrow\; x \in C.$$

If C is a subgroup of an ordered abelian group A, equivalently C is convex if and only if $\forall\, c \in C$ and $a \in A$:

$$0 < a < c \;\Rightarrow\; a \in C.$$

Proposition 1.5. *(Characterization of convex valuations). The following are equivalent:*

(1) *w is compatible with the order of K.*

(2) *R_w is convex.*

(3) *I_w is convex.*

(4) *$I_w < 1$.*

(5) *$1 + I_w \subseteq K^{>0}$.*

(6) *The residue map*

$$\begin{array}{ccc} R_w & \longrightarrow & R_w/I_w \\ a & \mapsto & a + I_w \end{array}$$

induces an ordering on Kw given by

$$a + I_w \geqslant 0 \;\Leftrightarrow\; a \geqslant 0.$$

(7) *The set*

$$\mathcal{U}_w^{>0} := \{a \in K : w(a) = 0 \;\wedge\; a > 0\}$$

of positive units is a convex subgroup of $(K^{>0}, \cdot, 1, <)$.

Proof. (1) $\Rightarrow$ (2). $0 \leqslant a \leqslant b \in R_w \Rightarrow w(a) \geqslant w(b) \geqslant 0$.

(2) $\Rightarrow$ (3). Let $a, b \in K$ with $0 < a < b \in I_w$. Since $w(b) > 0$, it follows that $w(b^{-1}) = -w(b) < 0$ and then $b^{-1} \notin R_w$.
Therefore also $a^{-1} \notin R_w$, because $0 < b^{-1} < a^{-1}$ and R_w is convex by assumption. Hence $w(a) > 0$ and $a \in I_w$.

(3) $\Rightarrow$ (4). Otherwise $1 \in I_w$ but $w(1) = 0$, contradiction.

(4) $\Rightarrow$ (5). Clear.

□

2. Comparison of convex valuations

Let w and w' be valuations on K. We say that w' is **finer** than w or w is **coarser** than w' if w' has a smallest valuation ring, i.e. if

$$R_{w'} \subsetneq R_w.$$

Lemma 2.1.

(1) *$R_{w'} \subsetneq R_w$ if and only if $I_w \subsetneq I_{w'}$.*

(2) *If w' is convex and $R_{w'} \subsetneq R_w$, then w is also convex.*

(3) *The set $\mathcal{R}$ of all convex valuation rings R_w is totally ordered by inclusion.*

(4) *The natural valuation is the finest convex valuation, i.e.*

$$R_v \subsetneq R_w,$$

for every convex valuation $w \neq v$.

3. The rank of ordered fields

Definition 3.1. Let K be an ordered field with natural valuation v. The set $\mathcal{R}$ of all valuation rings R_w of convex valuations $w \neq v$ is called the **rank** of K.

Examples 3.2.

- The rank of an archimedean ordered field is empty since its natural valuation is trivial.
- The rank of the rational function field $K = \mathbb{R}(t)$ with any order is a singleton.

4. Convex valuations and convex subgroups

Notation 4.1. For simplicity we denote by $w(K)$ the value group of a valuation w on K (even if $w(0) = \infty$).

To every convex valuation w on K we associate a convex subgroup G_w of $v(K)$, namely

$$G_w := \{v(a) : a \in K \wedge w(a) = 0\} = v(\mathcal{U}_w^{>0}).$$

Proposition 4.2.

$$w(K) \;\cong\; v(K)/G_w$$

canonically.

Proof. The map

$$\begin{array}{rcl} v(K)/G_w & \longrightarrow & w(K) \\ v(a) + G_w & \mapsto & w(a) \end{array}$$

is well defined and an isomorphism. □

We call G_w **the convex subgroup associated to** w. Note that the convex subgroup G_v associated to the natural valuation v is

$$G_v = \{0\}.$$

Conversely, given a convex subgroup G_w of $v(K)$ we define a map:

$$\begin{array}{rcl} w\colon K & \longrightarrow & v(K)/G_w \cup \{\infty\} \\ 0 \neq a & \mapsto & v(a) + G_w \\ 0 & \mapsto & \infty \end{array}$$

Then w is a convex valuation with $v(\mathcal{U}_w^{>0}) = G_w$. We call w the convex valuation associated to G_w.

We have proved the following theorem:

Theorem 4.3. *There is a bijection between the set of convex valuations on an ordered field K and the set of convex subgroups of the value group $v(K)$ associated to the natural valuation v.*