Inhaltsverzeichnis zur Vorlesung: Reelle algebraische Geometrie I  
Prof. Dr. Salma Kuhlmann, Dr. Maria Infusino, Charu Goel  

<table>
<thead>
<tr>
<th>Vorlesung (Datum)</th>
<th>Inhalt</th>
<th>Seite</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Vorlesung (22. Oktober 2009)</td>
<td>The field $\mathbb{R}(x)$ - Dedekind cuts - The orderings on $\mathbb{R}(x)$ - Order preserving embeddings</td>
<td>5</td>
</tr>
</tbody>
</table>
13. Vorlesung (1. Dezember 2009)
The Tarski-Seidenberg Principle Seite 52

The Tarski-Seidenberg Principle (Fortsetzung) Seite 56
Appendix 1: Order on the set of tuples of integers Seite 58

The polynomial ring $\mathbb{R}[X]$ - Borel measure - Preordering Seite 62

Introduction - Examples - Positivstellensatz Seite 65

Geometric version of Positivstellensatz - Exkurs in commutative algebra Seite 70

Exkurs in commutative algebra (continued) - Radical ideals and Real ideals - The Real Spectrum Seite 77

The Real Spectrum - Topologies on $Sper(A)$ - Abstract Positivstellensatz Seite 83

Generalities about polynomials - PSD- and SOS-polynomials - Convex sets, cones and extremality Seite 88

Convex Cones and generalization of Krein-Milman theorem - The cones $\mathcal{P}_{n,2d}$ and $\sum_{n,2d}$ - Proof of $\mathcal{P}_{3,4} = \sum_{3,4}$ Seite 92

Proof of Hilbert’s theorem Seite 97

Proof of Hilbert’s Theorem (continued) - The Motzkin Form - Robinson Method (1970) - The Robinson Form Seite 104

Ring of formal power series - Algebraic independence Seite 110

Algebraic independence and transcendence degree - Krull Dimension of a ring - Low Dimension Seite 114
Schmüdgen’s Positivstellensatz - Seite 118
Representation theorem (Stone-Krivine, Kadison-Dubois) -
Preprimes, modules and semi-ordering in rings

27. **Vorlesung (27. Mai 2010)**
Archimedean modules - Seite 123
Representation Theorem (Stone-Krivine, Kadison-Dubois)

Rings of bounded elements - Schmüdgen’s Positivstellensatz Seite 127

Schmüdgen’s Nichtnegativstellensatz - Application of Schmüdgen’s Seite 132
Positivstellensatz to the moment problem

Application of Schmüdgen’s Positivstellensatz to the moment problem Seite 136
Schmüdgen’s Nichtnegativstellensatz und Hankel matrices -
Finite solvability of the $K$-Moment Problem - Haviland’s Theorem
1. Orderings

Definition 1.1. \textit{(partielle Anordnung)} Let $\Gamma$ be a non-empty set and let $\leq$ be a relation on $\Gamma$ such that:

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

(ii) $\gamma_1 \leq \gamma_2$, $\gamma_2 \leq \gamma_1 \implies \gamma_1 = \gamma_2 \quad \forall \gamma_1, \gamma_2 \in \Gamma$,

(iii) $\gamma_1 \leq \gamma_2$, $\gamma_2 \leq \gamma_3 \implies \gamma_1 \leq \gamma_3 \quad \forall \gamma_1, \gamma_2, \gamma_3 \in \Gamma$.

Then $\leq$ is a \textbf{partial order} on $\Gamma$ and $(\Gamma, \leq)$ is said to be a \textbf{partially ordered set}.

Example 1.2. Let $X$ be a non-empty set. For every $A, B \subseteq X$, the relation $A \subseteq B \iff A \subseteq B$ is a partial order on the power set $\mathcal{P}(X) = \{ A : A \subseteq X \}$.

Definition 1.3. \textit{(totale Anordnung)} A partial order $\leq$ on a set $\Gamma$ is said to be \textbf{total} if

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

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

$\gamma_1 < \gamma_2 \iff \gamma_1 \leq \gamma_2 \text{ and } \gamma_1 \neq \gamma_2$,

$\gamma_1 \geq \gamma_2 \iff \gamma_2 \leq \gamma_1$,

$\gamma_1 > \gamma_2 \iff \gamma_2 \leq \gamma_1 \text{ and } \gamma_1 \neq \gamma_2$. 

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

$$(a_1, b_1) \leq (a_2, b_2) \iff a_1 \leq a_2 \text{ and } b_1 \leq b_2.$$ 

Then $(\mathbb{R} \times \mathbb{R}, \leq)$ 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

$$(a_1, b_1) \leq_l (a_2, b_2) \iff [a_1 < a_2] \text{ or } [a_1 = a_2 \text{ and } b_1 \leq b_2].$$ 

Then $(\mathbb{R} \times \mathbb{R}, \leq_l)$ 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 $\leq$ be a total order on $K$ such that:

(i) $x \leq y \Rightarrow x + z \leq y + z \quad \forall x, y, z \in K$,

(ii) $0 \leq x, 0 \leq y \Rightarrow 0 \leq xy \quad \forall x, y \in K$.

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

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

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

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

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

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

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

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

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

1. \(\text{sign}(ab) = \text{sign}(a) \text{sign}(b)\),
2. \(|ab| = |a| |b|\),
3. \(|a + b| \leq |a| + |b|\).

3. **Archimedean fields**

**Definition 3.1.** (archimedischer Körper) Let \((K, \leq)\) 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 \((\Gamma, \leq)\) be an ordered set and let \(\Delta \subseteq \Gamma\). Then

- \(\Delta\) is **cofinal** (kofinal) in \(\Gamma\) if
  \[ \forall \gamma \in \Gamma \; \exists \delta \in \Delta \; \text{such that} \; \gamma \leq \delta. \]
- \(\Delta\) is **coinitial** (koinitial) in \(\Gamma\) if
  \[ \forall \gamma \in \Gamma \; \exists \delta \in \Delta \; \text{such that} \; \delta \leq \gamma. \]
- \(\Delta\) is **coterminal** (koterminal) in \(\Gamma\) if \(\Delta\) is cofinal and coinitial in \(\Gamma\).

**Example 3.3.** Let \((K, \leq)\) 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 \((K, \leq)\) is an Archimedean field and \(Q \subseteq K\) is a subfield, then \((Q, \leq)\) is an Archimedean field.
- \((\mathbb{R}, \leq)\) is an Archimedean field and therefore also \((\mathbb{Q}, \leq)\) is.

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

\[ |a| \leq n|b| \text{ and } |b| \leq n|a|. \]

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

\[ ff(\mathbb{R}[x]) = \mathbb{R}(x) := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x] \text{ and } g(x) \neq 0 \right\}. \]
Let \( f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{R}[x] \) and let \( k \in \mathbb{N} \) the smallest index such that \( a_k \neq 0 \) (and therefore actually \( f(x) = a_nx^n + \cdots + a_kx^k \)). We define
\[
f(x) > 0 \iff a_k > 0
\]
and then for every \( f(x), g(x) \in \mathbb{R}[x] \) with \( g(x) \neq 0 \) we define
\[
\frac{f(x)}{g(x)} \geq 0 \iff f(x)g(x) \geq 0.
\]
This is a total order on \( K = \text{ff} (\mathbb{R}[x]) \) which makes \( (K, \leq) \) an ordered field. We claim that \( (K, \leq) \) 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 \( x \in K \) is infinitesimal and the element \( 1/x \in K \) is infinite. Therefore \( (K, \leq) \) is not Archimedean.
1. The field \( \mathbb{R}(x) \)

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

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

\[
 f(x) > 0 \iff a_k > 0
\]

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

\[
 \frac{f(x)}{g(x)} \geq 0 \iff f(x)g(x) \geq 0.
\]

This is a total order on

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

which makes \( (\mathbb{R}(x), \leq) \) an ordered field.

**Remark 1.2.** By the definition above

\[
 f(x) = x - r < 0 \quad \forall r \in \mathbb{R}, \; r > 0.
\]

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

\[
 0 < x < r \quad \forall r \in \mathbb{R}, \; r > 0.
\]

We can see that there is no other ordering on \( \mathbb{R}(x) \) which satisfies the above property:
Proposition 1.3. Let $\leq$ be the ordering on $\mathbb{R}(x)$ defined in 1.1. Then $\leq$ is the unique ordering on $\mathbb{R}(x)$ such that

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

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

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

Then (see Proposition 2.4 of last lecture)

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

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

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

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

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

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

Then

$$|xh(x)| \leq c|x| < |a_k|,$$

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

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

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

2. Dedekind cuts

Notation 2.1. Let $(\Gamma, \leq)$ 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 $L \leq U$)

Definition 2.2. (Dedekindschnitt) Let $(\Gamma, \leq)$ be a totally ordered set. A Dedekind cut of $(\Gamma, \leq)$ 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 \( L \cap U = \emptyset \). Therefore the subsets \( L, U \) form a partition of \( \Gamma \) (The letter "L" stands for "lower cut" and the letter "U" for "upper cut").

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

\[
\begin{align*}
\gamma_- & := (-\infty, \gamma], [\gamma, \infty[ \\
\gamma_+ & := (-\infty, \gamma], \gamma, \infty[
\end{align*}
\]

Moreover if we take \( L, U \in \{\emptyset, \Gamma\} \), then we have two more cuts:

\[
-\infty := (\emptyset, \Gamma), \quad +\infty := (\Gamma, \emptyset)
\]

Example 2.5. Consider the Dedekind cut \( (L, U) \) of \( (\mathbb{Q}, \leq) \) 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 \( (\Gamma, \leq) \). 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 \( (\Gamma, \leq) \) is free if \( L \neq \emptyset, U \neq \emptyset, L \) has no maximum element and \( U \) has no least element.

Definition 2.8. (Dedekindvollständigkeit) A totally ordered set \( (\Gamma, \leq) \) is said to be Dedekind complete if for every pair \( (L, U) \) of subsets of \( \Gamma \) with \( L \neq \emptyset, U \neq \emptyset \) and \( L \leq U \), there exists \( \gamma \in \Gamma \) such that

\[
L \leq \gamma \leq U.
\]

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

Examples 2.10.

- The ordered set of the reals \( (\mathbb{R}, \leq) \) is Dedekind complete, i.e. the set of Dedekind cuts of \( (\mathbb{R}, \leq) \) is \( \{a_\pm : a \in \mathbb{R}\} \cup \{-\infty, +\infty\} \).

- We have already seen in 2.5 that \( (\mathbb{Q}, \leq) \) 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 \( \mathbb{R}(x) \)

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

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

\leq \quad \mapsto \quad C_X^{\leq}

We now want to find a map

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

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

\[0 < y < r \quad \forall \ r \in \mathbb{R}, \ r > 0.\]

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 \((\mathbb{R}, \leq)\) into the set of orderings of \(\mathbb{R}(x)\). It is precisely the inverse of \(f\).

\[\square\]

4. ORDER PRESERVING EMBEDDINGS

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

\[\varphi : K \hookrightarrow F\]

is said to be an order preserving embedding if

\[a \leq b \quad \Rightarrow \quad \varphi(a) \leq \varphi(b) \quad \forall \ a, b \in K.\]

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

\[\varphi : K \hookrightarrow \mathbb{R}.\]

*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 \(I_a \leq F_a\) 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, \(\varphi\) 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 \(\varphi(a) + \varphi(b) \leq \varphi(a + b)\) and \(\varphi(a) + \varphi(b) \geq \varphi(a + b)\). This proves that \(\varphi\) is additive. Similarly one gets \(\varphi(ab) = \varphi(a)\varphi(b)\).

\[\square\]
# Real Algebraic Geometry Lecture Notes

(03: 27/10/09)

Salma Kuhlmann

## Contents

1. Preorderings and positive cones 1
2. A crucial Lemma 3
3. Several consequences 3

## 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 $\forall x, y \in K$

$$x \leqslant y \iff y - x \in P$$

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

$$\varphi : F \rightarrow K$$

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 $\text{char}(K) \neq 2$. 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 $\forall t_1, t_2, t_3, t_4 \in T$,

$$(t_1 - at_2)(t_3 - at_4) = t_1 t_3 + a^2 t_2 t_4 - a(t_1 t_4 + t_2 t_3) \in T - aT,$$

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

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

($\subseteq$) 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. $\forall n \in \mathbb{N}, \forall a_1, \ldots, a_n \in K$
   \[ \sum_{i=1}^{n} a_i^2 = 0 \implies a_1 = \cdots = a_n = 0. \]

Proof. (1) $\implies$ (2) $\implies$ (3) obvious. We show now (3) $\iff$ (4).

($\Rightarrow$) Let $\sum_{i=1}^{n} a_i^2 = 0$ and suppose $a_i \neq 0$ for some $1 \leq i \leq n$. 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). \qed

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
\[ a \geq_P 0 \text{ for every ordering } P \iff a \in \sum K^2. \]
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 $P \subseteq Q$ (equivalently $Q \cap K = P$).

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

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

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

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.

\[\square\]

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

\[L = K(\alpha) \cong K[x]/(f),\]

where \(f\) is the minimal polynomial of \(\alpha\) over \(K\). Therefore \(\deg(f) = n\), \(f(\alpha) = 0\) and for every \(g(x) \in K[x]\) 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 \(\forall i = 1, \ldots, s\) \(0 \neq g_i(x) \in K[x]\) and \(\deg(g) < n\). Since

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

it follows that

\[1 + \sum_{i=1}^{s} p_i g_i(x)^2 = f(x)h(x), \quad h(x) \in K[x].\]
Define \( d := \max\{\deg(g_i) : i = 1, \ldots, s\} \). Then \( d < n \) and the polynomial \( f(x)h(x) \) has degree \( 2d \). The coefficient of \( x^{2d} \) is of the form
\[
\sum_{i=1}^{r} p_i b_i^2, \\
\text{with } p_i \in P \text{ and } b_i \in K, \ b_i \neq 0, \text{ so}
\]
\[
\sum_{i=1}^{r} p_i b_i^2 > P \quad 0.
\]

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

Let \( h_1(x) \) be an irreducible factor of \( h(x) \) of odd degree and suppose \( \beta \) is a root of \( h_1(x) \). 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 \( n \).

\[\square\]

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).

$\text{(iii)} \Rightarrow (i)$. 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 $G = \text{Gal}(L/K)$, $|G| = [L : K] = 2^am, \ a \geq 1, m$ 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:

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

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 $L/K$. □
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 $(K, \leq)$ 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 \( c \in K, c \geq 0 \) such that 

\[
a^2 + b^2 = c^2.
\]

Since \( a^2 \leq a^2 + b^2 = c^2 \), \( |a| \leq c \), so \( c + a \geq 0 \), \( c - a \geq 0 \) \((-c \leq a \leq c)\).
Therefore \( \frac{1}{2}(c \pm a) \in K^2 \). Let \( d, e \in K, d, e \geq 0 \) such that 

\[
\frac{1}{2}(c + a) = d^2 \quad \text{and} \quad \frac{1}{2}(c - a) = e^2.
\]

So 

\[
d = \frac{\sqrt{c + a}}{\sqrt{2}} \quad \text{and} \quad e = \frac{\sqrt{c - a}}{\sqrt{2}}.
\]

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

\[
y^2 = (d + e\sqrt{-1})^2 = d^2 + (e\sqrt{-1})^2 + 2de\sqrt{-1} = \frac{1}{2}(c + a) - \frac{1}{2}(c - a) + 2 \cdot \frac{1}{2} \sqrt{(c - a)(c + a)} \sqrt{-1} = \frac{1}{2}a + \frac{1}{2}a + \sqrt{c^2 - a^2} \sqrt{-1} = a + \sqrt{b^2} \sqrt{-1} = a + b \sqrt{-1} = x.
\]

\[\square\]

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 \( G := \text{Gal}(L/K) \). Then \( |L : K| = |G| = 2^am, a \geq 1, m \) odd.

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

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

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 \(G_1 := \text{Gal}(L/K(\sqrt{-1}))\), let \(S_1\) be a subgroup of \(G_1\) of index 2, and \(F_1 := \text{Fix}(S_1)\). 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. \(\square\)

**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 \(R[x]\)

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

1. if \(f(x)\) is monic and irreducible then
   \[f(x) = x - a \quad \text{or} \quad f(x) = (x - a)^2 + b^2, \quad b \neq 0;\]

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

**Proof.** Let \(f(x) \in R[x]\) be monic and irreducible. Then \(\deg(f) \leq 2\).

Suppose not, and let \(\alpha \in R\) a root of \(f(x)\). Then

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

On the other hand, by 2.2

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

contradiction.

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

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

We claim that \(c - a^2 > 0\). If not,

\[
(c - a^2) \leq 0 \Rightarrow -(c - a^2) \geq 0 \Rightarrow a^2 - c \geq 0,
\]

the discriminant \(4(a^2 - c) \geq 0\), \(f(x)\) has a root in \(R\) and factors, contradiction.

Therefore \((c - a^2) \in R^2\) and there is \(b \in R\) such that \((c - a^2) = b^2 \neq 0\). \(\square\)
Corollary 3.2. (Zwischenwertsatz : Intermediate value Theorem) Let $R$ be a real closed field, $f(x) \in R[x]$. 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,

$$f(x) = d \prod_{i=1}^{n} (x - a_i) \prod_{j=1}^{m} (x - d_j)^2 + b_j^2$$

$$= d \prod_{i=1}^{n} l_i(x)q(x),$$

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

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

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

if we had that 

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

we would have 

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

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 $f(x)$. □

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

1. Counting roots in an interval 1
2. Bounding the roots 2
3. Changes of sign 3

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

1. Counting roots in an interval

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

$$f(x) = (x - a)^mh(x)$$

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

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

Corollary 1.2. (Generalized Intermediate Value Theorem: Verstärkung Zwischenwertsatz). Let $f(x) \in R[x]; a, b \in R, a < b, f(a)f(b) < 0$ (i.e. $f(a) < 0 < f(b)$ or $f(b) < 0 < f(a)$). Then the number of roots of $f(x)$ 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

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

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

Note that $g(x)$ 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 $g(x)$ is positive everywhere).

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

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

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

In particular if $L_i(x)$ changes sign we must have $L_i(a) < 0 < L_i(b)$ as well.
Let us count the number of distinct \( i \in \{1, \ldots, n\} \) 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
\[
|\{ i \in \{1, \ldots, n\} : L_i(a) < 0 < L_i(b)\}| = M \geq 1 \quad \text{odd.}
\]
Say these are \( L_1, \ldots, L_M \). 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 \( \forall i = 1, \ldots, M \) and \( M \) is odd, it follows that \( \sum \) is odd as well.

2. Bounding the roots

**Corollary 2.1.** Let \( f(x) \in R[x] \), \( f(x) = dx^m + d_{m-1}x^{m-1} + \cdots + d_0 \). Set
\[
D := 1 + \sum_{i=m-1}^{0} \left| \frac{d_i}{d} \right| \in R.
\]
Then
(i) \( a \in R, f(a) = 0 \implies |a| < D \); (i.e. \( f \) has no root in \( ]-\infty, -D[ \cup [D + \infty[ \) )
(ii) \( y \in [D, +\infty[ \implies \text{sign}(f(y)) = \text{sign}(d) \);
(iii) \( y \in ]-\infty, -D[ \implies \text{sign}(f(y)) = (-1)^m \text{sign}(d) \).

**Proof.**
(i) For every \( i = 0, \ldots, m-1 \) set \( b_i := \frac{d_i}{d} \) and compute for \( |y| \geq D \):
\[
f(y) = dy^m(1 + b_{m-1}y^{-1} + \cdots + b_0y^{-m}).
\]
Now
\[
|b_{m-1}y^{-1} + \cdots + b_0y^{-m}| \leq (|b_{m-1}| + \cdots + |b_0|)D^{-1} < 1.
\]
(ii) If \( y \geq D \) then \( f(y) = d\prod (y - a_i)^{m_i}q(y) \) where \( \text{deg}(q) \) is even and \( y - a_i > 0 \).
(iii) If \( y \leq -D \) 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 \( f(x) \in R[x] \), \( a < b \in R \) 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 \((f - k)(x)\)).

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

\[ f(x) = (x - a)^m(x - b)^ng(x), \]

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

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

where

\[ g_1(x) := m(x - b)g(x) + n(x - a)g(x) + (x - a)(x - b)g'(x). \]

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) \( g_1(x) \) has a root in \([a, b]\) and so does \( f'(x) \). \( \square \)

**Corollary 2.3.** *(Mittelwertsatz: Mean Value Theorem)* Let \( f(x) \in R[x] \), \( a < b \in R \). 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

\[ F(x) := f(x) - (x - a)f(b - a), \]

since \( F(a) = F(b) \). \( \square \)

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

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

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

\( \square \)
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 \((\text{Vorzeichenwechsel})\) if \(c_ic_{i+1} < 0\).

(ii) Let \((c_1, \ldots, c_n)\) a finite sequence in \(R\). After we have removed all zero’s by the sequence, we define 
\[
\text{Var}(c_1, \ldots, c_n) := |\{i \in \{1, \ldots, n\} : i \text{ is a change of sign}\}|
\]
\[
= |\{i \in \{1, \ldots, n\} : c_i c_{i+1} < 0\}|.
\]

Theorem 3.2. \((\text{Lemma von Descartes})\) Let \(f(x) = a_n x^n + \cdots + a_0 \in R[x], a_n \neq 0\). Then
\[
|\{a \in R : a > 0 \text{ and } f(a) = 0\}| \leq \text{Var}(a_n, \ldots, a_1, a_0).
\]

Proof. By induction on \(n = \text{deg}(f)\). 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
\[
f'(x) = na_n x^{n-1} + \cdots + ra_r x^{r-1},
\]
we know that there are \(\text{Var}(na_n, \ldots, ra_r) = \text{Var}(a_n, \ldots, a_r)\) many positive roots of \(f'\). Set \(c := \text{the smallest such positive root of } f'\) (by convention \(c := +\infty\) if none exists)

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

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

Case 2. Assume \(f\) has exactly \(1 + \text{Var}(a_n, \ldots, a_r)\) positive roots. We claim that in this case
\[
1 + \text{Var}(a_n, \ldots, a_r) = \text{Var}(a_n, \ldots, a_r, a_0).
\]

We observe that \(f\) has a root \(a\) in \([0, c]\).

For \(0 < x \leq c\) we have that \(\text{sign}(f'(x)) = \text{sign}(a_r) \neq 0\), so \(f\) is strictly monotone in the interval \([0, c]\) (Monotonicity Theorem). So
\[
a_r > 0 \Rightarrow a_0 = f(0) < f(a) = 0 \Rightarrow a_0 < 0,
\]
\[
a_r < 0 \Rightarrow a_0 = f(0) > f(a) = 0 \Rightarrow a_0 > 0.
\]

In both cases \(a_0 a_r < 0\) and the claim is established. \(\square\)

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

Proof. Consider \(f(x)\) and \(f(-x)\). By previous Theorem they have both at most \(m - 1\) strictly positive roots in \(R\). So \(f(x)\) has at most \(2m - 2\) non-zero roots and therefore at most \(2m - 1\) roots in \(R\). \(\square\)
REAL ALGEBRAIC GEOMETRY LECTURE NOTES
(07: 10/11/09)

SALMA KUHLMANN

Contents
1. Sturm's Theorem 1

Let $R$ be a real closed field.

1. Sturm's Theorem

Definition 1.1. 

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

\[ f_0 := f, \quad f_1 := f' \quad \text{and} \]
\[ f_0 = f_1 q_1 - f_2 \]
\[ f_1 = f_2 q_2 - f_3 \]
\[ \ldots \]
\[ f_{i-1} = f_i q_i - f_{i+1} \]
\[ \ldots \]
\[ f_{r-2} = f_{r-1} q_{r-1} - f_r \]
\[ f_{r-1} = f_r q_r, \]

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

2. Let $x \in R$. Set

\[ V_f(x) := \text{Var}(f_0(x), \ldots, f_r(x)). \]

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

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

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

\[ |\{c : a \leq c \leq b, \ f(c) = 0\}| = V_f(a) - V_f(b). \]
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

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

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

$$f_{i-1} = q_if_i - f_{i+1}, \quad \text{with } f_{i+1} \neq 0.$$  

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 $\mathrm{sign}(f_{i+1}(c)) = \pm 1$).

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

$$\mathrm{sign}(f_i(x)) \quad \mathrm{sign}(f_{i+1}(x))$$

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

We first examine the case $i = 0$.

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

<table>
<thead>
<tr>
<th>$x \to c_-$</th>
<th>$x = c$</th>
<th>$x \to c_+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_0(x)$</td>
<td>$-\mathrm{sign}(f_1(c))$</td>
<td>$\mathrm{sign}(f_1(c))$</td>
</tr>
<tr>
<td>$f_1(x)$</td>
<td>$\mathrm{sign}(f_1(c))$</td>
<td>$\mathrm{sign}(f_1(c))$</td>
</tr>
<tr>
<td>contribution to $V_f(x)$</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>$x \to d_-$</th>
<th>$x = d$</th>
<th>$x \to d_+$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_{i-1}(x)$</td>
<td>$-\mathrm{sign}(f_{i+1}(d))$</td>
<td>$-\mathrm{sign}(f_{i+1}(d))$</td>
</tr>
<tr>
<td>$f_i(x)$</td>
<td>$0$</td>
<td>$\mathrm{sign}(f_{i+1}(d))$</td>
</tr>
<tr>
<td>$f_{i+1}(x)$</td>
<td>$\mathrm{sign}(f_{i+1}(d))$</td>
<td>$\mathrm{sign}(f_{i+1}(d))$</td>
</tr>
<tr>
<td>contribution to $V_f(x)$</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

$$g_i := f_i/f_r \quad i = 0, \ldots, r.$$
The sequence of polynomials \((g_0, \ldots, g_r)\) satisfies the previous conditions (1) – (4). We can conclude by noticing that:

(i) \(\text{Var}(g_0(x), \ldots, g_r(x)) = \text{Var}(f_0(x), \ldots, f_r(x))\) (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 \(\varphi_i := \text{the leading coefficient of } f_i\).

Set

\[
V_f(-\infty) := \text{Var}((-1)^{d_0}\varphi_0, (-1)^{d_1}\varphi_1, \ldots, (-1)^{d_r}\varphi_r)
\]

\[
V_f(+\infty) := \text{Var}(\varphi_0, \varphi_1, \ldots, \varphi_r).
\]

Then we have:

**Corollary 1.3.** *The number of distinct roots of } f \text{ is } V_f(-\infty) - V_f(+\infty).
REAL ALGEBRAIC GEOMETRY LECTURE NOTES
(08: 12/11/09)

SALMA KUHLMANN

CONTENTS

1. Real closure 1
2. Order preserving extensions 2

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

\[ \mathcal{L} := \{(L, Q) : L \mid K \text{ algebraic, } Q \cap K = P\}. \]

\[ \square \]

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

$K \subseteq R_1$ and $K \subseteq R_2$

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 $f(x) \in K[x]$; then the number of roots of $f(x)$ in $R_1$ is equal to the number of roots of $f(x)$ 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

\[ \varphi: (K, P) \hookrightarrow (S, \sum S^2) \]

an order preserving embedding. Then \(\varphi\) extends to an order preserving embedding

\[ \psi: (L, \sum R^2 \cap L) \hookrightarrow (S, \sum S^2). \]

**Proof.** We recall that if \((K, P)\) and \((L, Q)\) are ordered fields, a field homomorphism \(\varphi: K \rightarrow L\) 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 \(L = K(\alpha)\). Since \(\alpha \in R\), \(\varphi(f)\) has at least one root \(\beta\) in \(S\),

\[ L := K(\alpha) \leftrightarrow \varphi(K)(\beta), \]

so there is at least one extension of \(\varphi\) from \(K\) to \(L\).

Let \(\psi_1, \ldots, \psi_r\) all such extensions of \(\varphi\) 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 \(\tau\) be an extension of \(\varphi\) from \(K\) to \(L'\). In particular \(\tau|_L\) is one of the \(\psi_i\)'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 \(\psi_1(b_1) < 0\).

\[ \square \]

**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

\[ \varphi: (K, P) \hookrightarrow (S, \sum S^2) \]

is an order preserving embedding. Then \(\varphi\) has a uniquely determined extension

\[ \psi: (R, \sum R^2) \hookrightarrow (S, \sum S^2). \]

**Proof.** Consider

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

Let \((L, \psi)\) be a maximal element. Then by Proposition 2.1 we must have \(L = R\).
Therefore we have an order preserving embedding $\psi$ of $R$ extending $\varphi$

$$\psi: R \hookrightarrow S.$$ 

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

Let $f = \text{PolMin}(\alpha | K)$ 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 $\psi: R \hookrightarrow S$ is order preserving, we must have $\psi(\alpha_i) = \beta_i$ for every $i = 1, \ldots, r$. In particular $\alpha = \alpha_j$ for some $1 \leq j \leq r$ 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 $\varphi: R_1 \rightarrow R_2$ $K$-isomorphism (i.e. with $\varphi|_K = \text{id}$).

**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 $p(x) = x^2 - a \in K^{ralg}[x]$ 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 $\varphi: (K, P) \rightarrow S$ an order preserving embedding. Let $L | K$ an algebraic extension. Then there is a bijective correspondence

$$\{ \text{extensions } \psi: L \rightarrow S \text{ of } \varphi \} \leftrightarrow \{ \text{extensions } Q \text{ of } P \text{ to } L \}$$

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

**Proof.**

$(\Rightarrow)$ Let $\psi: L \hookrightarrow S$ an extension of $\varphi$. 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 $\psi$ induces the extension $Q$.
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 $\varphi$ to $\sigma: R \to S$. 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

$$\psi_1: L \to S, \quad \psi_2: L \to S, \quad \psi_{1|K} = \psi_{2|K} = \varphi$$

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 $\psi_1$ and $\psi_2$ to get uniquely determined extensions

$$\sigma_1: R \to S, \quad \sigma_2: R \to S,$$

of $\psi_1$ and $\psi_2$ 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 $\psi_1 = \psi_2$.

\[ \square \]

**Corollary 2.7.** Let $(K,P)$ be an ordered field, $R$ a real closure, $[L:K] < \infty$.

Let $L = K(\alpha)$, $f = \text{MinPol}(\alpha \mid K)$. Then there is a bijection

$$\{\text{roots of } f \text{ in } R\} \to \{\text{extensions } Q \text{ of } P \text{ to } L\}.$$  

Proof. If $\beta$ is a root we consider the $K$-embedding

$$\varphi_\alpha: L \hookrightarrow R$$

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

**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 $p(x) = x^2 - 2$. 
1. Basic version of Tarski-Seidenberg

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

\[
S(X) := \begin{cases} 
  f_1(X) <_1 0 \\
  \vdots \\
  f_k(X) <_k 0 
\end{cases}
\]

where \(\forall i = 1, \ldots, k \ <_i \in \{\geq, >, =, \neq\}\) and \(f_i(X) \in \mathbb{Q}[X]\) or \(f_i(X) \in R[X]\). We say that \(S(X)\) 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 \(S(T; X)\) be a system with coefficients in \(\mathbb{Q}\) in \(m+n\) variables, with \(T = (T_1, \ldots, T_m)\) and \(X = (X_1, \ldots, X_n)\). Then there exist \(S_1(T), \ldots, S_l(T)\) systems in \(m\) variables and coefficients in \(\mathbb{Q}\) such that:

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

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

\[
S(T, X) := \begin{cases} 
  T_1X^2 + T_2X + T_3 = 0 
\end{cases}
\]
Let \( R \) be a real closed field and \((t_1, t_2, t_3) \in \mathbb{R}^3\). Then \( S(t; X) \) has a solution \( X \) in \( R \) if and only if
\[
(t_1 \neq 0 \land t_2^2 - 4t_1t_3 \geq 0) \lor (t_1 = 0 \land t_2 \neq 0) \lor (t_1 = t_2 = t_3 = 0)
\]
\[
S_1(T_1, T_2, T_3) \quad S_2(T_1, T_2, T_3) \quad S_3(T_1, T_2, T_3)
\]

Concise version:
\[
\forall T \left( \exists X : S(T; X) \iff \bigvee_{i=1}^{l} S_i(T) \right).
\]

**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
\[
S(T; X_1, \ldots, X_n) = S(T, X_1, \ldots, X_{n-1}; X_n).
\]

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

for any real closed field \( R \) and any \((t_1, \ldots, t_m, x_1, \ldots, x_{n-1}) \in \mathbb{R}^{m+n-1}\) we have
\[
\exists X_n : S(t_1, \ldots, t_m, x_1, \ldots, x_{n-1}; X_n) \iff \bigvee_{i=1}^{l} S_i(t_1, \ldots, t_m, x_1, \ldots, x_{n-1}).
\]

By induction hypothesis on \( n \):

for every fixed \( i, 1 \leq i \leq l \), \( \exists \) systems \( S_{ij}(T) \), \( j = 1, \ldots, l_i \) such that: for each real closed field \( R \) and each \( t \in \mathbb{R}^{m} \) the system
\[
S_i(t; X_1, \ldots, X_{n-1})
\]
has a solution \((x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1}\) if and only if \( t \) is a solution for one of the systems \( S_{ij}(T) ; j = 1, \ldots, l_i \).

Therefore for any real closed field \( R \) and any \( t \in \mathbb{R}^{m} \)
\[
S(t; X_1, \ldots, X_n) \text{ has a solution } x \in \mathbb{R}^{n} \text{ if and only if } t \text{ is a solution to one of the systems } \{ S_{ij}(T) : i = 1, \ldots, l, j = 1, \ldots, l_i \}
\]

2. **Tarski Transfer Principle I**

**Theorem 2.1.** Let \( S(T; X) \) be a system with coefficients in \( \mathbb{Q} \) in \( m + n \) variables. Let \((K, \leq)\) be an ordered field. Let \( R_1, R_2 \) be two real closed extensions of \((K, \leq)\). Then for every \( t \in K^m \), the system \( S(t; X) \) has a solution \( x \in R_1^n \) if and only if it has a solution \( x \in R_2^n \).
Proof. Let $t \in K^m \subseteq R_1^m \cap R_2^m$. Then there are systems $S_i(T)$ ($i = 1, \ldots, l$) with coefficients in $Q$ and variables $T_1, \ldots, T_m$ such that

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

\[ \square \]

3. TARSKI TRANSFER PRINCIPLE II

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

$$S(X) := \begin{cases} f_1(X) \leq_1 0 \\ \vdots \\ f_k(X) \leq_1 0 \end{cases}$$

where $\forall i = 1, \ldots, k \leq_1 \in \{\geq, >, =, \neq\}$ and $f_i(X) \in K[X_1, \ldots, X_n]$,

has a solution $\underline{x} \in R_1^n \iff$ 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 $\sigma(T, X)$ in $m + n$ variables with coefficients in $Q$ (in fact in $Z$) for which

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

Now we can apply Tarski Transfer I.\[ \square \]

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 $R$

$$S(X) := \begin{cases} f_1(X) <_1 0 \\ \vdots \\ f_k(X) <_1 0 \end{cases}$$

where $\forall i = 1, \ldots, k <_1 \in \{\geq, >, =, \neq\}$ and $f_i(X) \in R[X_1, \ldots, X_n]$,

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

Proof. Apply Tarski Transfer II with $K = R_2 = R$.\[ \square \]
5. Tarski Transfer Principle IV

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

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

where $\forall i = 1, \ldots, k \leq, >, =, \neq$ and $f_i(X) \in R[X_1, \ldots, X_n]$ has a solution $\bar{x} \in F^n \iff$ it has a solution $\bar{x} \in R^n$.

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

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

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

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

**Proof.** Apply Tarski Transfer III. $\square$

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 $I \subseteq R[X]$, if there exists an $R$-algebra homomorphism

$$\varphi: R[X]/I \rightarrow R_1$$

then there exists an $R$-algebra homomorphism

$$\psi: R[X]/I \rightarrow R.$$  

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

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

**Claim.** There is a bijection

$$\{\bar{x} \in R_1^n \text{ solution to } S(X)\} \longleftrightarrow \{\varphi: R[X]/I \rightarrow R_1 \text{ } R\text{-algebra homomorphism}\}$$
Proof of the claim:

Let $x \in \mathbb{R}^n_1$ be a solution to $S(X)$; then the evaluation homomorphism

$$\varphi: \mathbb{R}[X]/I \rightarrow \mathbb{R}_1$$

$$f + I \mapsto f(x)$$

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

Conversely: assume that

$$\varphi: \mathbb{R}[X]/I \rightarrow \mathbb{R}_1$$

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

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

In other words set $(x_1, \ldots, x_n) \in \mathbb{R}^n_1$ 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 $S(X)$ and the $R$-algebra homomorphism $\varphi$ is indeed given by point evaluation at $x = (x_1, \ldots, x_n) \in \mathbb{R}^n_1$.

Now apply Corollary 6.1.
1. Homomorphism Theorems

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

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

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

$$\varphi: A \to R_1$$

then there is an $R$-algebra homomorphism

$$\psi: A \to R.$$ 

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

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

**Proof.**

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

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

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

\[\square\]
We can see that Homomorphism Theorem II implies T-T-III:

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

We first need the following:

**Proposition 1.4.** Let

\[
S(\bar{x}) := \begin{cases} 
  f_1(\bar{x}) <_1 0 \\
  \vdots \\
  f_k(\bar{x}) <_k 0 
\end{cases}
\]

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

\[
\sigma(\bar{x}) := \begin{cases} 
  g_1(\bar{x}) \geq 0 \\
  \vdots \\
  g_s(\bar{x}) \geq 0 \\
  g(\bar{x}) \neq 0 
\end{cases}
\]

for some \( g_1, \ldots, g_s, g \in R[\bar{x}] \).

**Proof.**

- Replace each equality in the original system by a pair of inequalities:
  
  \[
  f_i = 0 \iff \begin{cases} 
    f_i \geq 0 \\
    -f_i \geq 0 
  \end{cases}
  \]

- Replace each strict inequality
  
  \[
  f_i > 0 \text{ by } \begin{cases} 
    f_i \geq 0 \\
    f_i \neq 0 
  \end{cases}
  \]

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

\[
S(\bar{x}) := \begin{cases} 
  f_1(\bar{x}) <_1 0 \\
  \vdots \\
  f_k(\bar{x}) <_k 0 
\end{cases}
\]

Rewrite it as
\[ S(\overline{x}) := \begin{cases} 
  f_1(\overline{x}) \geq 0 \\
  \vdots \\
  f_s(\overline{x}) \geq 0 \\
  g(\overline{x}) \neq 0
\end{cases} \]

with \( f_i(\overline{x}), g(\overline{x}) \in R[x_1, \ldots, x_n] \).

Suppose \( \overline{x} \in R^n \) is a solution of \( S(\overline{x}) \). Consider
\[
A := \frac{R[X_1, \ldots, X_n, Y_1, \ldots, Y_k, Z]}{(Y_1^2 - f_1, \ldots, Y_k^2 - f_k; gZ - 1)},
\]

which is a finitely generated \( R \)-algebra. Consider the \( R \)-algebra homomorphism \( \varphi \) such that
\[
\varphi: A \rightarrow R, \quad \overline{X}_i \mapsto x_i, \quad \overline{Y}_j \mapsto \sqrt{f_j(\overline{x})}, \quad Z \mapsto 1/g(\overline{x}).
\]

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

\[ \square \]

2. **Hilbert’s 17th problem**

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

We know that
\[ f \in \sum R[\overline{x}]^2 \Rightarrow f \geq 0. \]

Now take \( R = \mathbb{R} \). Conversely, for any \( f \in \mathbb{R}[\overline{x}] \) is it true that
\[ f \geq 0 \text{ on } \mathbb{R}^n \Rightarrow f \in \sum \mathbb{R}(\overline{x})^2. \]  

(Hilbert’s 17th problem).

**Remark 2.2.**

1. Hilbert knew that the answer is NO to the more natural question
\[ f \in \mathbb{R}[\overline{x}], \ f \geq 0 \text{ on } \mathbb{R}^n \Rightarrow f \in \sum \mathbb{R}[\overline{x}]^2 \ ? \]

2. If \( n = 1 \) then indeed \( f \geq 0 \text{ on } \mathbb{R} \Rightarrow f = f_1^2 + f_2^2 \).
(3) More generally Hilbert showed that:

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

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

Then

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

Note: only \( d \) even is interesting because

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

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

The first example was given by Motzkin 1967:

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

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

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

We want to show:

\[
f /\not\in T \Rightarrow \exists x \in R^n : f(x) < 0.
\]

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 \( f /\not\in P \). Then \( P \) is an ordering of \( F \) (see proof of Crucial Lemma 2.1 of Lecture 3).

Let \( \leq_P \) be the ordering such that \( (F, \leq_P) \) is an ordered field extension of the real closed field \( R \) (since \( R \) is a real closed field, it is uniquely ordered and we know that \( (F, \leq_P) \) is an ordered field extension). By construction \( f /\not\in P \) so \( f(x) < 0 \). Consider the system

\[
S(x) : \begin{cases}
    f(x) < 0, & f(x) \in R[x].
\end{cases}
\]

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

\[
X = (X_1, \ldots, X_n) \quad X_i \in R(x) = F.
\]

thus by T-T-IV \( \exists x \in R^n \text{ with } f(x) < 0. \)
1. Normal form of semialgebraic sets

Let $R$ be a fixed real closed field and $n \geq 1$. 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

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

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

(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

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

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

(iii) Consider

$$S(x) := \begin{cases} f_1(x) \prec_1 0 \\
\vdots \\
 f_k(x) \prec_k 0 \end{cases}$$

with $f_i(x) \in R[x]$; $\prec_i \in \{\geq, >, =, \neq\}$. The set of solutions of $S(x)$ is precisely the semialgebraic set
The solution set $S$ of a system $(\ast)$ is called a **basic semialgebraic subset** of $\mathbb{R}^n$.

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

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

is called an **algebraic set**.

(v) A subset of $\mathbb{R}^n$ of the form

$$U(f) := \{x \in \mathbb{R}^n : f(x) > 0\},
U(f_1, \ldots, f_k) := \{x \in \mathbb{R}^n : f_1(x) > 0, \ldots, f_k(x) > 0\}$$

$$= U(f_1) \cap \cdots \cap U(f_k)$$

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

(vi) A subset of $\mathbb{R}^n$ of the form

$$K(f) := \{x \in \mathbb{R}^n : f(x) \geq 0\},
K(f_1, \ldots, f_k) = K(f_1) \cap \cdots \cap K(f_k)$$

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 $\mathbb{R}^n$ 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

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

(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:**
\[ (\bigcup_i C_i) \cap (\bigcup_j D_j) = \bigcup_{i,j} (C_i \cap D_j). \]

**Complement:** It is enough to show that the complement of
\[ \{ x \in \mathbb{R}^n : f(x) < 0 \} \quad \forall \in \{ \geq, >, =, \neq \}, \]
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 \( \forall \in \{ \geq, >, =, \neq \} \):
\[ \{ x \in \mathbb{R}^n : f(x) \geq 0 \}^c = \{ x \in \mathbb{R}^n : -f(x) > 0 \} \]
\[ \{ x \in \mathbb{R}^n : f(x) > 0 \}^c = \{ x \in \mathbb{R}^n : f(x) = 0 \} \cup \{ x \in \mathbb{R}^n : -f(x) > 0 \} \]
\[ \{ x \in \mathbb{R}^n : f(x) = 0 \}^c = \{ x \in \mathbb{R}^n : f(x) \neq 0 \}. \]
□

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
\[ \pi : \mathbb{R}^{m+n} = \mathbb{R}^m \times \mathbb{R}^n \rightarrow \mathbb{R}^m \]
\[ (\underline{t}, \underline{x}) \mapsto \underline{t}. \]

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

**Proof.** Since
\[ \pi(\bigcup_i A_i) = \bigcup_i \pi(A_i), \]
it suffices to show the result for a basic semialgebraic subset \( A \) of \( \mathbb{R}^{m+n} \), i.e. show that \( \pi(A) \) is semialgebraic in \( \mathbb{R}^m \).

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

So we can view \( S \) as a system of polynomial equations and inequalities \( S(\underline{u}, T, X) \) with coefficient in \( \mathbb{Q} \) such that \( A \) is the set of solutions in \( \mathbb{R}^{m+n} \) of the system \( S(\underline{u}, T, X) \), i.e.
By Tarski-Seidenberg’s theorem, we have systems of polynomial equalities and inequalities with coefficients in \( \mathbb{Q} \), say \( S_1(u, T), \ldots, S_l(u, T) \), such that for any \( t \in \mathbb{R}^m \) the system \( S(u, t, X) \) has a solution \( x = (x_1, \ldots, x_n) \in \mathbb{R}^n \) if and only if \( (u, t) \) is a solution for one of \( S_1(u, T), \ldots, S_l(u, T) \), i.e.

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

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

**Definition 2.2.** Let \( A \subseteq \mathbb{R}^m \) and \( B \subseteq \mathbb{R}^n \). We say that \( f : A \to B \) is a **semi-algebraic map** if \( A \) and \( B \) are semi-algebraic and

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

is semi-algebraic.

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

2. if \( \Phi \) and \( \Psi \) are first order formulas, then
   \[
   \Phi \land \Psi, \ \Phi \lor \Psi, \ \neg \Phi
   \]
   are also first order formulas (with free variables given by the union of the free variables of \( \Phi \) and the free variables of \( \Psi \));
(3) if $\Phi$ is a first order formula then

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

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

The formulas obtained using just (1) and (2) are called \textbf{quantifier free}.
1. Quantifier elimination 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 \( f(x) \in \mathbb{Q}[x_1, \ldots, x_n], n \geq 1 \), then
   \[ f(x) \geq 0, \ f(x) > 0, \ f(x) = 0, \ f(x) \neq 0 \]
   are first order formulas (with free variables \( x = (x_1, \ldots, x_n) \));

2. If \( \Phi \) and \( \Psi \) are first order formulas, then
   \[ \Phi \land \Psi, \ \Phi \lor \Psi, \ \neg \Phi \]
   are also first order formulas (with free variables given by the union of the free variables of \( \Phi \) and the free variables of \( \Psi \));

3. If \( \Phi \) 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 \( \Phi \) 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 \( \Phi(x) \) and \( \Psi(x) \) are **equivalent** if for every real closed field \( R \) and every \( r \in R^n \),

\[ \Phi(r) \text{ holds in } R \iff \Psi(r) \text{ holds in } R. \]
If $\Phi$ and $\Psi$ 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 conjunctions 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 conjunction of formulas of type (1)). \qed

**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
\[
\begin{align*}
\Phi \lor \Psi & \sim \Phi' \lor \Psi' \\
\Phi \land \Psi & \sim \Phi' \land \Psi' \\
\neg \Phi & \sim \neg \Phi'.
\end{align*}
\]

**Closure under 3.** It is enough to consider $\exists x \Phi$, because
\[
\forall x \Phi \iff \neg \exists x (\neg \Phi).
\]

We claim that if $\Phi$ is equivalent to a quantifier free formula then $\exists x \Phi$ is equivalent to a quantifier free formula. Since
\[
\exists x (\Phi_1 \lor \cdots \lor \Phi_k) \sim (\exists x \Phi_1) \lor \cdots \lor (\exists x \Phi_k),
\]
using the normal form of quantifier free formulas (Remark 1.3), we can assume that $\Phi$ is a finite conjunction of polynomial equations and inequalities (i.e. a system $S(T, x)$).

Applying Tarski-Seidenberg’s Theorem:
\[
\exists x S(T; x) \Leftrightarrow \bigvee_{i=1}^{l} S_i(T),
\]
there exist finitely many finite conjunctions of polynomial equalities and inequalities $\vartheta_1, \ldots, \vartheta_l$ (corresponding to the systems $S_1(T), \ldots, S_l(T)$) such that
\[
\exists x \Phi \sim \vartheta_1 \lor \cdots \lor \vartheta_l.
\]
2. Definable sets

**Definition 2.1.** Let $\Phi(T, X)$ 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 $t \in R^m$. Then $\Phi(t, X)$ 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, $n \geq 1$. A subset $A \subseteq R^n$ is said to be definable (with parameters from $R$) in $R$ if there is a first order formula $\Phi(t, X)$ with parameters $t \in R^m$ and free variables $X = (X_1, \ldots, X_n)$, such that

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

**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

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

The Tarski-Seidenberg Principle is the following result.

**Theorem 1.** Let $f_i(T, X) = h_{i,m_i}(T)X^{m_i} + \ldots + h_{i,0}(T)$ for $i = 1, \ldots, s$ be a sequence of polynomials in $n+1$ variables $(T = (T_1, \ldots, T_n), X)$ with coefficients in $\mathbb{Z}$. Let $\epsilon$ be a function from $\{1, \ldots, s\}$ to $\{-1, 0, 1\}$. Then there exists a finite boolean combination $B(T) := S_1(T) \lor \ldots \lor S_p(T)$ 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 $t \in R^n$, the system

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

has a solution $x \in R$ if and only if $B(t)$ 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 $m := \max(\deg f_i, i = 1, \ldots, s)$. Then $N \leq sm$. Set $I_k := [x_k, x_{k+1}]$, $k = 0, \ldots, N$

**Remark 2.** $\text{sign}(f_i(x))$ is constant on $I_k$, for each $i \in 1, \ldots, s$, for each $k \in 0, \ldots, N$. 
Set $\text{sign}(f_i(I_k)) := \text{sign}(f_i(x)), \ x \in I_k$

**Notation II.** Let $\text{SIGN}_R(f_1, \ldots, f_s)$ be the matrix with $s$ rows and $2N + 1$ columns whose $i^{th}$ row (for $i = \{1, \ldots, s\}$) is $\text{sign}(f_i(I_0)), \text{sign}(f_i(x_1)), \text{sign}(f_i(I_1)), \ldots, \text{sign}(f_i(x_N)), \text{sign}(f_i(I_N))$.

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

$$
\text{SIGN}_R(f_1, \ldots, f_s) := \\
\begin{pmatrix}
\text{sign}f_1(I_0) & \text{sign}f_1(x_1) & \ldots & \text{sign}f_1(x_N) & \text{sign}f_1(I_N) \\
\text{sign}f_2(I_0) & \text{sign}f_2(x_1) & \ldots & \text{sign}f_2(x_N) & \text{sign}f_2(I_N) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
\text{sign}f_s(I_0) & \text{sign}f_s(x_1) & \ldots & \text{sign}f_s(x_N) & \text{sign}f_s(I_N)
\end{pmatrix}
$$

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

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

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

**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 $\epsilon : \{1, \ldots, s\} \rightarrow \{-1, 0, +1\}$. Set

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

\[
\begin{align*}
\text{sign}(f_1(X)) &= \epsilon(1) \\
& \vdots \\
\text{sign}(f_s(X)) &= \epsilon(s)
\end{align*}
\]

has a solution \( x \in R \) if and only if \( \text{SIGN}_R(f_1, \ldots, f_s) \in W(\epsilon) \).

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 \( f_i(T, X) := h_{i,m_i}(T)X^{m_i} + \ldots + h_{i,0}(T) \) 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 \( B(T) = S_1(T) \lor \ldots \lor S_p(T) \) of polynomial equations and inequalities in the variables \( T \) with coefficients in \( \mathbb{Z} \), such that, for every real closed field \( R \) and every \( t \in R^n \), we have

\[
\text{SIGN}_R(f_1(t, X), \ldots, f_s(t, X)) \in W' \iff B(t) \text{ holds true in } R.
\]

The proof of the main Proposition will follow by induction from the next main lemma, where we will show that \( \text{SIGN}_R(f_1, \ldots, f_s) \) is completely determined by the “\( \text{SIGN}_R \)” of a (possibly) longer but simpler sequence of polynomials, i.e. \( \text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s) \), 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.

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 $\text{SIGN}_R(f_1, \ldots, f_{s}) \in W_{s,m}$ is completely determined by $\text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s) \in W_{2s,m}$, 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 $\varphi : W_{2s,m} \longrightarrow W_{s,m}$

$$\text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s) \longrightarrow \text{SIGN}_R(f_1, \ldots, f_{s})$$

is well defined.

In other words, for any $(f_1, \ldots, f_s), (F_1, \ldots, F_s) \in R[X]$

$$\text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s) = \text{SIGN}_R(F_1, \ldots, F_{s-1}, F'_s, G_1, \ldots, G_s)$$

$$\Rightarrow \text{SIGN}_R(f_1, \ldots, f_{s}) = \text{SIGN}_R(F_1, \ldots, F_{s}).$$

Proof. Assume $w = \text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s)$ 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 $w$)

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

such that $f_s(x_{i_k}) = g_{\theta(k)}(x_{i_k})$

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

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

1
Proof of Claim I.

Case 1: $f_s$ has a root in $] - \infty, x_i [$. If $M \neq 0$, then $\text{sign}(f_s([ - \infty, x_1 [)) = 1$, equivalently $\text{sign}(f_s([ - \infty, x_1 [)) = sign f_s(x_i)$. 

$(\Rightarrow)$ We want to show that if $sign(f_s([ - \infty, x_1 [)) = sign f_s(x_i)$, then $f_s$ has a root in $] - \infty, x_i [$. 

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

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

Note that $sign f_s(x_i) \neq 0$ otherwise $f_s(x_i) = f(x_i) = 0$, so (by Rolle’s theorem) $f'_s$ has a root in $] x, x_i [$ and the only possibility is $x_1 \in ] x, x_i [$ (by our listing), but then $x_1 = x_i$, a contradiction]. 

Note also that $f_s$ cannot have two roots (counting multiplicity) in $] - \infty, x_i [$ [otherwise $f'_s$ will be forced to have a root in $] - \infty, x_i [$, a contradiction as before]. 

So $-sign f_s([ - \infty, x [) = sign f_s([ x, x_i ])) = sign f_s(x_i)$,

also (by same argument as before)

$-sign f_s([ - \infty, x [) = sign f'_s([ - \infty, x_1 [)$,

therefore, we get

$sign f'_s([ - \infty, x_1 [) = sign f_s(x_i)$.

\[ \square \text{ (case 1)} \]

Case 2: Similarly one proves that: $f_s$ has a root in $] x_i, + \infty [$ if and only if

$sign(f'_s([ x_N, + \infty [)) sign(g_{\theta(M)}(x_{iM})) = -1$, 

(i.e. if $sign f'_s([ x_N, + \infty [) = -sign f_s(x_{iM}) \neq 0$).

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

$sign(g_{\theta(k)}(x_{i_k})) sign(g_{\theta(k+1)}(x_{i_{k+1}})) = -1$, 

equivalently iff
\[ \text{sign} f_s(x_i) = -\text{sign} f_s(x_{i+1}). \]
(Proof is clear because if \( f_s \) has a root in \( x_i, x_{i+1} \], then this root is of multiplicity 1 and therefore a sign change must occur.)

Case 4: \( f_s \) has exactly one root in \( ]-\infty, +\infty[ \) if \( M = 0. \) \hfill \Box \text{ (claim I)}

Claim II. \( \text{SIGN}_R(f_1, \ldots, f_s) \) depends only on \( w. \)

Proof of Claim II.

Notation: Let \( y_1 < \ldots < y_L, \) with \( L \leq sm, \) be the roots in \( \mathbb{R} \) 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
\[
\rho : \{0, \ldots, L + 1\} \rightarrow \{0, \ldots, M + 1\} \cup \{(k, k+1) | k = 0, \ldots, M\}
\]
\[
l \mapsto \begin{cases} 
  k & \text{if } y_l = x_i, \\
  (k, k+1) & \text{if } y_l \in [x_i, x_{i+1}].
\end{cases}
\]

Note that by Claim I, \( L \) and \( \rho \) depends only on \( w. \) So, to prove claim II it is enough to show that \( \text{SIGN}_R(f_1, \ldots, f_s) \) depends only on \( \rho \) and \( w. \)

Also,
\[
\text{SIGN}_R(f_1, \ldots, f_s) := \begin{pmatrix}
  \text{sign} f_1(I_0) & \text{sign} f_1(y_1) & \text{sign} f_1(y_L) & \text{sign} f_1(I_L) \\
  \vdots & \vdots & \vdots & \vdots \\
  \text{sign} f_s(I_0) & \text{sign} f_s(y_1) & \text{sign} f_s(y_L) & \text{sign} f_s(I_L)
\end{pmatrix}
\]
is an \( s \times (2L + 1) \) matrix with coefficients in \( \{-1, 0, +1\}. \)

Case 1: \( j = 1, \ldots, s - 1 \)

For \( l \in \{0, \ldots, L + 1\} \) we have
\[
\begin{align*}
  & \text{• if } \rho(l) = k \Rightarrow \text{sign} (f_j(y_l)) = \text{sign} (f_j(x_i)), \\
  & \text{• if } \rho(l) = (k, k+1) \Rightarrow \text{sign} (f_j(y_l)) = \text{sign} (f_j(\, ]x_i, x_{i+1}[ \,)).
\end{align*}
\]

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

We also have
\[
\begin{align*}
  & \text{• if } \rho(l) = k \text{ or } (k, k+1) \Rightarrow \text{sign} (f_j(\, ]y_l, y_{l+1}[ \,)) = \text{sign} (f_j(\, ]x_i, x_{i+1}[ \,)).
\end{align*}
\]
So, \( \text{sign}(f_j(\lfloor y_l, y_{l+1} \rceil)) \) is known from \( w \) and \( \rho \), for all \( j = 1, \ldots, s - 1 \) and \( l \in \{0, \ldots, L + 1\} \).

Thus one can reconstruct the first \( s - 1 \) rows of \( \text{SIGN}_R(f_1, \ldots, f_s) \) from \( w \).

Case 2: \( j = s \)

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

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

So, \( \text{sign}(f_s(y_l)) \) is known from \( w \) and \( \rho \), for all \( l \in \{0, \ldots, L + 1\} \) and therefore can also be reconstructed from \( w \).

Now remains the most delicate case that concerns \( \text{sign}(f_s(\lfloor y_l, y_{l+1} \rceil)) \):

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

- if \( l \neq 0 \), \( \rho(l) = k \Rightarrow \text{sign}(f_s(\lfloor y_l, y_{l+1} \rceil)) = \begin{cases} \text{sign}(g_{\theta(k)}(x_{i_k})) & \text{if it is } \neq 0, \\ \text{sign}(f'_s(\lfloor x_{i_k}, x_{i_k+1} \rceil)) & \text{otherwise.} \end{cases} \]

This is because \( \rho(l) = k \) if \( y_l = x_{i_k} \), so:

- if \( g_{\theta(k)}(x_{i_k}) = f_s(x_{i_k}) \neq 0 \), then by continuity \( \text{sign} \) is constant, and
- if \( g_{\theta(k)}(x_{i_k}) = f_s(x_{i_k}) = 0 \), then on \( [x_{i_k}, x_{i_k+1}[ \):

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

(using 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 \( P(a) < P(b) \)).

- if \( l \neq 0 \), \( \rho(l) = (k, k + 1) \Rightarrow \text{sign}(f_s(\lfloor y_l, y_{l+1} \rceil)) = \text{sign}(f'_s(\lfloor x_{i_k}, x_{i_k+1} \rceil)) \).

We argue as follows (noting that \( \rho(l) = (k, k + 1) \) if \( y_l \in ]x_{i_k}, x_{i_k+1}[ \)):

\( \text{sign}(f_s(\lfloor y_l, y_{l+1} \rceil)) \) is constant so at any rate is equal to \( \text{sign}(f_s(\lfloor y_l, x_{i_k+1} \rceil)) \),

now using the fact that \( f_s(y_l) = 0 \) and the same lemma (stated above) we get, for any \( a \in ]y_l, x_{i_k+1}[ \):

\[
\begin{cases}
  f'_s \geq 0 \Rightarrow f_s(y_l) < f_s(a), & \text{so } f_s(a) > 0, \\
  f'_s \leq 0 \Rightarrow -f_s(y_l) < -f_s(a), & \text{so } f_s(a) < 0
\end{cases}
\]

i.e. \( f_s \) has same sign as \( f'_s \).

- if \( l = 0 \Rightarrow \text{sign}(f_s(\lfloor -\infty, y_1 \rceil)) = \text{sign}(f'_s(\lfloor -\infty, x_1 \rceil)) \) (as before). □
REAL ALGEBRAIC GEOMETRY LECTURE NOTES  
(14: 03/12/2009)  

SALMA KUHLMANN  

THE TARSKI-SEIDENBERG PRINCIPLE  

Main Proposition. Let $f_i(T, X) := h_{i,m_i}(T)X^{m_i} + \ldots + h_{i,0}(T)$ 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 $B(T) = S_1(T) \lor \ldots \lor S_p(T)$ of polynomial equations and inequalities in the variables $T$ with coefficients in $\mathbb{Z}$, such that, for every real closed field $\mathbb{R}$ and every $t \in \mathbb{R}^n$, we have  

$$\text{SIGN}_R(f_1(t, X), \ldots, f_s(t, X)) \in W' \iff B(t) \text{ holds true in } \mathbb{R}.$$  

Proof. Without loss of generality, we assume that none of $f_1, \ldots, f_s$ is identically zero and that $h_{i,m_i}(T)$ 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 $\sigma$ = the number of times $q$ appears in $\tau$,  

and  

- the number of times $p$ appears in $\sigma$ < the number of times $q$ appears in $\tau$.  

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

[Example: let $m = \max\{m_1, \ldots, m_s\} = m_s$ (say), $\sigma$ and $\tau$ 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.  

$$\sigma \sim (f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s),$$  

$$\tau \sim (f_1, \ldots, f_{s-1}, f_s)$$  

$^1$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 $\sigma < \tau$.

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

In particular using $p = m$ we have:

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

If $m = 0$, then there is nothing to show, since $\text{SIGN}_R(f_1(t, X), \ldots, f_s(t, X)) = \text{SIGN}_R(h_{1,0}(t), \ldots, h_{s,0}(t))$ [the list of signs of “constant terms”].

Suppose that $m \geq 1$ 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 $\varphi$ (as in main lemma). Set $W'' = \{\text{SIGN}_R(f_1, \ldots, f_{s-1}, f'_s, g_1, \ldots, g_s) \mid \text{SIGN}_R(f_1, \ldots, f_s) \in W'\}$.

- **Case 1.** $h_{i,m_i}(t) \neq 0$ for all $i = 1, \ldots, s$

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

$$\text{SIGN}_R(f_1(t, X), \ldots, f_s(t, X)) \in W' \iff \text{SIGN}_R(f_1(t, X), \ldots, f_{s-1}(t, X), f'_s(t, X), g_1(t, X), \ldots, g_s(t, X)) \in W'',$$

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

Set $M := N/\sim$
Note that if $\sigma', \tau'$ are permutations of $\sigma$ and $\tau$, 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 \( p_1, p_2 \in N \) such that \( P(p_1, \rho, \sigma) \) and \( P(p_2, \sigma, \tau) \) 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 inequality is strict, which leads to the same conclusion.

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

\( \Box \)

**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 \( A = \emptyset \) if and only if \( \sigma \sim \tau \), so by hypothesis we have \( A \neq \emptyset \). Thus, we can define \( p := \max A \).

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 \( P(p, \sigma, \tau) \) is satisfied, so \([\sigma] < [\tau]\); if \( f_p(\tau) < f_p(\sigma) \), then \( P(p, \tau, \sigma) \) is satisfied, so \([\tau] < [\sigma]\).

\( \Box \)

Note that we have an algorithm which determines how to order the pair \((\sigma, \tau)\) and gives us an appropriate \( p \):

\[
\begin{align*}
p &:= \max\{n_1, \ldots, n_s, m_1, \ldots, m_t\}. \\
\text{while } p \geq 0: \\
& \quad \text{if } f_p(\sigma) > f_p(\tau) \text{ return } (\sigma > \tau, p) \\
& \quad \text{if } f_p(\sigma) < f_p(\tau) \text{ return } (\sigma < \tau, p) \\
& \quad p := p - 1
\end{align*}
\]

**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 \( m_\sigma \) is left unchanged by permutation of \( \sigma \), 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, \( f_m(a) = 0 < f_m(b) \), 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 $A_0 := \{[\sigma] \in A \mid \sigma \text{ only contains zeros}\}$ 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 $f_0(a) = \text{length}(a) < \text{length}(b) = f_0(b)$. This proves that $\mathcal{P}(0, a, b)$ holds, hence $a < b$.
If $b \in A \setminus A_0$, then $m_b > 0 = m_a$ so $b > a$.

$m-1 \rightarrow m$: 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 $a \in A \setminus C$, $c < a$.
Indeed:

- if $a \in B \setminus C$, 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:

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

**Proposition 4**
The ordinal type of \((M, <)\) is \( \omega^\omega \)

*Proof.* For any \( n \in \mathbb{N} \), set \( A_n := \{ a \in M \mid m_a = n \} \).
We are going to build an isomorphism from \( \omega^\omega \) 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 \( n \in \mathbb{N} \), \( \phi_n \) is an isomorphism from \( \omega^{n+1} \) to \( A_n \).
- for any \( n \in \mathbb{N} \), \( \phi_{n+1} \) extends \( \phi_n \).

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

\[ n = 0 \quad \text{Note that we have } (0) < (0, 0) < (0, 0, 0) < (0, 0, 0, 0) < \ldots, \text{ so an isomorphism from } \omega \text{ to } A_0 \text{ is given by } n \mapsto (0, 0, \ldots, 0) \]\n\[ n \to n + 1 \quad \text{Assume we have an isomorphism } \phi_n : \omega^{n+1} \to A_n. \text{ Remember that } \omega^{n+2} \text{ is the order type of } (\omega \times \omega^{n+1}, <_{\text{lex}}). \]
Define: \( \phi_{n+1}(\alpha, \beta) := \phi_n(\beta) \wedge (n + 1, \ldots, n + 1) \) \( \alpha \) times
(here ‘\( \wedge \)’ means concatenation). This is an isomorphism from \( (\omega \times \omega^{n+1}, <_{\text{lex}}) \) to \( A_{n+1} \).

\( \square \)
POSITIVE POLYNOMIALS LECTURE NOTES
(01: 13/04/10)

SALMA KUHLMANN

Contents

1. The polynomial ring $\mathbb{R}[X]$ 1
2. Borel measure 2
3. Preordering 2

1. THE POLYNOMIAL RING $\mathbb{R}[X]$

**Notation 1.1.** $\mathbb{R}[X] := \mathbb{R}[X_1, \ldots, X_n]$ is the polynomial ring in $n$ variables and real coefficients, where $\mathbb{R}$ is the set of real numbers.

Note that $\mathbb{R}[X]$ is a vector space of countable dimension (a basis is $\{X^\alpha \mid \alpha \in \mathbb{Z}_+^n\}$, where $X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is a monomial).

**Definition 1.2.** A polynomial is said to be **homogenous** if it is a linear combination of monomials with same degree (or zero polynomial).

**Convention:** $\deg(0) := -\infty$, where “0” is the polynomial with 0 coefficients.

**Definition 1.3.** Let $f \in \mathbb{R}[x]$, the **homogenous decomposition** of $f$ is $f = h_0 + \ldots + h_d$, where $h_i$ are homogenous (or 0) and $\deg(h_i) = i$ if $h_i \neq 0$.

Note that if $h_d \neq 0$, then $d = \deg(h_d) = \deg(f)$.

**Remark 1.4.** Let $f, g \in \mathbb{R}[x]$; $f \neq 0, g \neq 0$, then:

(i) $\deg(fg) = \deg(f) + \deg(g)$

(ii) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$

(iii) $\deg(f + g) = \max\{\deg(f), \deg(g)\}$, if $\deg(f) \neq \deg(g)$. 
2. BOREL MEASURE

Definition 2.1. Let $X$ be a locally compact Hausdorff topological space (i.e. $\forall x \in X \exists U \ni x$ such that $\overline{U}$ is compact). A Borel measure $\mu$ on $X$ is a positive measure such that every $B \in \beta^c(X)$ is measurable, where $\beta^c(X) :=$ the smallest class of subsets of $X$ which contain all compact sets and is closed under finite unions, complements and countable intersections.

Further we will assume that $\mu$ is regular, i.e.
$\forall B \in \beta^c(X), \forall \epsilon > 0 \exists C, U \in \beta^c(X)$ with $C \subseteq B \subseteq U$, where $C$ is compact, $U$ is open and $\mu(C) + \epsilon \geq \mu(B) \geq \mu(U) - \epsilon$.

Definition 2.2. Let $K$ be a closed compact subset of $\mathbb{R}^n$. $K$ is said to be basic closed semi-algebraic if there exists a finite $S \subseteq \mathbb{R}[X]$, say $S = \{g_1, \ldots, g_s\}$ (for $s \in \mathbb{N}$) such that $K = K_S = \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \forall i = 1, \ldots, s\}$.

Notation 2.3. $\sum \mathbb{R}[X]^2 := \{\sigma = \sum_{i=1}^m f_i^2 \mid f_i \in \mathbb{R}[X], m \in \mathbb{N}\}$.

Theorem 2.4. (Schmüdgen’s Positivstellensatz) Let $K \subseteq \mathbb{R}^n$ be a compact semi-algebraic set, $K = K_S$ (as above). Let $L : \mathbb{R}[X] \rightarrow \mathbb{R}$ be a linear functional. Then $L$ can be represented by a positive Borel measure $\mu$ defined on $K$ (i.e. $L(f) = \int_K fd\mu$ for $f \in \mathbb{R}[X]$) if and only if $L(\sum g_i^{e_i} \ldots g_s^{e_s}) \geq 0 \forall \sigma \in \sum \mathbb{R}[X]^2$ and $e_1, \ldots, e_s \in \{0, 1\}$.

See Corollary 2.6 in lecture 13.

3. PREORDERING

Definition 3.1. Let $A$ be a commutative ring with 1,
$\Sigma A^2 := \{\sum a_i^2 \mid i \geq 0, a_i \in A\}$.

(1) A quadratic module $M$ in $A$ is a subset $M \subseteq A$ such that $M + M \subseteq M$, $a^2 M \subseteq M \forall a \in A, 1 \in M$.

(2) A preordering $T$ in $A$ is a quadratic module with $TT \subseteq T$.

$T$ is said to be proper if $-1 \notin T$. 
Remark 3.2. If $\frac{1}{2} \in A$ then $T = A$ is the only preordering in $A$ that is not proper.

Proof. For $a \in A$ one can write: $a = (\frac{a+1}{2})^2 + (-1)(\frac{a-1}{2})^2 \in T$ \hfill $\square$

Examples 3.3.

(1) $\Sigma A^2 \subseteq T$ for a preordering $T$ in $A$.

(2) Let $S = \{g_1, \ldots, g_s\} \subseteq A$, then

$$T_S := \left\{ \sum_{e_1, \ldots, e_s \in \{0,1\}} \sigma_e g_1^{e_1} \cdots g_s^{e_s} \mid \sigma_e \in \Sigma A^2, e = (e_1, \ldots, e_s) \right\}$$

is the preordering generated by $g_1, \ldots, g_s$.

Definition 3.4. A preordering $T \subseteq A$ is said to be finitely generated if $\exists$ a finite $S \subseteq A$ with $T = T_S$.

For example: $\Sigma A^2$ is finitely generated with $S = \phi$.

Example 3.5. Let $S \subseteq A = \mathbb{R}[X]$ be a finite subset. We associate to $S$ the basic closed semi-algebraic subset $K_S \subseteq \mathbb{R}^n$ and the finitely generated preordering $T_S \subseteq \mathbb{R}[X]$. We recall that $K_S := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \ \forall \ i = 1, \ldots, s\}, S = \{g_1, \ldots, g_s\}$.

For example: If $S = \phi : K_S = \mathbb{R}^n, T_S = \sum \mathbb{R}[X]^2$.

Definition 3.6. An element $f \in T_S$ is said to be positive semidefinite on $K_S$ if $f(x) \geq 0$ for all $x \in K_S$.

For $K \subseteq \mathbb{R}^n$, set $\text{Psd}(K) := \left\{ f \in \mathbb{R}[X] \mid f(x) \geq 0 \ \forall \ x \in K \right\}$

Note that $T_S \subseteq \text{Psd}(K_S)$.

Question. If $f \in \text{Psd}(K_S)$, then does $f \in T_S$?

Answer. No.

But there is a connection of $f$ with $T_S$ (which will become clear through the Positivstellensatz in the next lecture).
1. INTRODUCTION

Definition 1.1. For $K \subseteq \mathbb{R}^n$,

$$\text{Psd}(K) := \{ f \in \mathbb{R}[X] \mid f(x) \geq 0 \forall x \in K \}.$$ 

Let $S = \{ g_1, \ldots, g_s \} \subseteq \mathbb{R}[X]$, then

$$K_S := \{ x \in \mathbb{R}^n \mid g_i(x) \geq 0 \forall i = 1, \ldots, s \},$$

the basic closed semi-algebraic set defined by $S$ and

$$T_S := \left\{ \sum_{e_1, \ldots, e_s \in \{0,1\}} \sigma_{e_1} g_1^{e_1} \cdots g_s^{e_s} \mid \sigma_e \in \Sigma \mathbb{R}[X]^2, e = (e_1, \ldots, e_s) \right\},$$

the preordering generated by $S$.

We also introduce

$$M_S := \{ \sigma_0 + \sigma_1 g_1 + \sigma_2 g_2 + \cdots + \sigma_s g_s \mid \sigma_i \in \Sigma \mathbb{R}[X]^2 \},$$

the quadratic module generated by $S$.

Remark 1.2. (i) $M_S$ is a quadratic module in $\mathbb{R}[X]$.

(ii) $M_S \subseteq T_S \subseteq \text{Psd}(K_S)$.

(We shall study these inclusions in more detail later. In general these inclusions may be proper.)
Therefore by induction for \( n \geq 1 \), result follows since a nonzero polynomial \( f \in \mathbb{R}[X] \) has only finitely many zeroes.

Let \( n \geq 2 \) and \( 0 \neq f \in \mathbb{R}[X_1, \ldots, X_n] = \mathbb{R}[X_1, \ldots, X_{n-1}][X_n] \).

\[ f \neq 0 \Rightarrow f = g_0 + g_1X_n + \ldots + g_kX_n^k \]  
\( g_0, g_1, \ldots, g_k \in \mathbb{R}[X_1, \ldots, X_{n-1}]; \quad g_k \neq 0. \)

Since \( g_k \neq 0 \), so by induction on \( n \):

\[ \exists (x_1, x_2, \ldots, x_{n-1}) \text{ s.t. } g_k(x_1, x_2, \ldots, x_{n-1}) \neq 0. \]

\( \Rightarrow \) The polynomial in one variable \( X_n \) i.e. \( f(x_1, x_2, \ldots, x_{n-1}, X_n) \neq 0. \)

Therefore by induction for \( n = 1, \exists x_n \in \mathbb{R} \text{ s.t.} \)

\[ f(x_1, x_2, \ldots, x_{n-1}, x_n) \neq 0 \]

\( \square \)

**Remark 2.2.** If \( f \in \mathbb{R}[X], \; f \neq 0 \), then \( \mathbb{R}^n \setminus Z(f) = \{ x \in \mathbb{R}^n \mid f(x) \neq 0 \} \) is dense in \( \mathbb{R}^n \), where \( Z(f) := \{ x \in \mathbb{R}^n \mid f(x) = 0 \} \) is the zero set of \( f \).

Equivalently, \( Z(f) \) has empty interior. In other words, a polynomial which vanishes on a nonempty open set is identically the zero polynomial.

**Lemma 2.3.** Let \( \sigma := f_1^2 + \ldots + f_k^2 \); \( f_1, \ldots, f_k \in \mathbb{R}[X] \) and \( f_i \neq 0 \), then

(i) \( \sigma \neq 0 \)

(ii) \( \deg(\sigma) = 2 \max\{\deg f_i \mid i = 1, \ldots, k\} \)

[In particular \( \deg(\sigma) \) is even.]

**Proof.** (i) Since \( f_i \neq 0 \), so by lemma 2.1 \( \exists x \in \mathbb{R}^n \) s.t. \( f_i(x) \neq 0. \)

\[ \Rightarrow \sigma(x) = f_1(x)^2 + \ldots + f_k(x)^2 > 0 \]

\[ \Rightarrow \sigma \neq 0. \]

(ii) \( f_i = h_{i_0} + \ldots + h_{i_j}, \) where \( d = \max\{\deg f_i \mid i = 1, \ldots, k\} \); \( h_{i_j} \) homogeneous of degree \( j \) or \( h_{i_j} \equiv 0 \) for \( i = 1, \ldots, k. \)
Clearly \( \deg(\sigma) \leq 2d. \)

To show \( \deg(\sigma) = 2d \), consider the homogeneous polynomial
\[
h_{i_d}^2 + \ldots + h_{k_d}^2 := h_{2d}
\]

Note that if \( h_{2d} \neq 0 \), then \( \deg(h_{2d}) = 2d \) and \( h_{2d} \) is the homogeneous component of \( \sigma \) of highest degree (i.e. leading term), so \( \deg(\sigma) = 2d \).

Now we know that \( h_i^d \neq 0 \) for some \( i \in \{1, \ldots, k\} \), so by (i) we get \( h_{2d} \neq 0 \).

\[ \square \]

Now coming back to the inclusion: \( T_S \subseteq \text{Psd}(K_S) \)

**Example 2.4.(1)**

(i) \( S = \emptyset, n = 1 \Rightarrow K_S = \mathbb{R} \) and \( T_S = \sum \mathbb{R}[X]^2 \Rightarrow T_S = \text{Psd}(\mathbb{R}). \)

(ii) \( S = \{1 - X^2\}^3, n = 1 \Rightarrow K_S = [-1, 1] \) (compact),
\[
T_S = \left\{ \sigma_0 + \sigma_1(1 - X^2)^3 \mid \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2 \right\} = M_S.
\]

**Claim.** \( T_S \subseteq \text{Psd}(K_S) \)

For example: \( (1 - X^2) \in \text{Psd}([-1, 1]) \) (clearly),
but \( (1 - X^2) \notin T_S \), since if we assume for a contradiction that
\[
(1 - X^2) = \sigma_0 + \sigma_1(1 - X^2)^3,
\]
where \( \sigma_0 = \sum f_i^2 \). Then evaluating (1) at \( x = \pm 1 \) we get
\[
\sigma_0(\pm 1) = \sum f_i^2(\pm 1) = 0
\]
\[
\Rightarrow f_i(\pm 1) = 0
\]
\[
\Rightarrow f_i = (1 - X^2)g_i, \text{ for some } g_i \in \mathbb{R}[X]
\]
\[
\Rightarrow \sigma_0 = (1 - X^2)^2 \sum g_i^2
\]
Substituting \( \sigma_0 \) back in (1) we get
\[
1 = (1 - X^2)^2 \sum g_i^2 + (1 - X^2)^2 \sigma_1
\]
Evaluating (2) at \( x = \pm 1 \) yields 1 = 0, a contradiction.

(iii) \( S = \{X^3\}, n = 1 \Rightarrow K_S = [0, \infty) \) (noncompact),
\[
T_S = \left\{ \sigma_0 + \sigma_1X^3 \mid \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2 \right\} = M_S.
\]

**Claim.** \( T_S \subseteq \text{Psd}(K_S) \)

For example: \( X \in \text{Psd}(K_S) \), but \( X \notin T_S \) (we will use degree argument to show this).

We compute the possible degrees of elements \( t \in T_S; t \neq 0 \)
Let
\[
t = \sigma_0 + \sigma_1X^3; \sigma_0, \sigma_1 \in \sum \mathbb{R}[X]^2,
\]
then

- \( \sigma_0 \neq 0 \Rightarrow \deg(\sigma_0) \) is even.
- \( \sigma_1 \neq 0 \Rightarrow \deg(\sigma_1) \) is even.
- \( \sigma_0 \equiv 0 \Rightarrow \deg(t) \) is odd and \( \geq 3 \).
- \( \sigma_1 \equiv 0 \Rightarrow \deg(t) \) is even.
- \( \sigma_0 \neq 0, \sigma_1 \neq 0 \), then

\[
\text{even } = \deg(\sigma_0) \neq \deg(\sigma_1 x^3) \quad \text{[= odd]}
\]

So, \( \deg(t) = \max \{ \deg(\sigma_0), \deg(\sigma_1 x^3) \} \) is even or odd \( \geq 3 \).

This proves that \( X \not\in T_S \) and hence \( T_S \subseteq \text{Psd}(K_S) \).

\( \Box \)

Example 2.4.2) \( S = \phi, n = 2 \Rightarrow K_S = \mathbb{R}^2 \) and \( T_S = M_S = \sum \mathbb{R}[X, Y]^2 \).

We see that \( T_S \subseteq \text{Psd}(K_S) \)

For example: \( m(X, Y) := X^2 Y^4 + X^4 Y^2 - 3 X^2 Y^2 + 1 \in \text{Psd}(\mathbb{R}^2) \), but \( \notin T_S = \sum \mathbb{R}[X, Y]^2 \).

3. POSITIVSTELLENSATZ (Geometric Version)

Theorem 3.1. (Positivstellensatz: Geometric Version) Let \( A = \mathbb{R}[X] \). Let \( S = \{ g_1, \ldots, g_s \} \subseteq \mathbb{R}[X] \), \( K_S, T_S \) as defined above, \( f \in \mathbb{R}[X] \). Then

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

2. \( f \geq 0 \) on \( K_S \Leftrightarrow \exists \ m \in \mathbb{Z}_+, \exists \ p, q \in T_S \text{ s.t. } pf = f^{2^m} + q \)

3. \( f = 0 \) on \( K_S \Leftrightarrow \exists \ m \in \mathbb{Z}_+ \text{ s.t. } -f^{2^m} \in T_S \)

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

Important corollaries to the PSS are:

(i) The real Nullstellensatz

(ii) Hilbert’s 17th problem

(iii) Abstract Positivstellensatz

The proof of the PSS consists of two parts:
- Step I: prove that (1) \( \Rightarrow \) (2) \( \Rightarrow \) (3) \( \Rightarrow \) (4) \( \Rightarrow \) (1)
- Step II: prove (4) [using Tarski Transfer]
We shall start the proof with step II:
Clearly $K_S \neq \phi \Rightarrow -1 \notin T_S$ (since $-1 \in T_S \Rightarrow K_S = \phi$), so it only remains to prove the following proposition:

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

For proving this we need to recall some definitions and results:

**Definition 3.3.1.** Let $A$ be a commutative ring with 1, a preordering $P \subseteq A$ is said to be an ordering on $A$ if $P \cup -P = A$ and $p := P \cap -P$ is a prime (hence proper) ideal of $A$.

**Definition 3.3.2.** Let $P$ be an ordering in $A$, then Support$P := p$ (the prime ideal $P \cap -P$).

**Lemma 3.4.1.** Let $A$ be a commutative ring with 1. Let $P$ be a maximal proper preordering in $A$. Then $P$ is an ordering.

**Lemma 3.4.2.** Let $A$ be a commutative ring with 1 and $P \subseteq A$ an ordering. Then $P$ induces uniquely an ordering on $F := f f(A/p)$ defined by:

$$\forall a, b \in A, \quad \frac{a}{b} \geq_0 0 \text{ (in } F) \iff ab \in P,$$

where $\bar{a} = a + p$. 
1. Geometric version of Positivstellensatz

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

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

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

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

4. $K_S = \emptyset \iff -1 \in T_S$.

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

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

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

1
For proving this we need the following results:

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

**Proof.** We have to show:

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

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

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

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

Thus

$-1 = s_1 + at_1$ and

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

So (rewritting)

$-at_1 = 1 + s_1$ and

$at_2 = 1 + s_2$

Multiplying we get:

$-a^2t_1t_2 = 1 + s_1 + s_2 + s_1s_2$

$\Rightarrow -1 = s_1 + s_2 + s_1s_2 + a^2t_1t_2 \in P$, a contradiction.

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

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

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

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

Then as above in (i), we get:

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

So, $-1 = s_1 + at_1$ and

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

Rearranging and multiplying we get:

$(at_1)(bt_2) = (1 + s_1)(1 + s_2) = 1 + s_1 + s_2 + s_1s_2$

$\Rightarrow -1 = s_1 + s_2 + s_1s_2 + abt_1t_2$

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

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

$\forall a, b \in A, b \notin \mathfrak{p} : \frac{\overline{a}}{b} \geq_P 0$ (in $F$) $\iff ab \in P$, where $\overline{a} = a + \mathfrak{p}$. $\square$
Recall 1.3.3. (Tarski Transfer Principle) Suppose \((\mathbb{R}, \leq) \subseteq (F, \leq)\) is an ordered field extension of \(\mathbb{R}\). If \(x \in F^n\) satisfies a finite system of polynomial equations and inequalities with coefficients in \(\mathbb{R}\), then \(\exists r \in \mathbb{R}^n\) satisfying the same system. \(\square\)

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

Proof of Proposition 1.2. To show: \(-1 \not\in T_S \Rightarrow K_S \neq \phi\).

Set \(S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]\)

\(-1 \not\in T_S \Rightarrow T_S\) is a proper preordering.
By Zorn, extend \(T_S\) to a maximal proper preordering \(P\).
By lemma 1.3.1, \(P\) is an ordering on \(\mathbb{R}[X]_p\); \(p := P \cap -P\) is prime.
By lemma 1.3.2, let \((F, \leq_P) = (f f(\mathbb{R}[X]_p), \leq_P)\) is an ordered field extension of \((\mathbb{R}, \leq)\).

Now consider the system \(S := \{g_1 \geq 0 \}\)

\(\vdots\)

\(g_s \geq 0\).

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

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

Now apply TTP (recall 1.3.3) to conclude that:
\(\exists r \in \mathbb{R}^n\) satisfying the system \(S\), i.e. \(g_i(x) \geq 0\) : \(i = 1, \ldots, s\).
\(\Rightarrow r \in K_S \Rightarrow K_S \neq \phi\).
This completes step II. \(\square\)

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

\((1) \Rightarrow (2)\)

Let \(f \geq 0\) on \(K_S\), \(f \neq 0\).
Consider \(S' \subseteq \mathbb{R}[X, Y]\), \(S' := S \cup \{Yf - 1, -Yf + 1\}\)
So, \(K_{S'} = \{ (x, y) \mid g_i(x) \geq 0 ; yf(x) = 1 \}\).
Thus \( f(X, Y) = f(X) > 0 \) on \( K_S \), so applying (1) \( \exists p', q' \in T_S \) s.t.

\[
p'(X, Y) f(X) = 1 + q'(X, Y)
\]

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

\[
p(X) f(X) = f(X)^{2m} + q(X),
\]

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

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

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

Observe that \( p'(X, Y) \in T_S \), so \( p' \) is a sum of terms of the form:

\[
s(X, Y) g_1^{e_1} \ldots g_s^{e_s} \left( Yf(X) - 1 \right)^{e_{s+1}} \left( -Yf(X) + 1 \right)^{e_{s+2}} ; e_1, \ldots, e_s, e_{s+1}, e_{s+2} \in \{0, 1\}
\]

say \( s(X, Y) = \sum_j h_j(X, Y)^2 \).

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

So, the remaining terms are of the form

\[
s'(X, Y) g_1^{e_1} \ldots g_s^{e_s} \left( \sum_j h_j(X, \frac{1}{f(X)}) \right)^2 g_1^{e_1} \ldots g_s^{e_s}
\]

So, we want to choose \( m \) large enough so that \( f(X)^{2m} s'(X, \frac{1}{f(X)}) \in \Sigma R[X]^2 \).

Write \( h_j(X, Y) = \sum_i h_{j,i}(X) Y^i \)

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

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

\[
f(X)^m h_j(X, \frac{1}{f(X)}) = \sum_i h_{j,i}(X) f(X)^{m-i}, \text{ with } (m - i) \geq 0 \forall i
\]

so that \( f(X)^m h_j(X, \frac{1}{f(X)}) \in \mathbb{R}[X] \), for all \( j \).
So \( f(X)^2m \sigma(X, \frac{1}{f(X)}) = f(X)^2m \left( \sum_j \left[ h_j(X, \frac{1}{f(X)}) \right]^2 \right) \)

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

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

(2) \( \Rightarrow \) (3)

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

\[ p_1 f = f^{2m_1} + q_1 \quad \text{and} \quad -p_2 f = f^{2m_2} + q_2 \]

where \( p_1, p_2, q_1, q_2 \in T_S \), \( m_i \in \mathbb{Z}_+ \)

Multiplying yields:

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

\[ \Rightarrow -f^{2m} = \sum_{T_S} p_1 p_2 f^2 + f^{2m_1} q_2 + f^{2m_2} q_1 + q_1 q_2 \]

i.e. \(-f^{2m} \in T_S \), \( m \in \mathbb{Z}_+ \)

(3) \( \Rightarrow \) (4)

Assume \( K_S = \phi \)

\[ \Rightarrow \] the constant polynomial \( f(X) \equiv 1 \) vanishes on \( K_S \).

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

(4) \( \Rightarrow \) (1)

Let \( S' = S \cup \{-f\} \)

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

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

\[ \Rightarrow -1 = q - pf \quad \text{for some } p, q \in T_S \]

i.e. \( pf = 1 + q \)

This completes step I and hence the proof of Positivstellensatz.

We will now study other forms of the Real Nullstellensatz that will relate it to Hilbert’s Nullstellensatz.
2. EXKURS IN COMMUTATIVE ALGEBRA

Recall 2.1. Let $K$ be a field, $S \subseteq K[X]$. Define
\[ Z(S) := \{ x \in K^n \mid g(x) = 0 \ \forall g \in S \} \text{, the zero set of } S. \]

Proposition 2.2. Let $V \subseteq K^n$. Then the following are equivalent:
1. $V = Z(S)$; for some finite $S \subseteq K[X]$
2. $V = Z(S)$; for some set $S \subseteq K[X]$
3. $V = Z(I)$; for some ideal $I \subseteq K[X]$

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

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

(3) $\implies$ (1) Using Hilbert Basis Theorem (i.e. for a field $K$, every ideal in $K[X]$ is finitely generated):
\[ I = <S>, S \text{ finite} \implies Z(I) = Z(S). \]

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

Definition 2.4. Given a subset $A \subseteq K^n$, we form:
\[ I(A) := \{ f \in K[X] \mid f(a) = 0 \ \forall a \in A \}. \]

Proposition 2.5. Let $A \subseteq K^n$. Then
1. $I(A)$ is an ideal called the ideal of vanishing polynomials on $A$.
2. If $A = V$ is an algebraic set in $K^n$, then $Z(I(V)) = V$
3. the map $V \mapsto I(V)$ is a 1-1 map from the set of algebraic sets in $K^n$ into the set of ideals of $K[X]$. \hfill $\square$

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

Proof. Say (by Hilbert Basis Theorem) $I = <g_1, \ldots, g_s> \subseteq K[X]$. Then
\[ Z(I) = \{ x \in K^n \mid g_i(x) = 0 \ \forall i = 1, \ldots, s \}. \]
\[ I(\mathcal{Z}(I)) = \{ f \in K[X] \mid f(x) = 0 \ \forall \ x \in \mathcal{Z}(I) \}. \]

Assume \( f = h_1g_1 + \ldots + h_sg_s \in I \), then \( f(x) = 0 \ \forall \ x \in \mathcal{Z}(I) \)

[since by definition \( x \in \mathcal{Z}(I) \Rightarrow g_i(x) = 0 \ \forall \ i = 1, \ldots, s \)]

\[ \Rightarrow f \in I(\mathcal{Z}(I)). \]

But in general it is false that \( I(\mathcal{Z}(I)) = I \). Hilbert’s Nullstellensatz studies necessary and sufficient conditions on \( K \) and \( I \) so that this identity holds.
1. Exkurs in commutative algebra (continued) 1
2. Radical ideals and Real ideals 2
3. The Real Spectrum 5

1. EXKURS IN COMMUTATIVE ALGEBRA

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

is always true.

But in general it is false that

\[ I(\mathcal{Z}(I)) = I \]

Note 1.2. In other words we study the map

\[ I : \{ \text{algebraic sets in } K^n \} \rightarrow \{ \text{Ideals of } K[X] \} \]

\[ V \mapsto I(V) \]

• Clearly this map is 1-1 (proposition 2.5 of last lecture).

• What is the image of \( I \)?

Let \( I \) an ideal, \( I = I(V) \)

\[ \Rightarrow \mathcal{Z}(I) = \mathcal{Z}(I(V)) = V \]

(prop. 2.5 of last lecture)

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

So studying the equality (1) amounts to studying (2).
2. RADICAL IDEALS AND REAL IDEALS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Let $k$ (big enough) s.t. $2^k \geq m$, then
Now we show by induction on $k$ that:

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

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

$a^{2k+1} = (a^{2k})^2 \in I \quad \Rightarrow \quad a^{2k} \in I \quad \Rightarrow \quad a \in I$. 

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

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

$\Rightarrow (a^m)^2 + \sigma \in I \quad \Rightarrow \quad a^m \in I \quad \Rightarrow \quad a \in I$. $\square$

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

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

**Proposition 2.8.** Let $p \subseteq A$ be a prime ideal. Then $p$ is real $\iff$ $f f(A/p)$ is a real field.

**Proof.** $p$ is not real

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

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

$\iff f f(A/p)$ is not real. $\square$

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

(1) (Hilbert’s Nullstellensatz) Assume $K$ is algebraically closed, then $\overline{I(Z(I))} = \sqrt{I}$.

(Proved in B5)

(2) (Real Nullstellensatz) Assume $K$ is real closed, then
\[ I(\mathcal{Z}(I)) = \sqrt{I}. \]
(Will be deduced from Positivstellensatz)

**Corollary 2.10.** Consider the map:

\[ I : \{ \text{algebraic sets in } K^n \} \rightarrow \{ \text{ideals of } K[X] \} \]

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

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

□

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

We need the following 2 (helping) lemmas:

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

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

2. The following are equivalent for \( a \in A \):
   
   (i) \( a \in \sqrt{M \cap (-M)} \)
   
   (ii) \( a^{2m} \in M \cap (-M) \) for some \( m \in \mathbb{N}, m \geq 1 \)
   
   (iii) \( -a^{2m} \in M \) for some \( m \in \mathbb{N}, m \geq 1 \).

□

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

□

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

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

\[ I(K_S) = \sqrt{T_S \cap (-T_S)}. \]
Proof. \( f = 0 \) on \( K_S \iff -f^{2m} \in T_S \) for some \( m \in \mathbb{Z}_+ \)
(by (3) of PSS)
\( \iff f \in \sqrt{T_S \cap (-T_S)} \) (by lemma 2.11) \( \square \)

Corollary 2.15. (to Lemma 2.11 and 2.12) Let \( A \) be a commutative ring with 1. Let \( I \) be an ideal of \( A \). Consider the preordering \( T := \Sigma A^2 + I \), then
\( \sqrt[\circ]{I} = \sqrt{T \cap (-T)} \).
\( \square \)

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

Proof of RNSS [Theorem 2.9 (2)]. Let \( I \) be an ideal of \( \mathbb{R}[X] \)
We show that: \( I(\mathbb{Z}(I)) = \sqrt[\circ]{I} \)
\( \mathbb{R}[X] \) Noetherian \( \Rightarrow I = (h_1, \ldots, h_t) \) (by Hilbert Basis Theorem).
Consider \( S := \{\pm h_i \mid i = 1, \ldots, t \} \)
Then \( K_S = \mathbb{Z}(I) \) [clearly]
Now by Lemma 2.12, we have:
\( T = T_S = \Sigma \mathbb{R}[X]^2 + I \)
So we get,
\( I(\mathbb{Z}(I)) = I(K_S) = \sqrt{T \cap (-T)} = \sqrt[\circ]{I} \) (Cor 2.14)
(2.15) \( \square \)

3. THE REAL SPECTRUM

Definition 3.1. Let \( A \) be a commutative ring with 1. Then:
\( Spec(A) := \{p \mid p \text{ is prime ideal of } A \} \) is called the Spectrum of \( A \).
\( Spec_r(A) := \{ (p, \leq) \mid p \text{ is prime ideal of } A \text{ and } \leq \text{ is an ordering on the (formally real) field } ff(A/p) \} \) is called the Real Spectrum of \( A \).

Remark 3.2. (i) Several orderings may be defined on \( ff(A/p) \),
\( (p, \leq_1) \neq (p, \leq_2) \).
(ii) \((p, \leq) \in Sper(A) \Rightarrow p\) is real radical ideal. [see Proposition 2.8 and Remark 2.5 (i).]

**Note 3.3.** \(Sper(A) := \{\alpha = (p, \leq) \mid p\) is a real prime and \(\leq\) an ordering on \(f f(A/p)\}\).
Contents

1. The Real Spectrum 1
2. Topologies on $\mathcal{S}per(A)$ 2
3. Abstract Positivstellensatz 3

1. THE REAL SPECTRUM

Definition 1.1. Let $A$ be a commutative ring with 1. We set:

$$\mathcal{S}per(A) := \{ \alpha = (p, \leq) \mid p \text{ is a prime ideal of } A \text{ and } \leq \text{ is an ordering on } ff(A/p) \}.$$  

Note 1.2. $\mathcal{S}per(A) := \{ \alpha = (p, \leq) \mid p \text{ is a real prime and } \leq \text{ an ordering on } ff(A/p) \}.$

Definition 1.3. Let $\alpha = (p, \leq) \in \mathcal{S}per(A)$, then $p = \text{Supp}(\alpha)$, the Support of $\alpha$.

Recall 1.4. An ordering $P \subseteq A$ is a preorder with $P \cup -P = A$ and $p := P \cap -P$ prime ideal of $A$.

Definition 1.5. Alternatively, the Real Spectrum of $A$, $\mathcal{S}per(A)$ can be defined as:

$$\mathcal{S}per(A) := \{ P \mid P \subseteq A \text{, } P \text{ is an ordering of } A \}.$$  

Remark 1.6. The two definitions of $\mathcal{S}per(A)$ are equivalent in the following sense: The map

$$\varphi: \{ \text{Orderings in } A \} \sim \{ (p, \leq), p \text{ real prime, } \leq \text{ ordering on } ff(A/p) \}$$

$$P \mapsto p := P \cap -P, \leq, \text{ on } ff(A/p)$$
\[
\left( \text{where } \frac{\bar{a}}{b} \geq_P 0 \iff ab \in P \text{ with } \bar{a} = a + p \right)
\]
is bijective \[\varphi^{-1}(p, \leq) \text{ is } P := \{ a \in A \mid \bar{a} \geq 0 \}.\]

2. TOPOLOGIES ON \(\text{Sper}(A)\)

**Definition 2.1.** The **Spectral Topology** on \(\text{Sper}(A)\):
\(\text{Sper}(A)\) as a topological space, subbasis of open sets is:
\[\mathcal{U}(a) := \{ P \in \text{Sper}(A) \mid a \notin P \}, \ a \in A.\]
(\(\text{So a basis of open sets consists of finite intersection, i.e. of sets}\)
\[\mathcal{U}(a_1, \ldots, a_n) := \{ P \in \text{Sper}(A) \mid a_1, \ldots, a_n \notin P \}\]
Then close by arbitrary unions to get all open sets.
This is called **Spectral Topology**.

**Definition 2.2.** The **Constructible (or Patch) Topology** on \(\text{Sper}(A)\) is the topology that is generated by the open sets \(\mathcal{U}(a)\) and there complements \(\text{Sper}(A) \setminus \mathcal{U}(a)\), for \(a \in A\).
(\(\text{Subbasis for constructible topology is } \mathcal{U}(a), \text{Sper}(A) \setminus \mathcal{U}(a), \text{for } a \in A.\))

**Remark 2.3.** The constructible topology is finer than the Spectral Topology (i.e. more open sets).

**Special case:** \(A = \mathbb{R}[X]\)

**Proposition 2.4.** There is a natural embedding
\[P : \mathbb{R}^n \rightarrow \text{Sper}(\mathbb{R}[X])\]
given by
\[x \mapsto P_{\bar{x}} := \{ f \in \mathbb{R}[X] \mid f(x) \geq 0 \}.\]

**Proof.** The map \(P\) is well defined.

**Verify that** \(P_{\bar{x}}\) is indeed an ordering of \(A\).
Clearly it is a preordering, \(P_{\bar{x}} \cup -P_{\bar{x}} = \mathbb{R}[X]\).
\(p := P_{\bar{x}} \cap -P_{\bar{x}} = \{ f \in \mathbb{R}[X] \mid f(x) = 0 \}\) is actually a maximal ideal of \(\mathbb{R}[X]\),
since \(p = \ker (ev_{\bar{x}})\), the kernel of the evaluation map
\[ev_{\bar{x}} : \mathbb{R}[X] \rightarrow \mathbb{R}\]
\[f \mapsto f(x)\]
so, \( \mathbb{R}[X]/p \simeq \mathbb{R} \) (by first isomorphism theorem)

\[ \Rightarrow p \text{ maximal} \Rightarrow p \text{ is prime ideal.} \]

**Theorem 2.5.** \( \mathcal{P}(\mathbb{R}^n) \), the image of \( \mathbb{R}^n \) in \( \text{Sper}(\mathbb{R}[X]) \) is dense in \( \text{Sper}(\mathbb{R}[X]) \), Constructible Topology and hence in \( \text{Sper}(\mathbb{R}[X]) \), Spectral Topology. (i.e. \( \mathcal{P}(\mathbb{R}^n)_{\text{patch}} = \text{Sper}(\mathbb{R}[X]) \)).

**Proof.** By definition, a basic open set in \( \text{Sper}(\mathbb{R}[X]) \) has the form

\[ U = \{ P \in \text{Sper}(\mathbb{R}[X]) \mid f_i \notin P, g_j \in P; i = i, \ldots, s, j = 1, \ldots, t \}, \]

for some \( f_i, g_j \in \mathbb{R}[X] \).

Let \( P \in U \) (open neighbourhood of \( P \in \text{Sper}(\mathbb{R}[X]) \))

We want to show that: \( \exists y \in \mathbb{R}^n \) s.t. \( P_y \in U \)

Consider \( F = f f(\mathbb{R}[X]/p); p = \text{Supp}(P) = P \cap -P \) and \( \leq \) ordering on \( F \) induced by \( P \).

Then \( (F, \leq) \) is an ordered field extension of \( (\mathbb{R}, \leq) \).

Consider \( x = (x_1, \ldots, x_n) \in F^n \), where \( x_i = X_i + p \)

Then by definition of \( \leq \) we have (as in the proof of PSS):

\[ f_i(x) < 0 \text{ and } g_j(x) \geq 0 \; \forall i = i, \ldots, s, \; j = 1, \ldots, t. \]

By Tarski Transfer, \( \exists y \in \mathbb{R}^n \) s.t.

\[ f_i(y) < 0 \left( \Leftrightarrow f_i \notin P_y \right) \text{ and } g_j(y) \geq 0 \left( \Leftrightarrow g_j \in P_y \right) ; \; i = i, \ldots, s, \; j = 1, \ldots, t \]

\[ \Rightarrow P_y \in U \]
Notation 3.3. We write: $a > 0$ at $P$ if $a(P) = 1$
$a = 0$ at $P$ if $a(P) = 0$
$a < 0$ at $P$ if $a(P) = -1$

Note that (in this notation) $a \geq 0$ at $P$ iff $a \in P$.

Definition 3.4. Let $T \subseteq A$, then the Relative Spectrum of $A$ with respect to $T$ is

$$S_{per}^T(A) = \{ P \mid P \supseteq T; P \subseteq A \text{ is an ordering of } A \}.$$ 

Proposition 3.5. Let $T \subseteq A$ be a finitely generated preordering, say $T = T_S$; where $S = \{g_1, \ldots, g_s\} \subseteq A$. Then

$$S_{per}^T(A) = S_{per}^S(A) = \{ P \in Sper(A) \mid g_i(P) \geq 0 ; i = i, \ldots, s \} \quad \square$$

Remark 3.5. Let $T \subseteq A$

(i) $S_{per}^T(A)$ inherits the relative spectral (respectively constructible) topology.

(ii) In case $T = T_{\{g_1, \ldots, g_s\}}$ is a finitely generated preordering, then the proof of Theorem 2.5 goes through to give the following relative version for $S_{per}^T$:

Theorem 3.6. (Relative version of Theorem 2.5) Let $T = T_S$ = finitely generated preordering; $S = \{g_1, \ldots, g_s\}$. Let $K = K_S = \{ x \in \mathbb{R}^\alpha \mid g_i(x) \geq 0 \} \subseteq \mathbb{R}^\alpha$, a basic closed semi-algebraic set. Consider $(S_{per}^T, \text{Constructible Topology})$. Then

$$P : K \ni S_{per}^T(\mathbb{R}[X])$$

(defined as before)

$$x \mapsto P_x = \{ f \in \mathbb{R}[x] \mid f(x) \geq 0 \}$$

is well defined (i.e. $P_x \supseteq T \forall x \in K$).

Moreover $P(K)$ is dense in $(S_{per}^T(\mathbb{R}[X]), \text{Constructible Topology})$.

Proof. The proof is analogous to the proof of Theorem 2.5.
(Note the fact that $T$ is finitely generated is crucial here to be able to apply Tarski Transfer.) \square

Theorem 3.7. (Abstract Positivstellensatz) Let $A$ be a commutative ring, $T \subseteq A$ be a preordering of $A$ (not necessarily finitely generated). Then for $a \in A$:

1) $a > 0$ on $S_{per}^T(A) \iff \exists p, q \in T$ s.t. $pa = 1 + q$
(2) $a \geq 0$ on $\text{Sper}_T(A) \iff \exists p, q \in T, m \geq 0 \text{ s.t. } pa = a^{2m} + q$

(3) $a = 0$ on $\text{Sper}_T(A) \iff \exists m \geq 0 \text{ s.t. } -a^{2m} \in T$.

**Proof.** (1) Let $a > 0$ on $\text{Sper}_T(A)$. Suppose for a contradiction that there are no elements $p, q \in T$ s.t. $pa = 1 + q$ i.e. s.t. $-1 = q - pa$

i.e. $-1 \neq q - pa \forall p, q \in T$

Thus $-1 \notin T' := T - Ta$.

$\Rightarrow T'$ is a proper preordering.

So (by recall 3.1) $\exists P$ an ordering of $A$ with $T' \subseteq P$.

Now observe that $T \subseteq P$ i.e. $P \in \text{Sper}_T(A)$ but $-a \in P$ (i.e. $a(P) \leq 0$) i.e. $a \leq 0$

on $P$, a contradiction to the assumption. $\Box$

**Proposition 3.8.** Abstract Positivstellensatz $\Rightarrow$ Positivstellensatz.

**Proof.** $A = \mathbb{R}[X], T = T_S = T_{\{g_1, \ldots, g_l\}}, K = K_S$.

It suffices to show (2) of PSS [Theorem 1.1 of lecture 03 on 20/04/10], i.e. $f \geq 0$

on $K_S \iff \exists m \in \mathbb{Z}_+, \exists p, q \in T_S$ s.t. $pf = f^{2m} + q$.

Let $f \in \mathbb{R}[X]$ and $f \geq 0$ on $K_S$.

It suffices [by (2) of Theorem 3.7] to show that $f \geq 0$ on $\text{Sper}_T(\mathbb{R}[X])$:

If not then $\exists P \in \text{Sper}_T(\mathbb{R}[X])$ s.t. $f \notin P$

So, $P \in \mathcal{U}_T(f)$

(open neighbourhood of $P \in \text{Sper}_T(\mathbb{R}[X])$)

Now by [Theorem 3.6 i.e.] relative density of $\mathcal{P}(K)$ in $\text{Sper}_T(\mathbb{R}[X])$:

$\exists x \in K$ s.t. $P_x \in \mathcal{U}_T(f)$

$\Rightarrow f \notin P_x \Rightarrow f(x) < 0$, a contradiction to the assumption. $\Box$
POSITIVE POLYNOMIALS LECTURE NOTES
(06: 29/04/10)

SALMA KUHLMANN

Contents
1. Generalities about polynomials 1
2. PSD- and SOS- polynomials 2
3. Convex sets, cones and extremality 3

1. GENERALITIES ABOUT POLYNOMIALS

Definition 1.1. For a polynomial \( p \in \mathbb{R}[X_1, \ldots, X_n] \), we write
\[
p(X) = \sum_{i \in \mathbb{Z}_{\geq 0}^n} c_i \, X^i,
\]
where \( X^i = X_1^{i_1} \ldots X_n^{i_n} \) is a monomial of degree \( |i| = \sum_{k=1}^{n} i_k \) and \( c_i \, X^i \) is a term.

Definition 1.2. A polynomial \( p(X) \in \mathbb{R}[X] \) is called homogeneous or form if all terms in \( p \) have the same degree.

Notation 1.3. \( \mathcal{F}_{n,m} := \{ F \in \mathbb{R}[X_1, \ldots, X_n] \mid F \text{ is a form and } \deg(F) = m \} \), the set of all forms in \( n \) variables of degree \( m \) (also called set of \( n \)-ary \( m \)-ics forms), for \( n, m \in \mathbb{N} \).

Convention: \( 0 \in \mathcal{F}_{n,m} \).

Definition 1.4. Let \( p \in \mathbb{R}[X_1, \ldots, X_n] \) of degree \( m \). The homogenization of \( p \) w.r.t \( X_{n+1} \) is defined as
\[
p_h(x_1, \ldots, x_n, x_{n+1}) := x_m^{m+1} \, \frac{p(x_1, \ldots, x_n)}{x_{n+1}^{m+1}}, \ldots, \frac{x_n}{x_{n+1}^{m+1}}
\]
Note that \( p_h \) is a homogeneous polynomial of degree \( m \) and in \( n + 1 \) variables i.e. \( p_h \in \mathcal{F}_{n+1,m} \).

Proposition 1.5. (1) Let \( p(X) \in \mathbb{R}[X] \), \( \deg(p) = m \), then
number of monomials of \( p \leq \binom{m+n}{n} \)

(2) Let \( F(X) \in \mathcal{F}_{n,m} \), then

number of monomials of \( F \leq N := \binom{m+n-1}{n-1} \)

\[ \square \]

\textbf{Remark 1.6.} \( \mathcal{F}_{n,m} \) is a finite dimensional real vector space with \( \mathcal{F}_{n,m} = \mathbb{R}^N \).

2. PSD- AND SOS- POLYNOMIALS

\textbf{Definition 2.1.} (1) \( p(x) \in \mathbb{R}[X] \) is \textbf{positive semidefinite (psd)} if

\[ p(x) \geq 0 \ \forall \ x \in \mathbb{R}^n. \]

(2) \( p(x) \in \mathbb{R}[X] \) is \textbf{sum of squares (SOS)} if \( \exists \ p_i \in \mathbb{R}[X] \) s.t.

\[ p(x) = \sum_i p_i(x)^2. \]

\textbf{Notation 2.2.} \( \mathcal{P}_{n,m} := \) set of all forms \( F \in \mathcal{F}_{n,m} \) which are psd, and

\( \sum_{n,m} := \) set of all forms \( F \in \mathcal{F}_{n,m} \) which are sos.

\textbf{Lemma 2.3.} If a polynomial \( p \) is psd then \( p \) has even degree. \[ \square \]

\textbf{Remark 2.4.} From now on (using lemma 2.3) we will often write \( \mathcal{P}_{n,2d} \) and \( \sum_{n,2d} \).

\textbf{Lemma 2.5.} Let \( p \) be a homogeneous polynomial of degree \( 2d \), and \( p \) sos. Then

every sos representation of \( p \) consists of homogeneous polynomials only, i.e.

\[ p(x) = \sum_i p_i(x)^2 \Rightarrow p_i(x) \text{ homogenous of degree } d, \ i.e. \ p_i \in \mathcal{F}_{n,d}. \]

\[ \square \]

\textbf{Remark 2.6.} The properties of psd-ness and sos-ness are preserved under homogenization (see the following lemma).

\textbf{Lemma 2.7.} Let \( p(x) \) be a polynomial of degree \( m \). Then

(1) \( p \) is psd iff \( p_h \) is psd,

(2) \( p \) is sos iff \( p_h \) is sos. \[ \square \]

So we can focus our investigation of psdness of polynomials versus sosness of polynomials to those of forms, i.e. study and compare \( \sum_{n,m} \subseteq \mathcal{P}_{n,m} \).

\textbf{Theorem 2.8. (Hilbert)} \( \sum_{n,m} = \mathcal{P}_{n,m} \) iff
(i) $n = 2$ [i.e. binary forms] or
(ii) $m = 2$ [i.e. quadratic forms] or
(iii) $(n, m) = (3, 4)$ [i.e. ternary quartics].

For the ternary quartics case ($F_{3,4}$), we shall study the convex cones $P_{n,m}$ and $\sum_{n,m}$.

3. CONVEX SETS, CONES AND EXTREMALITY

Definition 3.1. A subset $C$ of $\mathbb{R}^n$ is convex if $a, b \in C \Rightarrow \lambda a + (1 - \lambda) b \in C$, for all $0 < \lambda < 1$.

Proposition 3.2. The intersection of an arbitrary collection of convex sets is convex.

Notation 3.3. $\mathbb{R}_+ := \{ x \in \mathbb{R} \mid x \geq 0 \}$.

Definition 3.4. Let $c_1, \ldots, c_k \in \mathbb{R}^n$. A convex combination of $c_1, \ldots, c_k$ is any vector sum

$$\alpha_1 c_1 + \ldots + \alpha_k c_k,$$

with $\alpha_1, \ldots, \alpha_k \in \mathbb{R}_+$ and $\sum_{i=1}^{k} \alpha_i = 1$.

Theorem 3.5. A subset $C \subseteq \mathbb{R}^n$ is convex if and only if it contains all the convex combinations of its elements.

Proof. ($\Rightarrow$) Let $C \subseteq \mathbb{R}^n$ be a convex set. By definition $C$ is closed under taking convex combinations with two summands. We show that it is also closed under finitely many summands.

Let $k > 2$. By Induction on $k$, assuming it true for fewer than $k$.

Given a convex combination $c = \alpha_1 c_1 + \ldots + \alpha_k c_k$, with $c_1, \ldots, c_k \in C$.

Note that we may assume $0 < \alpha_i < 1$ for $i = i, \ldots, k$; otherwise we have fewer than $k$ summands and we are done.

Consider $d = \frac{\alpha_2}{1 - \alpha_1} c_2 + \ldots + \frac{\alpha_k}{1 - \alpha_1} c_k$.

we have $\frac{\alpha_2}{1 - \alpha_1}, \ldots, \frac{\alpha_k}{1 - \alpha_1} > 0$ and $\frac{\alpha_2}{1 - \alpha_1} + \ldots + \frac{\alpha_k}{1 - \alpha_1} = 1$.

Thus $d$ is a convex combination of $k - 1$ elements of $C$ and $d \in C$ by induction.

Since $c = \alpha_1 c_1 + (1 - \alpha_1) d$, it follows that $c \in C$. \qed
Definition 3.6. The intersection of all convex sets containing a given subset $S \subseteq \mathbb{R}^n$ is called the convex hull of $S$ and is denoted by $\text{cvx}(S)$.

Remark 3.7. The convex hull of $S \subseteq \mathbb{R}^n$ is a convex set and is the uniquely defined smallest convex set containing $S$.

Theorem 3.8. For any $S \subseteq \mathbb{R}^n$, 
\[ \text{cvx}(S) = \{ \text{all convex combinations of the elements of } S \} \]

Proof. ($\supseteq$) The elements of $S$ belong to $\text{cvx}(S)$, so all their convex combinations belong to $\text{cvx}(S)$ by Theorem 3.5. 
($\subseteq$) On the other hand we observe that the set of convex combinations of elements of $S$ is itself a convex set: 
let $c = \alpha_1 c_1 + \ldots + \alpha_k c_k$ and $d = \beta_1 d_1 + \ldots + \beta_l d_l$, where $c_i, d_i \in S$, then 
$\lambda c + (1 - \lambda) d = \alpha_1 \lambda c_1 + \ldots + \alpha_k \lambda c_k + (1 - \lambda) \beta_1 d_1 + \ldots + (1 - \lambda) \beta_l d_l$, $0 \leq \lambda \leq 1$ is just another convex combination of elements of $S$. 
So by minimality property of $\text{cvx}(S)$, it follows that $\text{cvx}(S) \subseteq$ the set of all convex combinations of the elements of $S$.□

Corollary 3.9. The convex hull of a finite subset \{s_1, \ldots, s_k\} $\subseteq \mathbb{R}^n$ consists of all the vectors of the form $\alpha_1 s_1 + \ldots + \alpha_k s_k$ with $\alpha_1, \ldots, \alpha_k \geq 0$ and $\sum_i \alpha_i = 1$. □

Definitions 3.10. (1) A set which is the convex hull of a finite subset of $\mathbb{R}^n$ is called a convex polytope, i.e. $C \subseteq \mathbb{R}^n$ is a convex polytope if $C = \text{cvx}(S)$ for some finite $S \subseteq \mathbb{R}^n$.
(2) A point in a polytope is called a vertex if it is not on the line segment joining any other two distinct points of the polytope.

Remark 3.11. (1) Convex polytope is necessarily closed and bounded, i.e. compact.
(2) A convex polytope is always the convex hull of its vertices.

More general version for compact sets is the Krein Milman theorem:

Theorem 3.12. (Krein-Milman) Let $C \subseteq \mathbb{R}^n$ be a compact and convex set. Then $C$ is the convex hull of its extreme points. □

Definitions 3.13. $x \in C$ is extreme if $C \setminus \{x\}$ is convex.
This lecture was held by Dr. Annalisa Conversano.

Contents

1. Convex Cones and generalization of Krein Milman theorem 1
2. The cones $\mathcal{P}_{n,2d}$ and $\sum_{2,2d}$ 3
3. Proof of $\mathcal{P}_{3,4} = \sum_{3,4}$ 4

1. CONVEX CONES AND GENERALIZATION OF KREIN MILMAN THEOREM

We want to prove: $\mathcal{P}_{3,4} = \sum_{3,4}$

(i.e each positive semidefinite form in 3 variables of degree 4 is a sum of squares.)

To do it, we need several notions and intermediate results.

Definition 1.1. $C \subseteq \mathbb{R}^k$ is a convex cone if

- $x, y \in C \Rightarrow x + y \in C$, and
- $x \in C, \lambda \in \mathbb{R}_+ \Rightarrow \lambda x \in C$

(i.e if it is closed under addition and under multiplication by non-negative scalars.)

Fact 1.2. $C \subseteq \mathbb{R}^k$ is a convex cone if and only if it is closed under non-negative linear combinations of its elements, i.e.

$\forall n \in \mathbb{N}, \forall x_1, \ldots, x_n \in C, \forall \lambda_1, \ldots, \lambda_n \in \mathbb{R}_+ : \lambda_1 x_1 + \ldots + \lambda_n x_n \in C.$

Definition 1.3. Let $S \subseteq \mathbb{R}^k$. Then

$\text{Cone}(S) := \{\text{non-negative linear combinations of elements from } S\}$

is the convex cone generated by $S$.

Fact 1.4. For every $S \subseteq \mathbb{R}^k$, $\text{Cone}(S)$ is the smallest convex cone which includes $S$. 
Fact 1.5. If $S \subseteq \mathbb{R}^k$ is convex, then
\[ \text{Cone}(S) := \{ \lambda x \mid \lambda \in \mathbb{R}_+, x \in S \}. \]

Definition 1.6. $R \subseteq \mathbb{R}^k$ is a ray if $\exists \ x \in \mathbb{R}^k, \ x \neq 0$ s.t.
\[ R = \{ \lambda x \mid \lambda \in \mathbb{R}_+ \} := x^+ \]
(A ray $R$ is a half-line.)

Definition 1.7. Let $C \subseteq \mathbb{R}^k$ be a convex set:

1. a point $c \in C$ is an extreme point if $C \setminus \{ c \}$ is convex.
2. a ray $R \subseteq C$ is an extreme ray if $C \setminus R$ is convex.

Notation 1.8. Let $C \subseteq \mathbb{R}^k$ convex.

1. $\text{ext}(C) := \text{set of all extreme points in } C$
2. $\text{rext}(C) := \text{set of all extreme rays in } C$

Definition 1.9. (1) A straight line $L \subseteq \mathbb{R}^k$ is a translate of a 1-dimensional subspace, i.e.
\[ L = \{ x + \lambda y \mid \lambda \in \mathbb{R} \}, \text{ for some } x, y \in \mathbb{R}^k, y \neq 0. \]

2. $C \subseteq \mathbb{R}^k$ is line free if $C$ contains no straight lines.

Theorem 1.10. (Klee) Let $C \subseteq \mathbb{R}^k$ be a closed line free convex set. Then
\[ C = \text{cvx} (\text{ext}(C) \cup \text{rext}(C)) \]

Remark 1.11. (a) Let $C \subseteq \mathbb{R}^k$ be a convex cone and $\underline{x} \in C, \underline{x} \neq 0$. Then $\underline{x}$ is not extreme. Also $\underline{x}^+ \subset C$.

(b) Let $C \subseteq \mathbb{R}^k$ be a line free convex cone. Then $\text{ext}(C) = \{ 0 \}$.

Proof. If not, then $C \setminus \{ 0 \}$ is not convex, so
\[ \exists \ x, y \in C \setminus \{ 0 \}, \exists 0 < \lambda < 1 \text{ s.t. } \lambda \underline{x} + (1 - \lambda) \underline{y} \notin C \setminus \{ 0 \}. \]
But $C$ is convex, so
\[ \lambda \underline{x} + (1 - \lambda) \underline{y} = 0. \]
That means that $\underline{x}^+ \cup \underline{y}^+$ is a straight line in $C$, a contradiction. \qed
Corollary 1.12. (Generalization of Krein-Milman to closed line free convex cone) Let $C \subseteq \mathbb{R}^k$ be a closed line free convex cone. Then $C = \text{cvx}(\text{rext}(C))$

Proof. By Remark 1.11, $\text{ext}(C) = \{0\}$. Applying Theorem 1.10, we get $C = \text{cvx}(\text{rext}(C))$. □

Remark 1.13. Let $C$ be a line free convex cone

1. $0 \neq \bar{x} \in C$ belongs to an extreme ray (equivalently, the ray $\{\lambda \bar{x} | \lambda \in \mathbb{R}_+\}$ generated by $\bar{x}$ is extreme) if and only if whenever $\bar{x} = x_1 + x_2$, with $x_1, x_2 \in C$, then $x_i = \lambda_i \bar{x}$; $\lambda_i \in \mathbb{R}_+, \lambda_1 + \lambda_2 = 1$ (i.e. $x_1, x_2$ belong to the ray generated by $\bar{x}$).

2. The set of convex linear combinations of points in extremal rays = the set of sum of points in extremal rays.

2. THE CONES $\mathcal{P}_{n,2d}$ and $\Sigma_{2,2d}$

Lemma 2.1. $\mathcal{P}_{n,2d}$ is a closed convex cone.

Proof. It is trivial that $\mathcal{P}_{n,2d}$ is a convex cone. Next we prove that $\mathcal{P}_{n,2d}$ is closed: Let $(P_k)_{k \in \mathbb{N}}$ be a sequence in $\mathcal{P}_{n,2d}$ converging to $P$. Then for all $x \in \mathbb{R}^n$, $P_k(x) \to P(x)$.

We want (to show that) $P \in \mathcal{P}_{n,2d}$, otherwise $\exists x_0 \in \mathbb{R}^n$, s.t. $P(x_0) = -\epsilon$, $\epsilon > 0$.

And since $P_k(x_0) \to P(x_0)$ in $\mathbb{R}^n, \forall \epsilon > 0, \exists m \in \mathbb{N} \text{ s.t. } \forall k > m : |P_k(x_0) - P(x_0)| < \epsilon$, thus (taking the same $\epsilon$ as above): $|P_k(x_0) + \epsilon| < \epsilon \Rightarrow P_k(x_0) < 0$, a contradiction (since $P_k \in \mathcal{P}_{n,2d} \forall k$). So, $P \in \mathcal{P}_{n,2d}$ and hence $\mathcal{P}_{n,2d}$ is closed. □

Lemma 2.2. The cone $\mathcal{P}_{n,2d}$ is line free.

Proof. Suppose not, then there exists a straight line $L$ in $\mathcal{P}_{n,2d}$. Write $L = \{F + \lambda G | \lambda \in \mathbb{R}\}; F, G \in \mathcal{P}_{n,2d}, G \neq 0$.

Since $-G \notin \mathcal{P}_{n,2d}$, take $x_0$ s.t. $-G(x_0) < 0$.

Then for (large enough $\lambda$ i.e.) $\lambda \to -\infty$ we have $F(x_0) + \lambda G(x_0) < 0$. 
\[ \Rightarrow L \notin \mathcal{P}_{n,2d}. \]

Hence \( \mathcal{P}_{n,2d} \) is line free.

**Corollary 2.3.** \( \mathcal{P}_{n,2d} \) is the convex hull of its extremal rays.

**Proof.** By Lemma 2.1 and Lemma 2.2, \( \mathcal{P}_{n,2d} \) is a line free closed convex cone. And therefore by the generalization of Krein-Milman (Corollary 1.12) it is the convex hull of its extremal rays.

**Definition 2.4.** A form \( F \in \mathcal{P}_{n,2d} \) is **extremal** in \( \mathcal{P}_{n,2d} \) if
\[ F = F_1 + F_2, \quad F_1, F_2 \in \mathcal{P}_{n,2d} \Rightarrow F_i = \lambda_i F; \quad i = 1, 2 \text{ for } \lambda_i \in \mathbb{R}_+ \text{ satisfying } \lambda_1 + \lambda_2 = 1. \]

Similar definition for \( \sum_{n,2d} \).

**Note 2.5.** By Remark 1.13 this just means that the ray generated by \( F \) is extremal.

**Remark 2.6.**
1. \( F \in \sum_{n,2d} \) extremal \( \Rightarrow \) \( F = G^2 \) for some \( G \in \mathcal{P}_{n,d} \).
2. The converse of (1) is not true in general.
   For example: \( (x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2 \) is not extremal in \( \sum_{2,4} \).
3. \( G^2 \) is extremal in \( \sum_{n,2d} \) \( \Rightarrow \) \( G^2 \) is extremal in \( \mathcal{P}_{n,2d} \).
   For instance Choi et al showed that
   \[ p := f^2, \quad f(x, y, z) = x^4y^2 + y^4z^2 + x^4 + 3x^2y^2z^2 + (x^2y + y^2z - z^2x - xyz)^2 \]
   is extremal in \( \sum_{3,12} \) but not in \( \mathcal{P}_{3,12} \).

**Notation 2.7.** We denote by \( \mathcal{E}(\mathcal{P}_{n,2d}) \) the set of all extremal forms in \( \mathcal{P}_{n,2d} \).

**Lemma 2.8.** Let \( E \in \mathcal{P}_{n,2d} \). Then
\[ E \in \mathcal{E}(\mathcal{P}_{n,2d}) \text{ if and only if } \forall F \in \mathcal{P}_{n,2d} \text{ with } E \geq F \exists \alpha \in \mathbb{R}_+ \text{ such that } F = \alpha E. \]

**Proof.** \((\Rightarrow)\) Let \( E \in \mathcal{E}(\mathcal{P}_{n,2d}), F \in \mathcal{P}_{n,2d} \) s.t \( E \geq F \), then
\[ G := E - F \in \mathcal{P}_{n,2d}, \text{ so } E = F + G. \]
Since \( E \) is extremal \( \exists \alpha, \beta \geq 0, \alpha + \beta = 1 \) such that \( F = \alpha E \) and \( G = \beta E \).
\((\Leftarrow)\) Let \( F_1, F_2 \in \mathcal{P}_{n,2d} \) so that \( E = F_1 + F_2 \), then \( E \geq F_1 \), so \( \exists \alpha \geq 0 \) such that \( F_1 = \alpha E \). Therefore \( F_2 = E - F_1 = (1 - \alpha)E \) with \( 1 - \alpha \geq 0 \) (since \( E, F_2 \in \mathcal{P}_{n,2d} \)). Thus \( E \) is extremal. \( \square \)
Corollary 2.9. Every \( F \in P_{n,2d} \) is a finite sum of forms in \( E(P_{n,2d}) \).

*Proof.* By Corollary 2.3 and Remark 1.13 (2). \( \square \)

3. PROOF OF \( P_{3,4} = \sum_{3,4} \)

Corollary 2.9 is the first main item in the proof of Hilbert’s Theorem (Theorem 2.8 of lecture 6) for the ternary quartic case. The second main item is the following lemma (which will be proved in the next lecture):

**Lemma 3.1.** Let \( T(x,y,z) \in P_{3,4} \). Then \( \exists \) a quadratic form \( q(x,y,z) \neq 0 \) s.t. \( T \geq q^2 \), i.e. \( T - q^2 \) is psd.

**Theorem 3.2.** \( P_{3,4} = \sum_{3,4} \)

*Proof.* Let \( F \in P_{3,4} \). By Corollary 2.9, \( F = E_1 + \ldots + E_k \), where \( E_i \) is extremal in \( P_{3,4} \) for \( i = 1, \ldots, k \).

Applying Lemma 3.1 to each \( E_i \) we get 
\( E_i \geq q_i^2 \), for some quadratic form \( q_i \neq 0 \)

Since \( E_i \) is extremal, by Lemma 2.8, we get 
\( q_i^2 = \alpha_i E_i ; \) for some \( \alpha_i > 0, \forall i = 1, \ldots, k \)

and so \( E_i = \left( \frac{1}{\sqrt{\alpha_i}} q_i \right)^2 \) and hence \( F \in \sum_{3,4} \). \( \square \)
Theorem 1.1. (Recall Theorem 2.8 of lecture 6) \( \sum_{n,m} = \mathcal{P}_{n,m} \) iff

(i) \( n = 2 \) or

(ii) \( m = 2 \) or

(iii) \( (n, m) = (3, 4) \).

In lecture 7 (Theorem 3.2) we showed the proof of (Hilbert’s) Theorem 1.1 part (iii), i.e. for ternary quartic forms: \( \mathcal{P}_{3,4} = \sum_{3,4} \) using generalization of Krein-Milman theorem (applied to our context), plus the following lemma:

Lemma 1.2. (3.1 of lecture 7) Let \( T(x, y, z) \in \mathcal{P}_{3,4} \). Then \( \exists \) a quadratic form \( q(x, y, z) \neq 0 \) s.t. \( T \geq q^2 \), i.e. \( T - q^2 \) is psd.

Proof. Consider three cases concerning the zero set of \( T \).

Case 1. \( T > 0 \), i.e. \( T \) has no non trivial zeros.

Let \( \phi(x, y, z) := \frac{T(x, y, z)}{(x^2 + y^2 + z^2)^2}, \forall (x, y, z) \neq 0. \)

Let \( \mu := \inf_{\mathbb{S}^2} \phi \geq 0 \), where \( \mathbb{S}^2 \) is the unit sphere.

Since \( \mathbb{S}^2 \) is compact and \( \phi \) is continuous, \( \exists (a, b, c) \in \mathbb{S}^2 \) s.t. \( \mu = \phi(a, b, c) > 0 \)

Therefore \( \forall (x, y, z) \in \mathbb{S}^2: T(x, y, z) \geq \mu(x^2 + y^2 + z^2)^2. \)
Claim: $T(x, y, z) \geq \mu(x^2 + y^2 + z^2)^2$ for all $(x, y, z) \in \mathbb{R}^3$.
Indeed, it is trivially true at the point $(0, 0, 0)$, and
for $(x, y, z) \in \mathbb{R}^3 \setminus \{0\}$ denote $N := \sqrt{x^2 + y^2 + z^2}$, then \( \left( \frac{x}{N}, \frac{y}{N}, \frac{z}{N} \right) \in \mathbb{S}^2 \), which implies that
\[
T\left( \frac{x}{N}, \frac{y}{N}, \frac{z}{N} \right) \geq \mu \left( \left( \frac{x}{N} \right)^2 + \left( \frac{y}{N} \right)^2 + \left( \frac{z}{N} \right)^2 \right)^2.
\]
So, by homogeneity we get
\[
T(x, y, z) \geq \mu(x^2 + y^2 + z^2)^2 = \left( \sqrt{\mu}(x^2 + y^2 + z^2) \right)^2,
\]
as claimed. □

Case 2. $T$ has exactly one (nontrivial) zero.
By changing coordinates, we may assume w.l.o.g. that zero to be $(1, 0, 0)$, i.e. $T(1, 0, 0) = 0$.
Writing $T$ as a polynomial in $x$ one gets
\[
T(x, y, z) = ax^4 + (b_1y + b_2z)x^3 + f(y, z)x^2 + 2g(y, z)x + h(y, z),
\]
where $f, g$ and $h$ are binary quadratic, cubic and quartic forms respectively.
Reducing $T$: Since $T(1, 0, 0) = 0$ we get $a = 0$.
Further, suppose $(b_1, b_2) \neq (0, 0)$, it $\Rightarrow \exists (y_0, z_0) \in \mathbb{R}^2$ s.t. $b_1y_0 + b_2z_0 < 0$, then taking $x$ big enough $\Rightarrow T(x_0, y_0, z_0) < 0$, a contradiction to $T \geq 0$. Thus $b_1 = b_2 = 0$ and therefore
\[
T(x, y, z) = f(y, z)x^2 + 2g(y, z)x + h(y, z)
\]
(1)
Next, clearly $h(y, z) \geq 0$ [since otherwise $T(0, y_0, z_0) = h(y_0, z_0) < 0$ for some $(y_0, z_0) \in \mathbb{R}^2$, a contradiction].
Also $f(y, z) \geq 0$, if not, say $f(y_0, z_0) < 0$ for some $(y_0, z_0)$, then taking $x$ big enough we get $T(x, y_0, z_0) < 0$, a contradiction.
Thus $f, h \geq 0$.
From (1) we can write:
\[
fT(x, y, z) = (xf + g)^2 + (fh - g^2)
\]
(2)
Claim: $fh - g^2 \geq 0$
If not, say $(fh - g^2)(y_0, z_0) < 0$ for some $(y_0, z_0)$. Then there are two cases to be considered here:
Case (i): $f(y_0, z_0) = 0$. In this case we claim $g(y_0, z_0) = 0$ because if not then $T(x, y_0, z_0) = 2g(y_0, z_0)x + h(y_0, z_0) < 0$ and we take $|x_0|$ large enough so that $2g(y_0, z_0)x_0 + h(y_0, z_0) < 0$, a contradiction.
Case (ii): \( f(y_0, z_0) > 0 \), we take \( |x_0| \) such that \( x_0 f(y_0, z_0) + g(y_0, z_0) = 0 \), then
\[ fT(x_0, y_0, z_0) = (fh - g^2)(y_0, z_0) < 0, \]
a contradiction.
So our claim is established and \( fh - g^2 \geq 0 \).
Now the polynomial \( f \) is a psd binary form, thus by Lemma 1.3 below \( f \) is sum of two squares. Let us consider the two subcases:

**Case 2.1.** \( f \) is a perfect square. Then \( f = f_1^2 \), with \( f_1 = by + cz \) for some \( b, c \in \mathbb{R} \).
Up to multiplication by a constant \((-c, b)\) is the unique zero of \( f_1 \) and so of \( f \).

Thus
\[
(fh - g^2)(-c, b) = -(g(-c, b))^2 \leq 0
\]
which is a contradiction unless \( g(-c, b) = 0 \) which means \(^1\) that \( f_1 | g \), i.e. \( g(y, z) = f_1(y, z)g_1(y, z) \). Then from (2) we get
\[
T \geq (xf + g)^2
= (x f_1^2 + f_1 g_1)^2
= f_1^2 (x f_1 + g_1)^2
= f(x f_1 + g_1)^2.
\]
Hence \( T \geq (xf_1 + g_1)^2 \) as required.

**Case 2.2.** \( f = f_1^2 + f_2^2 \), with \( f_1, f_2 \) linear in \( y, z \).
Now \( f_1 \neq \lambda f_2 \) [otherwise we are in Case 2.1]
i.e. \( f_1, f_2 \) don’t have same non-trivial zeroes, otherwise they would be multiples of each other and \( f \) would be a perfect square. Hence \( f > 0 \).

**Claim 1:** \( fh - g^2 > 0 \)
If not, i.e. if \( \exists (y_0, z_0) \neq (0, 0) \) s.t. \( (fh - g^2)(y_0, z_0) = 0 \), then \( (y_0, z_0) \) could be completed to a zero \( (-g(y_0, z_0), y_0, z_0) \) of \( T \), which contradicts our hypothesis that \( T \) has only 1 zero \((1, 0, 0)\). Thus \( fh - g^2 > 0 \).

**Claim 2:** \( \frac{fh - g^2}{f^3} \) has a minimum \( \mu > 0 \) on the unit circle \( \mathbb{S}^1 \). (clear)

So, just as in Case 1,
\[
fh - g^2 \geq \mu f^3 \quad \forall (y, z) \in \mathbb{R}^2.
\]
\[ T \geq fh - g^2 \geq \mu f^3, \text{ by (2)} \]
\[ T \geq \mu f^2 \geq (\sqrt{\mu} f)^2, \text{ as claimed.} \]

---

\(^1\)See (5) implies (2) of Theorem 4.5.1 in *Real Algebraic Geometry* by J. Bochnak, M. Coste, M.-F. Roy or (5) implies (2) of Theorem 12.7 in *Positive Polynomials and Sum of Squares* by M. Marshall.
Case 3. $T$ has more than one zero.

Without loss of generality, assume $(1,0,0)$ and $(0,1,0)$ are two of the zeros of $T$. As in case 2, reduction $\Rightarrow T$ is of degree at most 2 in $x$ as well as in $y$ and so we can write:

$$T(x,y,z) = f(y,z)x^2 + 2g(y,z)zx + z^2h(y,z),$$

where $f, g, h$ are quadratic forms and $f, h \geq 0$.

And so

$$fT = (xf + zg)^2 + z^2(fh - g^2),$$

with $fh - g^2 \geq 0$ [Indeed, if $(fh - g^2)(y_0, z_0) < 0$ for some $(y_0, z_0)$, then we must have case distinction as on bottom of page 2 i.e. $f(y_0, z_0) = 0$ or $f(y_0, z_0) > 0$].

Using Lemma 1.3 if $f$ or $h$ is a perfect square, then we get the desired result as in the Case 2.1. Hence we suppose $f$ and $h$ to be sum of two squares and again as before (as in Case 2.2) $f, h > 0$. We consider the following two possible subcases on $fh - g^2$:

**Case 3.1.** Suppose $fh - g^2$ has a zero $(y_0, z_0) \neq (0,0)$.

Set $x_0 = \frac{g(y_0, z_0)}{f(y_0, z_0)}$ and

$$T_1 := T(x + x_0z, y, z) = x^2f + 2xz(g + x_0f) + z^2(h + 2x_0g + x_0^2f)$$

Evaluating (3) at $(x + x_0z, y, z)$, we get

$$fT_1 = fT(x + x_0z, y, z) = \left((x + x_0)f + zg\right)^2 + z^2(fh - g^2),$$

Multiplying (4) by $f$, we get

$$fT'_1 = fT(x + x_0z, y, z) = x^2f^2 + 2xzf(g + x_0f) + z^2f(h + 2x_0g + x_0^2f)$$

Now compare the coefficients of $z^2$ in (3)' and (4)' to get

$$(x_0f + g)^2 + (fh - g^2) = f(h + 2x_0g + x_0^2f),$$

i.e. $h + 2x_0g + x_0^2f = \frac{(fh - g^2) + (x_0f + g)^2}{f} \forall (y, z) \neq (0,0)$

In particular, $h + 2x_0g + x_0^2f$ is psd and has a zero, namely $(y_0, z_0) \neq (0,0)$.

Thus $(h + 2x_0g + x_0^2f)$, being a psd quadratic in $y, z$, which has a nontrivial zero $(y_0, z_0)$, is a perfect square [since by the arguments similar to Case 2.2, it cannot be a sum of two (or more) squares].

Say $(h + 2x_0g + x_0^2f) = h_1^2$, with $h_1(y, z)$ linear and $h_1(y_0, z_0) = 0$

Now $(g + x_0f)(y_0, z_0) = g(y_0, z_0) + x_0f(y_0, z_0) = 0$. So, $g + x_0f$ vanishes at every zero of the linear form $h_1$. Therefore, we have $g + x_0f = g_1h_1$ for some $g_1$. 


So (from (4)), \( T_1 = fx^2 + 2xzg_1h_1 + z^2h_1^2 \)
\( = (zh_1 + xg_1)^2 + x^2(f - g_1^2) \)
\( \Rightarrow h_1^2T_1 = h_1^2(zh_1 + xg_1)^2 + x^2(h_1^2f - (h_1g_1)^2) \)
\( = h_1^2(zh_1 + xg_1)^2 + x^2(hf - g^2) \)
\( \geq 0 \)
\( \Rightarrow h_1^2T_1 \geq h_1^2(zh_1 + xg_1)^2 \)
\( \Rightarrow T(x + x_0z, y, z) =: T_1 \geq (zh_1 + xg_1)^2 \)
By change of variables \((x \rightarrow x - x_0z)\), we get \( T \geq \) a square of a quadratic form, as desired.

**Case 3.2.** Suppose \( fh - g^2 > 0 \) (i.e. \( fh - g^2 \) has no zero).

Then (as in **Case 2.2**), \( \exists \mu > 0 \) s.t. \( \frac{fh - g^2}{(y^2 + z^2)f} \geq \mu \) on \( S^1 \)
and so \( fh - g^2 \geq \mu(y^2 + z^2)f \forall (y, z) \in \mathbb{R}^2 \).

Hence, by (†)
\[
fT = (xf + zg)^2 + z^2(fh - g^2) \geq z^2(fh - g^2) \geq \mu z^2(y^2 + z^2)f,
\]
giving as required
\[
T \geq (\sqrt{\mu}y)^2 + (\sqrt{\mu}z)^2 \geq \mu \]
\( \Rightarrow T \geq (\sqrt{\mu}z)^2 \)
\( \square \)(**Case 3**)

This completes the proof of the Lemma 1.2.

Next we prove Theorem 1.1 part (i), i.e. for binary forms. This was also used as a helping lemma in the proof of above lemma:

**Lemma 1.3.** If \( f \) is a binary psd form of degree \( m \), then \( f \) is a sum of squares of binary forms of degree \( m/2 \), that is, \( \mathcal{P}_{2,m} = \sum_{2,m} \). In fact, \( f \) is sum of two squares.

**Proof.** If \( f \) is a binary form of degree \( m \), we can write
\[
f(x, y) = \sum_{k=0}^{m} c_k x^k y^{m-k}; \ c_k \in \mathbb{R}
\]
\[ y^n \sum_{k=0}^{m} c_k \left( \frac{x}{y} \right)^k, \]

where \( m \) is an even number and \( c_m \neq 0 \), since \( f \) is psd.

Without loss of generality let \( c_m = 1 \).

Put \( g(t) = \sum_{k=0}^{m} c_k t^k \).

Over \( \mathbb{C} \), \( g(t) = \prod_{k=1}^{m/2} (t - z_k)(t - \bar{z}_k) \); \( z_k = a_k + ib_k, a_k, b_k \in \mathbb{R} \)

\[ = \prod_{k=1}^{m/2} ((t - a_k)^2 + b_k^2) \]

\[ \Rightarrow f(x, y) = y^n g \left( \frac{x}{y} \right) = \prod_{k=1}^{m/2} ((x - a_k y)^2 + b_k^2 y^2) \]

Then using iteratively the identity

\[(X^2 + Y^2)(Z^2 + W^2) = (XZ - YW)^2 + (YZ + XW)^2, \]

we obtain that \( f(x, y) \) is a sum of two squares. \( \square \)

**Example 1.4.** Using the ideas in the proof of above lemma, we write the binary form

\[ f(x, y) = 2x^6 + y^6 - 3x^4y^2 \]

as a sum of two squares:

Consider \( f \) written in the form

\[ f(x, y) = y^6 \left( 2 \left( \frac{x}{y} \right)^6 + 1 - 3 \left( \frac{x}{y} \right)^4 \right) \]

So, the polynomial \( g(t) = 2t^6 - 3t^4 + 1 \). This polynomial has double roots 1 and -1 and complex roots \( \pm \frac{1}{\sqrt{2}} i \).

Thus

\[ g(t) = 2(t - 1)^2(t + 1)^2(t^2 + \frac{1}{2}) = (t^2 - 1)^2(2t^2 + 1). \]

Therefore we have

\[ f(x, y) = y^6 g \left( \frac{x}{y} \right) = (x^2 - y^2)^2(2x^2 + y^2) = 2x^2(x^2 - y^2)^2 + y^2(x^2 - y^2)^2 \]

written as a sum of two squares. \( \square \)
Next we prove Theorem 1.1 part (ii), i.e. for quadratic forms:

**Lemma 1.5.** If \( f(x_1, \ldots, x_n) \) is a psd quadratic form, then \( f(x_1, \ldots, x_n) \) is sos of linear forms, that is, \( P_{n,2} = \sum_{n,2} \).

**Proof.** If \( f(x_1, \ldots, x_n) \) is a quadratic form, then we can write

\[
f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} x_i a_{ij} x_j, \quad \text{where } A = [a_{ij}] \text{ is a symmetric matrix with } a_{ij} \in \mathbb{R}.
\]

We have \( f = X^T A X \), where \( X^T = [x_1, \ldots, x_n] \).

By the spectral theorem for Hermitian matrices, there exists a real orthogonal matrix \( S \) and a diagonal matrix \( D = \text{diag}(d_1, \ldots, d_n) \) such that \( D = S^T A S \). Then

\[
f = X^T S S^T A S S^T X = (S^T X)^T S^T A S (S^T X)
\]

Putting \( Y = [y_1, \ldots, y_n]^T = S^T X \), we get

\[
f = Y^T S^T A S Y = Y^T D Y = \sum_{i=1}^{n} d_i y_i^2, \quad d_i \in \mathbb{R}.
\]

Since \( f \) is psd, we have \( d_i \geq 0 \ \forall \ i \), and so

\[
f = \sum_{i=1}^{n} \left( \sqrt{d_i} y_i \right)^2,
\]

Thus

\[
f(x_1, \ldots, x_n) = \sum_{i=1}^{n} \left( \sqrt{d_i} (s_{1,i} x_1 + \ldots, s_{n,i} x_n) \right)^2,
\]

that is, \( f \) is sos of linear forms. \( \square \)
1. PROOF OF HILBERT’S THEOREM (Continued)

Theorem 1.1. (Recall) (Hilbert) \( \sum_{n,m} = \mathcal{P}_{n,m} \) iff

(i) \( n = 2 \) or

(ii) \( m = 2 \) or

(iii) \( (n,m) = (3,4) \).

And in all other cases \( \sum_{n,m} \not\subseteq \mathcal{P}_{n,m} \).

Note that here \( m \) is necessarily even because a psd polynomial must have even degree (see Lemma 2.3 in lecture 6).

We have shown one direction (\( \Leftarrow \)) of Hilbert’s Theorem (1.1 above), i.e. if \( n = 2 \) or \( m = 2 \) or \( (n,m) = (3,4) \), then \( \sum_{n,m} = \mathcal{P}_{n,m} \). To prove the other direction we have to show that:

\[ \sum_{n,m} \not\subseteq \mathcal{P}_{n,m} \text{ for all pairs } (n,m) \text{ s.t. } n \geq 3, m \geq 4 \text{ (m even)} \text{ with } (n,m) \neq (3,4). \]  

(1)
Hilbert showed (using algebraic geometry) that $\sum_{3,6} \not\subseteq \mathcal{P}_{3,6}$ and $\sum_{4,4} \not\subseteq \mathcal{P}_{4,4}$. This is a reduction of the general problem (1), indeed we have:

**Lemma 1.2.** If $\sum_{3,6} \not\subseteq \mathcal{P}_{3,6}$ and $\sum_{4,4} \not\subseteq \mathcal{P}_{4,4}$, then $\sum_{n,m} \not\subseteq \mathcal{P}_{n,m}$ for all $n \geq 3, m \geq 4$ and $(n, m) \neq (3, 4)$, $(m$ even).

*Proof.* Clearly, given $F \in \mathcal{P}_{n,m} - \sum_{n,m}$, then $F \in \mathcal{P}_{n,j+m} - \sum_{n,j+m}$ for all $j \geq 0$.

Moreover, we claim: $F \in \mathcal{P}_{n,m} - \sum_{n,m} \Rightarrow x_i^2F \in \mathcal{P}_{n,m+2i} - \sum_{n,m+2i} \forall i \geq 0$

*Proof of claim:* Assume for a contradiction that $x_i^2|f_j \forall j$, so $F \in \mathcal{P}_{n,m} - \sum_{n,m} \Rightarrow \sum_{j=1}^k f_j^2(x_1, \ldots, x_n)$.

Hilbert described a method (non constructive) to produce counter examples in the 2 crucial cases, but no explicit examples appeared in literature for next 80 years.

In 1967 Motzkin presented a specific example of a ternary sextic form that is positive semidefinite but not a sum of squares.

### 2. THE MOTZKIN FORM

**Proposition 2.1.** The Motzkin form

$$M(x, y, z) = z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2 \in \mathcal{P}_{3,6} - \sum_{3,6}.$$  

*Proof.* Using the arithmetic geometric inequality (Lemma 2.2 below) with $a_1 = z^6, a_2 = x^4y^2, a_3 = x^2y^4$ and $\alpha_1 = \alpha_2 = \alpha_3 = \frac{1}{3}$, clearly gives $M \geq 0$.

Degree arguments and exercise 3 of ÜB 6 from Real Algebraic Geometry course (WS 2009-10) gives $M$ is not a sum of squares.

**Lemma 2.2.** (Arithmetic-geometric inequality I) Let $a_1, a_2, \ldots, a_n \geq 0 ; n \geq 1$. Then
\[
\frac{a_1 + a_2 + \ldots + a_n}{n} \geq (a_1 a_2 \ldots a_n)^{\frac{1}{n}}.
\]

**Lemma 2.3. (Arithmetic-geometric inequality II)** Let \( \alpha_i \geq 0, a_i \geq 0; i = 1, \ldots, n \) with \( \sum_{i=1}^{n} \alpha_i = 1. \) Then
\[
\alpha_1 a_1 + \ldots + \alpha_n a_n - \alpha_1^{a_1} \ldots a_n^{a_n} \geq 0
\]
(with equality iff all the \( x_i \) are equal).

**Proof.** Exercise 2 in ÜB 5.

### 3. ROBINSON’S METHOD (1970)

In 1970’s R. M. Robinson gave a ternary sextic based on the method described by Hilbert, but after drastically simplifying Hilbert’s original ideas. He used it to construct examples of forms in \( P_{4,4} - \sum_{4,4} \) as well as forms in \( P_{3,6} - \sum_{3,6} \).

This method is based on the following lemma:

**Lemma 3.1.** A polynomial \( P(x,y) \) of degree at most 3 which vanishes at eight of the nine points \( (x,y) \in \{-1,0,1\} \times \{-1,0,1\} \) must also vanish at the ninth point.

**Proof.** Assign weights to the following nine points:

\[
w(x,y) = \begin{cases} 1, & \text{if } x, y = \pm 1 \\ -2, & \text{if } (x = \pm 1, y = 0) \text{ or } (x = 0, y = \pm 1) \\ 4, & \text{if } x, y = 0 \end{cases}
\]

Define the weight of a monomial as:

\[
w(x^k y^l) := \sum_{i=1}^{9} w(q_i) x^k y^l(q_i), \text{ for } q_i \in \{-1,0,1\} \times \{-1,0,1\}
\]

Define the weight of a polynomial \( P(x,y) = \sum_{k,l} c_{k,l} x^k y^l \) as:

\[
w(P) := \sum_{k,l} c_{k,l} w(x^k y^l)
\]

**Claim 1:** \( w(x^k y^l) = 0 \) unless \( k \) and \( l \) are both strictly positive and even.

**Proof of claim 1:** Let us compute the monomial weights
• if \( k = 0, l \geq 0 \): then we have
  \[
  w(x^k y^l) = 1 + (-1)^l + 1 + (-1)^l + (-2) + (-2)(-1)^l = 0
  \]

• if \( l = 0, k \geq 0 \): then similarly we have \( w(x^k y^l) = 0 \), and

• if \( k, l > 0 \): then we have
  \[
  w(x^k y^l) = 1 + (-1)^l + (-1)^l + (-1)^k = \begin{cases} 0 & \text{if either } k \text{ or } l \text{ is odd} \\ 4 & \text{otherwise} \end{cases}
  \]

  \( \Box \) (claim 1)

**Claim 2:** \( w(P) = \sum_{i=1}^{9} w(q_i)P(q_i) \)

**Proof of claim 2:** \( w(P) := \sum_{k,l} c_{k,l} w(x^k y^l) = \sum_{k,l} c_{k,l} \sum_{i=1}^{9} w(q_i) x^k y^l(q_i) = \sum_{i=1}^{9} w(q_i) \sum_{k,l} c_{k,l} x^k y^l(q_i) = \sum_{i=1}^{9} w(q_i)P(q_i) \)

  \( \Box \) (claim 2)

Now, claim 1 and definition of \( w(P) \Rightarrow \deg(P(x,y)) \leq 3 \) then \( w(P) = 0 \).

Also, from claim 2 we get:

\[
P(1,1)+P(1,-1)+P(-1,1)+P(-1,-1)+(-2)P(1,0)+(-2)P(-1,0)+(-2)P(0,1)+(-2)P(0,-1)+4P(0,0) = 0
\]

Now verify that if \( P(x,y) = 0 \) for any eight (of the nine) points, then we are left with \( \alpha P(x,y) = 0 \) (for some \( \alpha \neq 0, \alpha = \pm 1, \pm 2 \)) at the ninth point. \( \Box \)

4. THE ROBINSON FORM

**Theorem 4.1.** Robinsons form \( R(x,y,z) = x^6 + y^6 + z^6 - (x^4y^2 + x^4z^2 + y^4x^2 + y^4z^2 + z^4x^2 + z^4y^2) + 3x^2y^2z^2 \) is psd but not a sos, i.e. \( R \in P_{3,6} - \sum_{3,6} \).

**Proof.** Consider the polynomial

\[
P(x,y) = (x^2 + y^2 - 1)(x^2 - y^2)^2 + (x^2 - 1)(y^2 - 1)
\]

(2)

Note that \( R(x,y,z) = P_h(x,y,z) = z^6 P(x/z, y/z) \).

By our observation: \( P_h \) is psd iff \( P \) psd; \( P_h \) is sos iff \( P \) is sos,
We shall show that $P(x,y)$ is psd but not sos.

Multiplying both sides of (2) by $(x^2 + y^2 - 1)$ and adding to (2) we get:

$$(x^2 + y^2)P(x,y) = x^2(x^2 - 1)^2 + y^2(y^2 - 1)^2 + (x^2 + y^2 - 1)^2(x^2 - y^2)^2$$

(3)

From (3) we see that $P(x,y) \geq 0$, i.e. $P(x,y)$ is psd.

Assume $P(x,y) = \sum_j P_j(x,y)^2$ is sos

$\deg P(x,y) = 6$, so $\deg P_j \leq 3 \forall j$.

By (2) it is easy to see that $P(0,0) = 1$ and $P(x,y) = 0$ for all other eight points $(x,y) \in \{-1, 0, 1\}^2 \setminus \{(0,0)\}$, therefore every $P_j(x,y)$ must also vanish at these eight points.

Hence by Lemma 3.1 (above) it follows that: $P_j(0,0) = 0 \forall j$.

So $P(0,0) = 0$, which is a contradiction. □

**Proposition 4.2.** The quarternary quartic $Q(x,y,z,w) = w^4 + x^2y^2 + y^2z^2 + x^2z^2 - 4xyzw$ is psd, but not sos, i.e., $Q \in \mathcal{P}_{4,4} - \sum_{4,4} \mathcal{P}.$

**Proof.** The arithmetic-geometric inequality (Lemma 2.3) clearly implies $Q \geq 0$.

Assume now that $Q = \sum_j q_j^2$, $q_j \in \mathcal{F}_{4,2}$.

Forms in $\mathcal{F}_{4,2}$ can only have the following monomials:

$x^2, y^2, z^2, w^2, xy, xz, xw, yz, yw, zw$

If $x^2$ occurs in some of the $q_j$, then $x^4$ occurs in $q_j^2$ with positive coefficient and hence in $\sum q_j^2$ with positive coefficient too, but this is not the case.

Similarly $q_j$ does not contain $y^2$ and $z^2$.

The only way to write $x^2w^2$ as a product of allowed monomials is $x^2w^2 = (xw)^2$.

Similarly for $y^2w^2$ and $z^2w^2$.

Thus each $q_j$ involves only the monomials $xy, xz, yz$ and $w^2$.

But now there is no way to get the monomial $xyzw$ from $\sum q_j^2$, hence a contradiction. □
Proposition 4.3. The ternary sextic $S(x, y, z) = x^4 y^2 + y^4 z^2 + z^4 x^2 - 3x^2 y^2 z^2$ is psd, but not a sos, i.e., $S \in \mathcal{P}_{3,6} - \sum_{3,6}$.

Proof. Exercise 3 of ÜB 5. \qed
1. Ring of formal power series

Definition 1.1. (Recall) Let \( S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[x_1, \ldots, x_n] \), then

\[
K_S := \{x \in \mathbb{R}^n \mid g_i(x) \geq 0 \ \forall \ i = 1, \ldots, s\},
\]

\[
T_S := \left\{ \sum_{e_1, \ldots, e_s \in \{0, 1\}} \sigma_e g_1^{e_1} \cdots g_s^{e_s} \mid \sigma_e \in \Sigma\mathbb{R}[X]^2, e = (e_1, \ldots, e_s) \right\}
\] is the preordering generated by \( S \).

Proposition 1.2. Let \( n \geq 3 \). Let \( S \) be a finite subset of \( \mathbb{R}[x] \) such that \( K_S \subseteq \mathbb{R}^n \) has non-empty interior. Then \( \exists f \in \mathbb{R}[x] \) such that \( f \geq 0 \) on \( \mathbb{R}^n \) and \( f \notin T_S \).

To prove proposition 1.2 we need to learn a few facts about formal power series rings:

Definition 1.3. \( \mathbb{R}\llbracket x \rrbracket := \mathbb{R}\llbracket x_1, \ldots, x_n \rrbracket \) ring of formal power series in \( x = (x_1, \ldots, x_n) \) with coefficients in \( \mathbb{R} \), i.e., \( f \in \mathbb{R}\llbracket x \rrbracket \) is expressible uniquely in the form

\[ f = f_0 + f_1 + \ldots, \]

where \( f_i \) is a homogenous polynomial of degree \( i \) in the variables \( x_1, \ldots, x_n \).

Here:

- Addition is defined point wise, and
multiplication is defined using distributive law:

\[
\left( \sum_{i=0}^{\infty} f_i \right) \left( \sum_{i=0}^{\infty} g_i \right) = (f_0g_0) + (f_0g_1 + f_1g_0) + (f_0g_2 + f_1g_1 + f_2g_0) + \ldots = \sum_{k=0}^{\infty} \left( \sum_{i+j=k} f_ig_j \right)
\]

So, both addition and multiplication are well defined and \(\mathbb{R}[[x]]\) is an integral domain and \(\mathbb{R}[x] \subseteq \mathbb{R}[[x]]\).

**Notation 1.4.** Fraction field of \(\mathbb{R}[[x]]\) is denoted by \(\mathbb{F}(\mathbb{R}[[x]]) := \mathbb{R}((x))\).

The valuation \(v : \mathbb{R}[[x]] \to \mathbb{Z} \cup \{\infty\}\) defined by:

\[
v(f) = \begin{cases} 
\text{least } i \text{ s.t. } f_i \neq 0, & \text{if } f \neq 0 \\
\infty, & \text{if } f = 0
\end{cases}
\]

extends to \(\mathbb{R}((x))\) via

\[
v\left(\frac{f}{g}\right) := v(f) - v(g).
\]

**Lemma 1.5.** Let \(f \in \mathbb{R}[[x]]; f = f_k + f_{k+1} + \ldots\), where \(f_i\) homogeneous of degree \(i, f_k \neq 0\). Assume that \(f\) is a sos in \(\mathbb{R}[[x]]\).

Then \(k\) is even and \(f_k\) is a sum of squares of forms of degree \(\frac{k}{2}\).

*Proof.* \(f = g_1^2 + \ldots + g_l^2\), and

\[g_i = g_{ij} + g_{i,j+1} + \ldots, \text{ with } j = \min\{v(g_i) : i = 1, \ldots, l\}\]

Then \(f_0 = \ldots = f_{2j-1} = 0\) and \(f_{2j} = \sum_{i=1}^{k} g_{ij}^2 \neq 0\)

So, \(k = 2j\). \(\square\)

**1.6. Units in \(\mathbb{R}[[x]]\):** Let \(f = f_0 + f_1 + \ldots\), with \(v(f) = 0\) i.e. \(f_0 \neq 0\). Then \(f\) factors as

\[f = a(1 + t); \text{ where}
\]

\(a \in \mathbb{R}, a \neq 0, t \in \mathbb{R}[[x]]\) and \(v(t) \geq 1\) with \(a := f_0 \in \mathbb{R} \setminus \{0\}; \ t := \frac{1}{f_0}(f_1 + f_2 + \ldots)\).

**Lemma 1.7.** \(f \in \mathbb{R}[[x]]\) is a unit of \(\mathbb{R}[[x]]\) if and only if \(f_0 \neq 0\) (i.e. \(v(f) = 0\)).

*Proof.* \[
\frac{1}{1 + t} = 1 - t + t^2 - \ldots, \text{ for } t \in \mathbb{R}[[x]]; \ v(t) \geq 1
\]
is a well defined element of $\mathbb{R}[x]$. 

So, if $v(f) = 0$, then $f = a(1 + t)$ with $a \in \mathbb{R}, a \neq 0$ gives 

$$f^{-1} = \frac{1}{a(1 + t)} \in \mathbb{R}[x].$$

\[ \square \]

**Corollary 1.8.** It follows that $\mathbb{R}[x]$ is a local ring because $I = \{ f \mid v(f) \geq 1 \}$ is a maximal ideal (quotient is a field $\mathbb{R}$).

**Lemma 1.9.** Let $f \in \mathbb{R}[x]$ a positive unit, i.e. $f_0 > 0$. Then $f$ is a square in $\mathbb{R}[x]$.

Proof. $f = a(1 + t); a > 0, v(t) \geq 1$

$$\sqrt{f} = \sqrt{a} \sqrt{1 + t},$$

where $\sqrt{1 + t} := (1 + t)^{1/2} = 1 + \frac{1}{2}t - \frac{1}{8}t^2 + \ldots$ is a well defined element of $\mathbb{R}[x]$. \[ \square \]

**Lemma 1.10.** Suppose $n \geq 3$. Then $\exists f \in \mathbb{R}[x]$ such that $f \geq 0$ on $\mathbb{R}^n$ and $f$ is not a sum of squares in $\mathbb{R}[x]$.

Proof. Let $f \in \mathbb{R}[x]$ be any homogeneous polynomial which is $\geq 0$ on $\mathbb{R}^n$ but is not a sum of squares in $\mathbb{R}[x]$ (by Hilbert’s Theorem such a polynomial exists). Now by lemma 1.5 it follows that $f$ is not sos in $\mathbb{R}[x]$. \[ \square \]

Now we prove Proposition 1.2:

**Proof of Proposition 1.2.** Let $S = \{g_1, \ldots, g_s\}$

- W.l.o.g. assume $g_i \neq 0$, for each $i = 1, \ldots, s$. So $g := \prod_{i=1}^{s} g_i \neq 0$

int$(K_S) \neq \emptyset \Rightarrow \exists p := (p_1, \ldots, p_n) \in \text{int}(K_S)$ with $\prod_{i=1}^{s} g_i(p) \neq 0$.

Thus $g_i(p) > 0 \forall i = i, \ldots, s$.

- W.l.o.g. assume $p = 0$ the origin

(by making a variable change $Y_i := X_i - p_i$, and noting that $\mathbb{R}[Y_1, \ldots, Y_n] = \mathbb{R}[X_1, \ldots, X_n]$)

So $g_i(0, \ldots, 0) > 0$ for each $i = i, \ldots, s$ (i.e. has positive constant term), that means $g_i \in \mathbb{R}[X]$ is a positive unit in $\mathbb{R}[X] \forall i = 1, \ldots, s$.

By Lemma 1.9 (on positive units in power series): $g_i \in \mathbb{R}[X]^2 \forall i = i, \ldots, s$. 

So the preordering $T_S^A$ generated by $S = \{g_1, \ldots, g_s\}$ in the ring $A := \mathbb{R}[X]$ is just $\Sigma \mathbb{R}[X]^2$.

Now using Lemma 1.10 : \( \exists f \in \mathbb{R}[X], f \geq 0 \) on $\mathbb{R}^n$ but $f$ is not a sum of squares in $\mathbb{R}[X]$ (i.e. $f \notin \Sigma \mathbb{R}[X]^2 = T_S^A$).

So clearly $f \notin T_S$ . □ (Proposition 1.2)

Proposition 1.2 that we just proved is just a special case of the following result due to Scheiderer:

**Theorem 1.11.** Let $S$ be a finite subset of $\mathbb{R}[X]$ such that $K_S$ has dimension $\geq 3$. Then \( \exists f \in \mathbb{R}[X]; f \geq 0 \) on $\mathbb{R}^n$ and $f \notin T_S$ .

To prove this result we need:
(1) a reminder about dimension of semi algebraic sets, and
(2) more facts about non singular zeros.

2. ALGEBRAIC INDEPENDENCE

Let $E/F$ be a field extension:

**Definition 2.1.** (1) $a \in E$ is **algebraic** over $F$ if it is a root of some non zero polynomial $f(x) \in F[x]$, otherwise $a$ is a **transcedental** over $F$.

(2) $A = \{a_1, \ldots, a_n\} \subseteq E$ is called **algebraically independent** over $F$ if there is no nonzero polynomial $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ s.t. $f(a_1, \ldots, a_n) = 0$.

In general $A \subseteq E$ is algebraically independent over $F$ if every finite subset of $A$ is algebraic independent over $F$.

(3) A **transcendence base** of $E/F$ is a maximal subset (w.r.t. inclusion) of $E$ which is algebraically independent over $F$.
POSITIVE POLYNOMIALS LECTURE NOTES
(11: 20/05/10)

SALMA KUHLMANN

Contents
1. Algebraic independence and transcendence degree 1
2. Krull Dimension of a ring 2
3. Low Dimension 3

1. ALGEBRAIC INDEPENDENCE AND TRANSCENDENCE DEGREE

Definition 1.1. (Recall) Let $E/F$ be a field extension:

(1) $A \subseteq E$ is called **algebraically independent** over $F$ if $\forall a_1, \ldots, a_n \in A$ there exists no nonzero polynomial $f \in F[x_1, \ldots, x_n]$ s.t. $f(a_1, \ldots, a_n) = 0$.

(2) $A \subseteq E$ is called a **transcendence basis** of $E/F$ if $A$ is a maximal subset (w.r.t. inclusion) of $E$ which is algebraically independent over $F$.

Lemma 1.2. Let $E/F$ be a field extension.

(1) (Steinitz exchange) $S \subseteq E$ is algebraically independent over $F$ iff $\forall s \in S : s$ is transcendental over $F(S - \{s\})$ (the subfield of $E$ generated by $S - \{s\}$).

(2) $S \subseteq E$ is a transcendence base for $E/F$ if $S$ is algebraically independent over $F$ and $E$ is algebraic over $F(S)$.

Proof. Exercise 1 of ÜB 6.

Theorem 1.3. The extension $E/F$ has a transcendence base and any two transcendence bases of $E/F$ have the same cardinality.

Proof. The existence follows by Zorn’s lemma and the second statement uses the Steinitz exchange lemma (above).
Definition 1.4. The cardinality of a transcendence base of $E/F$ is called the transcendence degree of $E/F$, denoted by $\text{trdeg}(E)$ over $F$.

2. KRULL DIMENSION OF A RING

Definition 2.1 Let $A$ be a commutative ring with $1$.

1. A chain of prime ideals of $A$ is of the form $\{0\} \subseteq \mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_k \subseteq \ldots \subseteq A$, where $\mathfrak{p}_i$ are prime ideals of $A$.

2. The Krull dimension of $A$, denoted by $\dim(A)$ is defined to be the maximum $k$ such that there is a chain of prime ideals of length $k$ in $A$, i.e. $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \ldots \subseteq \mathfrak{p}_k$ [dim$(A)$ can be infinite if arbitrary long chains].

Theorem 2.2. Let $F$ be a field and $I$ be any prime ideal in $F[X]$. Then

$$\dim\left(\frac{F[X]}{I}\right) = \text{trdeg}\left(\frac{f \cdot F[X]}{I}\right).$$

Recall 2.3. For $S \subseteq F^n$

$$I(S) = \{f \in F[X] \mid f(\mathbf{x}) = 0, \forall \mathbf{x} \in S\}$$

is the ideal of polynomials vanishing on $S$.

Definition 2.4. Dimension of semi-algebraic sets $\subseteq \mathbb{R}^n$: Let $K \subseteq \mathbb{R}^n$ be a semi-algebraic set. Then

$$\dim(K) := \dim\left(\frac{\mathbb{R}[X]}{I(K)}\right).$$

In the lecture 10 (Proposition 1.2) we have proved the following proposition:

Proposition 2.5. Suppose $n \geq 3$. Let $S = \{g_1, \ldots, g_s\}$ be a finite subset of $\mathbb{R}[X]$ such that $K_S \subseteq \mathbb{R}^n$ and $\text{int}(K_S) \neq \emptyset$. Then there exists $f \in \mathbb{R}[X]$ such that $f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

This is just a special case of the following result due to Scheiderer:

Theorem 2.6. (Scheiderer) (Theorem 1.11 of lecture 10) Let $S$ be a finite subset of $\mathbb{R}[X]$ and $K_S \subseteq \mathbb{R}^n$ s.t. $\dim K_S \geq 3$. Then there exists $f \in \mathbb{R}[X]; f \geq 0$ on $\mathbb{R}^n$ and $f \notin T_S$.

To deduce Proposition 2.5 using Theorem 2.6 it suffices to prove the following lemma:
**Lemma 2.7.** Let $K \subseteq \mathbb{R}^n$ be a semi algebraic subset. Then
\[
\text{int}(K) \neq \emptyset \Rightarrow \dim(K) = n
\]

*Proof.* We have \( \dim(K) = \dim \left( \frac{\mathbb{R}[X]}{I(K)} \right) \), and we claim that \( I(K) = \{0\} \):
\[f \in I(K) \Rightarrow f = 0 \text{ on } K \Rightarrow f = 0 \text{ on } \text{int}(K) \Rightarrow f \text{ vanishes on a nonempty open set} \Rightarrow f \equiv 0 \text{ (by Remark 2.2 of lecture 2)}. \]
So, \( \dim(K) = \dim(\mathbb{R}[X]) = \text{trdeg}(\mathbb{R}(X)) \text{ over } \mathbb{R} = n \quad \blacksquare \)

### 3. LOW DIMENSIONS

**Proposition 3.1.** Let \( n = 2, K_S \subseteq \mathbb{R}^2 \) and \( K_S \) contains a 2-dimensional affine cone. Then \( \exists f \in \mathbb{R}[X, Y]; f \geq 0 \text{ on } \mathbb{R}^2; f \notin T_S \).

**Definition 3.2.** (For \( n = 1 \)) Let \( K \) be a basic closed semi algebraic subset of \( \mathbb{R} \). Then \( K \) is a finite union of intervals.
The natural description \( S \) of \( K \) as basic closed semi algebraic subset is defined as
1. if \( a \in \mathbb{R} \) is the smallest element of \( K \), then take the polynomial \( X - a \in S \)
2. if \( a \in \mathbb{R} \) is the greatest element of \( K \), then take the polynomial \( a - X \in S \)
3. if \( a, b \in K, a < b, (a,b) \cap K = \emptyset \), then take the polynomial \((X-a)(X-b) \in S \)
4. no other polynomial should be in \( S \).

**Proposition 3.3.** Let \( K \subseteq \mathbb{R} \) be a basic closed semi algebraic subset and \( S \) is the natural description of \( K \). Then \( \forall f \in \mathbb{R}[X] : f \geq 0 \text{ on } K \Rightarrow f \in T_S \), i.e. for every basic semi algebraic subset \( K \) of \( \mathbb{R} \), there exists a description \( S \) (namely the natural) so that \( T_S \) is saturated.

**Proposition 3.4.** Let \( K \subseteq \mathbb{R} \) be a non-compact basic semi algebraic subset and \( S' \) be a description of \( K \). Then \( T_{S'} \) is saturated \( \iff S' \supseteq S \) (up to a scalar multiple factor).

**Remark 3.5.** Summarizing:
(1) \( \dim(K_S) \geq 3 \Rightarrow T_S \) is not saturated.

(2) \( \dim(K_S) = 2 \Rightarrow T_S \) can be or cannot be saturated (depending on the geometry of \( K \) and \( S \)).

(3) \( \dim(K_S) = 1 \Rightarrow T_S \) can be or cannot be saturated [but depends on \( K \) and description \( S \) of \( K \), if \( n \geq 2 \)].

After all this discussion about positive polynomials, strictly positive polynomials, we now want to show **Schmüdgen’s Positivstellensatz**:

**Theorem 3.6.** (Schmüdgen’s Positivstellensatz) Let \( S = \{ g_1, \ldots, g_s \} \) be a finite subset of \( \mathbb{R}[X_1, \ldots, X_n] \) and \( K_S \subseteq \mathbb{R}^n \) be a compact basic closed semi algebraic set. And let \( f \in \mathbb{R}[X] \) s.t. \( f > 0 \) on \( K_S \). Then \( f \in T_S \).

**Note** that this holds for every finite description \( S \) of \( K \).

To prove this we first need Representation Theorem (Stone-Krivine, Kadison-Dubois), which will be proved in the next lecture.
POSITIVE POLYNOMIALS LECTURE NOTES
(12: 25/05/10)

SALMA KUHLMANN

Contents

1. Schm"udgen’s Positivstellensatz 1
2. Representation theorem (Stone-Krivine, Kadison-Dubois) 1
3. Preprimes, modules and semi-ordering in rings 3

1. SCHM"UDGEN’S POSITIVSTELLENSATZ

Theorem 1.1. (Recall 3.6 of lecture 11) Let \( S = \{g_1, \ldots, g_s\} \) be a finite subset of \( \mathbb{R}[X_1, \ldots, X_n] \) and \( K_S \subseteq \mathbb{R}^n \) be a compact basic closed semi algebraic set. And let \( f \in \mathbb{R}[X] \) s.t. \( f > 0 \) on \( K_S \). Then \( f \in T_S \).

To prove this we first need Representation Theorem (Stone-Krivine, Kadison-Dubois):

2. REPRESENTATION THEOREM (STONE-KRIVINE, KADISON-DUBOIS)

Let \( A \) be a commutative ring with 1. Let

\[ \chi := \text{Hom}(A, \mathbb{R}) = \{ \alpha \mid \alpha : A \to \mathbb{R}, \alpha \text{ ring homomorphism} \}. \]

Notation 2.1. If \( M \subseteq A \) denote

\[ \chi_M = \{ \alpha \in \chi \mid \alpha(M) \subseteq \mathbb{R}_+ \}. \]

Notation 2.2. For \( a \in A \) define a map

\[ \hat{a} : \chi \to \mathbb{R} \text{ by } \hat{a}(\alpha) := \alpha(a) \]
Remark 2.3. (i) Let $M \subseteq A$, with notations 2.1 and 2.2 we see that
\[
\chi_M := \{ \alpha \in \chi \mid \alpha(M) \subseteq \mathbb{R}_+ \} \\
= \{ \alpha \in \chi \mid \alpha(a) \geq 0, \forall a \in M \} \\
= \{ \alpha \in \chi \mid \hat{a}(\alpha) \geq 0, \forall a \in M \}
\]
So, $\chi_M$ is “the nonnegativity set” of $M$ in $\chi$.

Observation 2.4. $a \in M \Rightarrow \hat{a} \geq 0$ on $\chi_M$, because if $\alpha \in \chi_M$, then $\hat{a}(\alpha) \geq 0$ (by definition).

Conversely, answer the question: for $a \in A$, if $\hat{a} > 0$ on $\chi_M \Rightarrow a \in M$?

Exkurs 2.5. One can view $\chi = \text{Hom}(A, \mathbb{R})$ as a topological subspace of (Sper $A$, spectral topology) as follows:

1. Embedding of $\text{Hom}(A, \mathbb{R})$ in Sper $A$:
   Consider the map defined by
   \[
   \text{Hom}(A, \mathbb{R}) \to \text{Sper } A \\
   \alpha \mapsto P_\alpha := \alpha^{-1}(\mathbb{R}_+),
   \]
   where (recall that) Sper($A$):= \{ $P$ ; $P$ is an ordering of $A$ \}.

   Then
   (i) this map is well defined i.e. $P_\alpha \subseteq A$ is an ordering.
   (ii) this map is injective : $\alpha \neq \beta \Rightarrow P_\alpha \neq P_\beta$.
   (iii) support($P_\alpha$) = ker $\alpha$.

2. Topology on $\chi$:
   Endow $\chi$ with a topology : for $a \in A$
   \[
   \{u(\hat{a}) = \{ \alpha \in \chi \mid \hat{a}(\alpha) > 0 \}; a \in A\}
   \]
   is a sub-basis of open sets. Then
   (iv) for $a \in A$, the map $\hat{a} : \chi \to \mathbb{R}$ is continuos in this topology.
   (v) in fact this topology on $\chi$ is the weakest topology on $\chi$ for which $\hat{a}$ is continuous for all $a \in A$,
   i.e. if $\tau$ is any other topology on $\chi$ which makes all these maps $\hat{a}$ (for $a \in A$) continuous then $\tau$ has more open sets than this weakest topology (i.e. $u(\hat{a})$ lies in $\tau$).
(vi) this topology is also the topology induced on $\chi$ via the embedding $\alpha \mapsto P_\alpha$ giving Sper $A$ the spectral topology [just use the fact that $\hat{a}(\alpha) > 0 \iff a \notin -P_\alpha \iff a >_{P_\alpha} 0$. Spectral topology: $u(a) = \{ P : a \notin -P \} = \{ P \mid a >_P 0 \}$.]

Now we are back to the question (in Observation 2.4): for $a \in A$, does $\hat{a} > 0$ on $\chi_M \Rightarrow a \in M$ ?

Yes under additional assumptions on the subset $M$ that we shall now study:

3. PREPRIMES, MODULES AND SEMI-ORDERINGS IN RINGS

Let $A$ be a commutative ring with 1 and $\mathbb{Q} \subseteq A$. Concept of preordering generalizes in two directions:

(i) Preprimes

(ii) Modules (special case: quadratic modules)

**Definitions 3.1.**

1. A **preprime** is a subset $T$ of $A$ such that
   $$T + T \subseteq T; \quad TT \subseteq T; \quad \mathbb{Q}_+ \subseteq T.$$

2. Let $T$ be a preprime of $A$. $M \subseteq A$ is a **$T$-module** if
   $$M + M \subseteq M; \quad TM \subseteq M; \quad 1 \in M \text{ (i.e. } T \subseteq M).$$
   [Note that in particular, a preprime $T$ is a $T$-module.]

3. A preprime $T$ of $A$ is said to be **generating** if $T - T = A$.
   [Note that if $T$ is any preprime then $T - T$ is already a subring of $A$ because
   $$(t_1 - t_2) + (t_3 - t_4) = (t_1 + t_3) - (t_2 + t_4)$$
   $$(t_1 - t_2)(t_3 - t_4) = (t_1t_3 + t_2t_4) - (t_1t_4 + t_2t_3).$$]

**Proposition 3.2.** Every preordering $T$ of $A$ is a generating preprime.

**Proof.** (i) For $\frac{m}{n} \in \mathbb{Q} : \frac{m}{n} = \left(\frac{1}{n}\right)^2 mn = \frac{1}{n^2} + \ldots + \frac{1}{n^2}$
   (mn-times)
   so $\mathbb{Q}_+ \subseteq T$. 


(ii) For $a \in A$, $a = \left( \frac{1 + a}{2} \right)^2 - \left( \frac{1 - a}{2} \right)^2$.

So $A = T - T$. $\square$

Definitions 3.3. (1) A quadratic module is a $T$-module over the preprime $T = \sum A^2$.

(2) A $T$-module $M$ is proper if $(-1) \not\in M$.

(3) A semi-ordering $M$ is a quadratic module such that moreover

$M \cup (-M) = A$; $M \cap (-M) = p$ is a prime ideal in $A$.

Proposition 3.4.
(a) Suppose $T$ is a generating preprime and $M$ is a maximal proper $T$-module, then $M \cup (-M) = A$.

(b) Suppose $T$ is a preordering and $M$ a maximal proper $T$-module then $p = M \cap (-M)$ is a prime ideal.

(c) Therefore: if $T$ is a preordering and $M$ is a maximal proper $T$-module then $M$ is a semi-ordering.

Proof. Similar to proof in the preordering case
(a) Let $a \in A$, $a \not\in M \cup (-M)$.

By maximality of $M$, we have:

$-1 \in (M + aT)$ and $-1 \in (M - aT)$.

Therefore, $-1 = s_1 + at_1$ and $-1 = s_2 - at_2$; for some $s_1, s_2 \in M$ and $t_1, t_2 \in T$.

This implies $-at_1 = 1 + s_1$ and $at_2 = 1 + s_2$.

So $-at_1t_2 = t_2 + s_1t_2$ and $at_2t_1 = t_1 + s_2t_1$.

So $0 = t_2 + t_1 + s_1t_2 + t_1s_2$.

So $-t_1 = t_2 + s_1t_2 + t_1s_2 \in M$.

Now since $T$ is generating, so pick $t_3, t_4 \in T$ such that $a = t_3 - t_4$, then

$-1 = s_1 + at_1 = s_1 + (t_3 - t_4)t_1 = s_1 + t_3s_2 + t_4(-s_1) \in M$. This is a contradiction.

(b) $p = M \cap (-M)$.

Clearly $p \cup p \subseteq p$, $-p = p$, $0 \in p$, $Tp \subseteq p$.

Since $A = T - T \Rightarrow Ap \subseteq p$. Thus $p$ is an ideal clearly.

So far we have only used that $T$ is a generating preprime, to show that $p$ is a prime ideal we need that $T$ is preordering:
Suppose $ab \in p, a \notin p$. Without loss of generality assume $a \notin M$.

Now this implies: $-1 \in M + aT$, so $-1 = s + at$; $s \in M, t \in T$

$\Rightarrow -b^2 = sb^2 + ab^2t \in M + p \subseteq M$.

Now since $b^2 \in T \subseteq M$, this implies $b^2 \in M \cap -M = p$.

So we are reduced to showing: $b^2 \in p \Rightarrow b \in p$.

Suppose $b^2 \in p, b \notin p$. Without loss of generality $b \notin M$.

Thus $-1 = s + bt$, for some $s \in M$ and $t \in T$.

So $1 + 2s + s^2 = (1 + s)^2 = (-bt)^2 = b^2t^2 \in p = M \cap -M$.

Thus $-1 = 2s + s^2 + (-b^2t^2) \in M$, a contradiction since $-1 \notin M$.

(c) Clear.

Thus $-1 = 2s + s^2 + (-b^2t^2) \in M$, a contradiction since $-1 \notin M$.

(c) Clear.

Our next aim is to show that under the additional assumption: “$M$ is archime-
1. ARCHIMEDEAN MODULES

Let $A$ be a commutative ring, $Q \subseteq A$, $T$ a preprime.

**Definition 1.1.** Let $M$ a $T$-module. $M$ is **archimedean** if:

$$\forall a \in A, \exists N \geq 1, N \in \mathbb{Z}^+ \text{ s.t. } N + a, N - a \in M.$$  

**Proposition 1.2.** Let $T$ be a generating preprime, $M$ a maximal proper $T$-module. Assume that $M$ is archimedean. Then $\exists \alpha \in \text{Hom}(A, \mathbb{R})$ s.t. $M = \alpha^{-1}(\mathbb{R}^+)$ = $P_\alpha$.  

(In particular, $M$ is an ordering, not just a semi-ordering.)

**Proof.** Let $a \in A$, define:

$\text{cut} (a) = \{ r \in Q \mid r - a \in M \}$, this is an **upper cut** in $Q$ (i.e. final segment of $Q$).

**Claim 1:** $\text{cut}(a) \neq \emptyset$ and $Q \setminus (\text{cut}(a)) = L(a) \neq \emptyset$, where $L(a)$ is a **lower cut** in $Q$.

Proof of claim 1. Since $M$ is archimedean $\exists n \geq 1 \text{ s.t. } n - a \in M$, so $\text{cut}(a) \neq \emptyset$.

Also $\exists m \geq 1 \text{ s.t. } (m + a) \in M$.

If $-(m + 1) - a \in M$, then adding we get $-1 \in M$, a contradiction (since $M$ is proper). So we have $-(m + 1) - a \notin M$, which $\Rightarrow -(m + 1) \in Q \setminus (\text{cut}(a)) = L(a)$.  

$\square$(claim 1)

Now define a map $\alpha : A \rightarrow \mathbb{R}$ by

$$\alpha(a) := \inf (\text{cut}(a))$$
\( \alpha \) is well-defined.

**Claim 2:** \( \alpha(1) = 1, \alpha(M) \subseteq \mathbb{R}_+; \alpha(a \pm b) = \alpha(a) \pm \alpha(b) \forall a, b \in A \) and \( \alpha(tb) = \alpha(t) \alpha(b) \forall t \in T, b \in A \).

This is left as an exercise.

**Claim 3:** \( \alpha(ab) = \alpha(a) \alpha(b) \forall a, b \in A \)

Proof of claim 3. \( T \) generating \( \Rightarrow a = t_1 - t_2, t_1, t_2 \in T \)

so, \( \alpha(ab) = \alpha(t_1b - t_2b) = \alpha(t_1a) - \alpha(t_2b) \)

\[ = \alpha(t_1)\alpha(b) - \alpha(t_2)\alpha(b) \] [by claim 2]

\[ = (\alpha(t_1) - \alpha(t_2))\alpha(b) = \alpha(t_1 - t_2)\alpha(b) = \alpha(a)\alpha(b). \]

\( \square \) (claim 3)

**Claim 4:** \( \alpha^{-1}(\mathbb{R}_+) = M \)

Proof of claim 4. By Claim 2, \( M \subseteq \alpha^{-1}(\mathbb{R}_+) \)

so, by maximality of \( M \) and since \( P_\alpha = \alpha^{-1}(\mathbb{R}_+) \) is an ordering it follows that \( M = \alpha^{-1}(\mathbb{R}_+) \).

\( \square \)

**Corollary 1.3.** Let \( A \) be a commutative ring with 1, \( T \) an archimedean preprime, \( M \) a \( T \)-module, \( -1 \notin M \) (i.e. \( M \) proper \( T \)-module). Then \( \chi_M \neq \emptyset \).

**Proof.** Since \( T \) is archimedean, \( T \) is generating (because \( a = (n + a) - n \), for \( a \in A \) and \( M \) is a proper archimedean module (archimedean module because for an archimedean preprime \( T \), every \( T \)-module is also archimedean). By Zorn’s lemma extend \( M \) to a maximal proper archimedean module \( Q \). Apply Proposition 1.2 to \( Q \) to get \( \alpha \in \text{Hom}(A, \mathbb{R}) \) such that \( Q = \alpha^{-1}(\mathbb{R}_+) \). This implies \( M \subseteq \alpha^{-1}(\mathbb{R}_+) \).

So, \( \alpha \in \chi_M \), which implies \( \Rightarrow \chi_M \neq \emptyset \). \( \square \)

2. REPRESENTATION THEOREM (STONE-KRIVINE, KADISON-DUBOIS)

The following corollary (to Proposition 1.2 and Corollary 1.3) answers the question raised in 2.4 of lecture 12:

**Corollary 2.1.** (Stone-Krivine, Kadison-Dubois) Let \( A \) be a commutative ring, \( T \) an archimedean preprime in \( A \), \( M \) a proper \( T \)-module. Let \( a \in A \) and

\[ \hat{a} : \chi \to \mathbb{R} \] defined by

\[ \hat{a}(\alpha) := \alpha(a) \]

If \( \hat{a} > 0 \) on \( \chi_M \), then \( a \in M \).
Proof. Assume  \( \hat{a} > 0 \) on \( \chi_M \), i.e. \( \hat{a}(\alpha) > 0 \ \forall \ \alpha \in \chi_M \).

To show: \( a \in M \)

- Consider \( M_1 := M = aT \)

  Since \( \alpha(a) > 0 \ \forall \ \alpha \in \chi_M \), we have \( \chi_{M_1} = \emptyset \) [because if \( \alpha \in \chi_{M_1} \), then \( \alpha(M_1) \subseteq \mathbb{R}^+ \). So, \( \alpha(-a) = -\alpha(a) \geq 0 \). So, \( \alpha(a) \leq 0 \), but \( \alpha \in \chi_M \) so \( \alpha(a) > 0 \), a contradiction].

  So (since \( M_1 \) is an archimedean \( T \)-module), we can apply Corollary 1.3 to \( M_1 \) to deduce that \( -1 \in M_1 \).

  Write \( -1 = s - at \), \( s, t \in T \)

  \( \Rightarrow at - 1 = s \in M \) \( \star \)

- Consider \( \Sigma := \{ r \in \mathbb{Q} \mid r + a \in M \} \)

  We claim that: \( \exists \rho \in \Sigma; \rho < 0 \)

  Once the claim is established we are done (with the proof of corollary) because

  \[ a = \left( a + \rho \right) + \left( -\rho \right) \in M. \]

  Proof of the claim: First observe that \( \Sigma \neq \emptyset \) (since \( \exists n \geq 1 \) s.t \( n + a \in T \subseteq M \), so \( n \in \Sigma \)).

  Now fix \( r \in \Sigma \), \( r \geq 0 \) and fix an integer \( k \geq 1 \) s.t \( (k - t) \in T \)

  Write: \( kr - 1 + ka = \left( k - t \right) \left( r + a \right) + \left( at - 1 \right) + rt \in M \)

  Multiplying by \( \frac{1}{k} \), we get

  \[ \left( r - \frac{1}{k} \right) + a \in M, \text{ i.e. } \left( r - \frac{1}{k} \right) \in \Sigma \]

  Repeating we eventually find \( \rho \in \Sigma, \rho < 0 \). \( \square \)

Note 2.2. For a quadratic module \( M \subseteq \mathbb{R}[X] \), set

\[ K_M := \{ x \in \mathbb{R}^n \mid g(x) \geq 0 \ \forall \ g \in M \}. \]

Note that if \( M = M_S \) with \( S = \{ g_1, \ldots, g_s \} \), then \( K_S = K_M \).

We have the following corollaries to Corollary 2.1. (Stone-Krivine, Kadison-Dubois):
Corollary 2.3. (Putinar’s Archimedean Positivstellensatz) Let $M \subseteq \mathbb{R}[X]$ be an archimedean quadratic module. Then for each $f \in \mathbb{R}[X]$:

$$f > 0 \text{ on } K_M \Rightarrow f \in M.$$ 

Corollary 2.4. Let $A = \mathbb{R}[X]$ and $S = \{g_1, \ldots, g_s\}$. Assume that the finitely generated preordering $T_S$ is archimedean. Then for all $f \in A$:

$$f > 0 \text{ on } K_S \Rightarrow f \in T_S.$$ 

Remark 2.5.

1. To apply the corollary we need a criterion to determine when a preordering (quadratic module) is archimedean.

2. $T_S$ is archimedean $\Rightarrow$ for $f = \sum X_i^2$ : $\exists N$ s.t. $N - f = N - \sum X_i^2 \in T_S$

   $\Rightarrow N - \sum X_i^2 \geq 0$ on $K_S$.

   $\Rightarrow K_S$ is bounded. Also $K_S$ is closed.

   So $T_S$ is archimedean implies $K_S$ is compact.
POSITIVE POLYNOMIALS LECTURE NOTES
(14: 01/06/10)

SALMA KUHLMANN

Contents
1. Rings of bounded elements 1
2. Schmüdgen’s Positivstellensatz 2

1. RINGS OF BOUNDED ELEMENTS

Let $A$ be a commutative ring with 1, $\mathbb{Q} \subseteq A$ and $M$ be a quadratic module $\subseteq A$.

**Definition 1.1.** Consider

$$B_M = \{ a \in A \mid \exists n \in \mathbb{N} \text{ s.t. } n + a \text{ and } n - a \in M \}.$$ 

$B_M$ is called the *ring of bounded elements*, which are bounded by $M$.

**Proposition 1.2.**

1. $M$ is an archimedean module of $A$ iff $B_M = A$.
2. $B_M$ is a subring of $A$.
3. $\forall a \in A, a^2 \in B_M \Rightarrow a \in B_M$.
4. More generally, $\forall a_1, \ldots, a_k \in A, \sum_{i=1}^k a_i^2 \in B_M \Rightarrow a_i \in B_M \forall i = 1, \ldots, k$.

**Proof.** (1) Clear.

(2) Clearly $\mathbb{Q} \subseteq B_M$ and $B_M$ is an additive subgroup of $A$.

To show: $a, b \in B_M \Rightarrow ab \in B_M$

Using the identity

$$ab = \frac{1}{4}[(a + b)^2 - (a - b)^2],$$
we see that in order to show that $B_M$ is closed under multiplication it is sufficient to show that: \( \forall a \in A : a \in B_M \Rightarrow a^2 \in B_M \).

Let $a \in B_M$. Then $n \pm a \in M$ for some $n \in \mathbb{N}$. Now $n^2 + a^2 \in M$.

Also \( 2n(n^2 - a^2) = (n^2 - a^2)((n + a) + (n - a)) \)

So, \( (n^2 - a^2) = \frac{1}{2n}[(n + a)(n^2 - a^2) + (n - a)(n^2 - a^2)] \)

\( = \frac{1}{2n}[(n + a)^2(n - a) + (n - a)^2(n + a)] \in M. \)

So $(n^2 + a^2)$ and $(n^2 - a^2)$ both $\in M$. So by definition $a^2 \in B_M$. \( \square \) (2)

(3) Assume $a^2 \in B_M$. Say $n - a^2 \in M$, for $n \geq 1, n \in \mathbb{N}$, then use the identity:

\( (n \pm a) = \frac{1}{2}[(n - 1) + (n - a^2) + (a \pm 1)^2] \in M. \)

So, $a \in B_M$. \( \square \) (3)

(4) If $\sum a_i^2 \in B_M$, Say $(n - \sum a_i^2) \in M$, then

\( (n - a_i^2) = (n - \sum a_i^2) + \sum_{j \neq i} a_j^2 \in M. \)

So, $a_i^2 \in B_M$ and so by (3), $a_i \in B_M$. \( \square \) (4)

**Corollary 1.3.** Let $M$ be a quadratic module of $\mathbb{R}[X]$. Then $M$ is archimedean iff there exists $N \in \mathbb{N}$ such that

\[ N - \sum_{i=1}^{n} X_i^2 \in M \]

**Proof.** ($\Rightarrow$) Clear.

($\Leftarrow$) First note that $\mathbb{R}_+ \subseteq M$ so, $\mathbb{R} \subseteq B_M$ ($B_M$ subring).

Also $N - \sum_{i=1}^{n} X_i^2$ and $N + \sum_{i=1}^{n} X_i^2 \in M$. Therefore by definition $\sum_{i=1}^{n} X_i^2 \in B_M$.

So (by Proposition 1.2) $X_1, \ldots, X_n \in B_M$. This implies $\mathbb{R}[X_1, \ldots, X_n] \subseteq B_M$ and so $M$ is archimedean. \( \square \)

2. SCHMÜDGEN’S POSITIVSTELLENSATZ

**Theorem 2.1.** Let $S = \{g_1, \ldots, g_s\} \subseteq \mathbb{R}[X]$. Assume that $K = K_S = \{x \mid g_i(x) \geq 0\}$ is compact. Then there exists $N \in \mathbb{N}$ such that

\[ N - \sum_{i=1}^{n} X_i^2 \in T_S = T. \]
In particular $T_S$ is an archimedean preordering (by Corollary 1.3) and thus $\forall f \in \mathbb{R}[X]: f > 0$ on $K_S \Rightarrow f \in T_S$.

**Proof.** [Reference: Dissertation, Thorsten Wörmann]

- $K$ compact $\Rightarrow$ $K$ bounded $\Rightarrow \exists k \in \mathbb{N}$ such that $(k - \sum_{i=1}^{n} X_i^2) > 0$ on $K$.

- By applying the Positivstellensatz to above we get: $\exists p, q \in T_S$ such that $p(k - \sum_{i=1}^{n} X_i^2) = 1 + q$. So, $p(k - \sum_{i=1}^{n} X_i^2)^2 = (1 + q)(k - \sum_{i=1}^{n} X_i^2)$. So,

$(1 + q)(k - \sum_{i=1}^{n} X_i^2) \in T_S$.

- Set $T' = T + (k - \sum_{i=1}^{n} X_i^2)T$. By Corollary 1.3, $T'$ is an archimedean preordering. Therefore $\exists m \in \mathbb{N}$ such that $(m - q) \in T'$; say: $m - q = t_1 + t_2(k - \sum_{i=1}^{n} X_i^2)$ for some $t_1, t_2 \in T$.

- So, $(m - q)(1 + q) = t_1(1 + q) + t_2(k - \sum_{i=1}^{n} X_i^2)(1 + q) \in T_S$. So $(m - q)(1 + q) \in T_S$.

- Adding

$(m - q)(1 + q) = mq - q^2 + m - q \in T_S$, \hspace{1cm} (1)

$\left(\frac{m}{2} - q\right)^2 = \frac{m^2}{4} + q^2 - mq \in T_S$. \hspace{1cm} (2)

yields

$\left(m + \frac{m^2}{4} - q\right) \in T_S$. \hspace{1cm} (3)

- Multiplying L.H.S. of (3) by $k \in T_S$, and adding $(k - \sum_{i=1}^{n} X_i^2)(1 + q) \in T_S$

and $q\left(\sum_{i=1}^{n} X_i^2\right) \in T_S$, yields

$k\left(m + \frac{m^2}{4} - q\right) + (k - \sum_{i=1}^{n} X_i^2)(1 + q) + q\left(\sum_{i=1}^{n} X_i^2\right) \in T_S$.
i.e. \( km + k \frac{m^2}{4} + k - \sum_{i=1}^{n} X_i^2 \in T_S \)

i.e. \( k (\frac{m}{2} + 1)^2 - \sum_{i=1}^{n} X_i^2 \in T_S \)

Set \( N := k (\frac{m}{2} + 1)^2 \).

(End of Schm"udgen’s Positivstellensatz)

2.2. Final Remarks on Schmüdgen’s Positivstellensatz (SPSS):

1. **Corollary (Schmüdgen’s Nichtnegativstellensatz):**
   
   \( f \geq 0 \) on \( K_S \Rightarrow \forall \epsilon \text{ real}, \epsilon > 0 : f + \epsilon \in T_S \).

2. **SPSS fails in general if we drop the assumption that “K is compact”.**

   For example:
   
   (i) Consider \( n = 1, S = \{X^3\} \), then \( K_S = [0, \infty) \) (noncompact). Take \( f = X + 1 \). Then \( f > 0 \) on \( K_S \). **Claim:** \( f \notin T_S \), indeed elements of \( T_S \) have the form \( t_0 + t_1 X^3 \), where \( t_0, t_1 \in \sum \mathbb{R}[X]^2 \). We have shown before at the beginning of this course (in 2.4 of lecture 2) that non zero elements of this preordering either have even degree or odd degree \( \geq 3 \).

   (ii) Consider \( n \geq 2, S = \emptyset \), then \( K_S = \mathbb{R}^n \). Take strictly positive versions of the Motzkin polynomial
   
   \[ m(X_1, X_2) := 1 - X_1^2 X_2^2 + X_1^2 X_2^4 + X_1^4 X_2^2, \]
   
   i.e. \( m_\epsilon := m(X_1, X_2) + \epsilon ; \epsilon \in \mathbb{R}_+ \). Then \( m_\epsilon > 0 \) on \( K_S = \mathbb{R}^2 \), and it is easy to show that \( m_\epsilon \notin T_S = \sum \mathbb{R}[X]^2 \forall \epsilon \in \mathbb{R}_+ \).

3. **SPSS fails in general for a quadratic module instead of a preordering.** [Mihaei Putinar’s question answered by Jacobi + Prestel in Dissertation of T. Jacobi (Konstanz)]

4. **SPSS fails in general if the condition “\( f > 0 \) on \( K_S \)” is replaced by “\( f \geq 0 \) on \( K_S \)”**.

   Example (Stengle): Consider \( n = 1, S = \{(1 - X^2)^3\}, K_S = [-1, 1] \) compact.
   
   Take \( f := 1 - X^2 \geq 0 \) on \( K_S \) but \( 1 - X^2 \notin T_S \). (This example has already been considered at the beginning of this course in 2.4 of lecture 2).
5. PSS holds for any real closed field but not SPSS:

Example: Let $R$ be a non archimedean real closed field. Take $n = 1, S = \{(1 - X^2)^3\}$, then $K_S = [-1, 1]_R = \{x \in R \mid -1 \leq x \leq 1\}$. Take $f = 1 + t - X^2$, where $t \in R^{>0}$ is an infinitesimal element (i.e. $0 < t < \epsilon$, for every positive rational $\epsilon$). Then $f > 0$ on $K_S$. We claim that $f \notin T_S$.

Let $v$ be the natural valuation on $R$. So $v(t) > 0$ for $t > 0$. Now suppose for a contradiction that $f \in T_S$. Then $1 + t - X^2 = f = t_0 + t_1(1 - X^2)^3; t_0, t_1 \in \sum R[X]^2$ (1)

Let $t_i = \sum f_{ij}^2$; for $i = 0, 1$ and $f_{ij} \in R[X]$.

Let $s \in R$ be the coefficient of the lowest value appearing in the $f_{ij}$, i.e. $v(s) = \min\{v(a) \mid a \text{ is coefficient of some } f_{ij}\}$.

Case I. if $v(s) \geq 0$, then applying the residue map $\left(\theta_v \rightarrow \overline{\theta_v} := \frac{\theta_v}{I_v}\right)$; defined by $x \mapsto \overline{x}$, where $\theta_v$ is the valuation ring; to (1), we obtain

$$1 - X^2 = \overline{t_0} + \overline{t_1}(1 - X^2)^3$$

and since $\overline{t} = \sum \overline{f_{ij}^2} \in \sum \overline{R[X]^2}; i = 0, 1$; we get a contradiction to Example 2.4 (ii) of Lecture 2.

Case II. if $v(s) < 0$. Dividing $f$ by $s^2$ and applying the residue map we obtain

$0 = \overline{\frac{t_0}{s^2}} + \overline{\frac{t_1}{s^2}}(1 - X^2)^3$

(Note that $v(s^2) = 2v(s) = \min\{v(a)\}$; $a$ is coefficient of some $f_{ij}^2$, i.e. $v(s^2) \leq v(a)$ for any coefficient $a$, so $\frac{f_{ij}^2}{s^2}$ has coefficients with value $\geq 0$.)

So we obtain

$$0 = \overline{t_0} + \overline{t_1}(1 - X^2)^3$$

with $\overline{t_0}, \overline{t_1} \in \sum \overline{R[X]^2}$ not both zero.

Since $\overline{t_0}, \overline{t_1}$ have only finitely many common roots in $\overline{R}$ and $1 - X^2 > 0$ on the finite set $(-1, 1)$, this is impossible. \hfill \Box (claim)

6. SPSS holds over archimedean real closed fields.
1. Schmüdgen’s Nichtnegativstellensatz

1.1. Schmüdgen’s Nichtnegativstellensatz (Recall 2.2.1 of lecture 14): Let $K_S$ be a compact basic closed semi algebraic set and $f \in \mathbb{R}[X]$. Then

$f \geq 0$ on $K_S \Rightarrow \forall \epsilon > 0 : f + \epsilon \in T_S$.

Corollary 1.2. Let $K = K_S$ be a compact basic closed semi algebraic set and $L \neq 0$ be a linear functional $L : \mathbb{R}[X] \rightarrow \mathbb{R}$ with $L(r) = r \forall r \in \mathbb{R}$. Then

$L(T_S) \geq 0 \Rightarrow L(\text{Psd}(K_S)) \geq 0$

(i.e. $L(f) \geq 0 \forall f \in T_S$) (i.e. $L(f) \geq 0 \forall f \geq 0$ on $K_S$).

Proof. W.l.o.g. $L(1) = 1, L \neq 0$. Let $f \in \text{Psd}(K_S)$ and assume $L(T_S) \geq 0$,

To show: $L(f) \geq 0$

By 1.1, $\forall \epsilon > 0 : f + \epsilon \in T_S$

So, $L(f + \epsilon) \geq 0$ i.e. $L(f) \geq -\epsilon \forall \epsilon > 0$ real

$\Rightarrow L(f) \geq 0$. □

We shall now relate this to the problem of representation of linear functionals via integration along measures (i.e. $\int d\mu$).
2. APPLICATION OF SPSS TO THE MOMENT PROBLEM

Let $X$ be a Hausdorff topological space.

**Definition 2.1.** $X$ is **locally compact** if $\forall \ x \in X \ \exists \ \text{open } U \in X \ s.t. \ x \in U$ and $\bar{U}$ (closure) is compact.

**Notation 2.2.** $\mathcal{B}(X) : = \text{set of Borel measurable sets in } X = \text{the smallest family of subsets of } X \text{ containing all compact subsets of } X, \text{ closed under finite } \bigcup, \text{ set theoretic difference } A \setminus B \text{ and countable } \bigcap$.

**Definition 2.3.** A **Borel measure** $\mu$ on $X$ is a positive measure on $X$ s.t. every set in $\mathcal{B}(X)$ is measurable. We also require our measure to be **regular** i.e. $\forall B \in \mathcal{B}(X)$ and $\forall \epsilon > 0 \ \exists \ K, \ U \in \mathcal{B}(X), \ K \text{ compact, } U \text{ open s.t. } K \subseteq B \subseteq U$ and $\mu(K) + \epsilon \geq \mu(B) \geq \mu(U) - \epsilon$.

**2.4. Moment problem** is the following:
Given a closed set $K \subseteq \mathbb{R}^n$ and a linear functional $L : \mathbb{R}[X] \rightarrow \mathbb{R}$

**Question:**

when does $\exists$ a Borel measure $\mu$ on $K$ s.t. $\forall f \in \mathbb{R}[X] : L(f) = \int f \, d\mu$ ? (1)

**Necessary condition for (1):** $\forall f \in \mathbb{R}[X], f \geq 0 \text{ on } K \Rightarrow L(f) \geq 0$ (2)

in other words: $L(\text{Psd}(K)) \geq 0$ (3)

Is this necessary condition also sufficient?
The answer is YES.

**Theorem 2.5.** (Haviland) Given $K \subseteq \mathbb{R}^n$ closed and $L : \mathbb{R}[X] \rightarrow \mathbb{R}$ a linear functional with $L(1) > 0$:

$\exists$ $\mu$ as in (1) iff $\forall f \in \mathbb{R}[X] : L(f) \geq 0 \text{ if } f \geq 0 \text{ on } K$,
i.e. (1) $\iff$ (2) $\iff$ (3).

We shall prove Haviland’s Theorem later. For now we shall deduce a corollary to SPSS.
Corollary 2.6. Let \( K_S = \{ x \mid g_i(x) \geq 0; i = 1, \ldots, s \} \subset \mathbb{R}^n \) be a basic closed semi-algebraic set and compact, \( L : \mathbb{R}[X] \rightarrow \mathbb{R} \) a linear functional with \( L(1) > 0 \). If \( L(T_S) \geq 0 \), then \( \exists \mu \) positive Borel measure on \( K \) s.t. \( L(f) = \int_K f \, d\mu \) \( \forall f \in \mathbb{R}[X] \).

Remark 2.7. Let \( S = \{ g_1, \ldots, g_s \} \).

1. \( L(T_S) \geq 0 \) can be written as
   \[
   L(h^e_1 \cdots g^e_s) \geq 0 \forall h \in \mathbb{R}[X], e_1, \ldots, e_s \in \{0, 1\}.
   \]

2. Compare Haviland to Schm"udgen’s moment problem, for compact \( K_S \): we do not need to check \( L(\text{Psd}(K_S)) \geq 0 \) we only need to check \( L(T_S) \geq 0 \).

3. Reformulation of question (1) (in 2.4) in terms of moment sequences:
   Let \( L : \mathbb{R}[X] \rightarrow \mathbb{R} \), with \( L(1) = 1 \). Consider \( \{ X^\alpha = X_1^{a_1} \cdots X_n^{a_n}; \alpha \in \mathbb{N}^n \} \) a monomial basis for \( \mathbb{R}[X] \). So \( L \) is completely determined by the (multi)sequence of real numbers \( \tau(\alpha) := L(X^\alpha) ; \alpha = (a_1, \ldots, a_n) \in \mathbb{N}^n \) (i.e. \( \tau : \mathbb{N}^n \rightarrow \mathbb{R} \) is a function) and conversely, every such sequence determines a linear functional \( L : \mathbb{R}[X] \rightarrow \mathbb{R} \):

   \[
   L(\sum_{\alpha} a_\alpha X^\alpha) := \sum_{\alpha} a_\alpha L(X^\alpha).
   \]

So, (1) (in 2.4) can be reformulated as:

Given \( K \subset \mathbb{R}^n \) closed, and a multisequence \( \tau(\alpha) = \tau_\alpha : \mathbb{N}^n \rightarrow \mathbb{R} \) of real numbers, \( \exists \mu \) positive borel measure on \( K \) s.t. \( \int_K X^\alpha \, d\mu = \tau_\alpha \) for all \( \alpha \in \mathbb{N}^n \) ?

Definition 2.8. A function \( \tau : \mathbb{N}^n \rightarrow \mathbb{R} \) is a \( K \)-moment sequence if \( \exists \mu \) positive borel measure on \( K \) s.t. \( \tau(\alpha) = \int_K X^\alpha \, d\mu \) for all \( \alpha \in \mathbb{N}^n \)

So (1) can be reformulated as: given \( K \) and a function \( \tau : \mathbb{N}^n \rightarrow \mathbb{R} \), when is \( \tau \) a \( K \)-moment sequence?

Definition 2.9. A function \( \tau : (\mathbb{Z}_+)^n \rightarrow \mathbb{R} \) is called \textit{psd} if

\[
\sum_{i,j=1}^m \tau(k_i + k_j) \, c_i \, c_j \geq 0,
\]

for \( m \geq 1 \), arbitrary distinct \( k_1, \ldots, k_m \in (\mathbb{Z}_+)^n ; c_1, \ldots, c_m \in \mathbb{R} \).
Definition 2.10. Given $\tau : (\mathbb{Z}_+)^n \rightarrow \mathbb{R}$ a function and a fixed polynomial $g(X) = \sum_{\ell \in \mathbb{Z}_+^n} a_\ell X^\ell \in \mathbb{R}[X]$. Define a new function $g(E)_\tau : (\mathbb{Z}_+)^n \rightarrow \mathbb{R}$ by

$$g(E)_\tau(l) := \sum_{\ell \in \mathbb{Z}_+^n} a_\ell \tau(k + l); \text{ for any } l \in (\mathbb{Z}_+)^n.$$

Lemma 2.11. Let $L : \mathbb{R}[X] \rightarrow \mathbb{R}$ be a linear functional and denote by

$$\tau : (\mathbb{Z}_+)^n \rightarrow \mathbb{R}$$

the corresponding multisequence (i.e. $\tau(k) := L(X^k) \forall k \in (\mathbb{Z}_+)^n$).

Fix $g \in \mathbb{R}[X], \ g(X) = \sum_{\ell \in \mathbb{Z}_+^n} a_\ell X^\ell \in \mathbb{R}[X]$. Then $L(h^2 g) \geq 0$ for all $h \in \mathbb{R}[X]$ if and only if the multisequence $g(E)_\tau$ is psd.
1. Application of Schmüdgen’s Positivstellensatz to the moment problem

2. Schmüdgen’s nichtnegativstellensatz and Hankel matrices

3. Finite solvability of the $K$-Moment Problem

4. Haviland’s Theorem

1. APPLICATION OF SPSS TO THE MOMENT PROBLEM (continued)

**Lemma 1.1.** (Lemma 2.11 of last lecture) Let $L : \mathbb{R}[X] \rightarrow \mathbb{R}$ be a linear functional and denote by

$$\tau : (\mathbb{Z}_+)^n \rightarrow \mathbb{R}$$

the corresponding multisequence (i.e. $\tau(k) := L(X^k) \forall k \in (\mathbb{Z}_+)^n$).

Fix $g \in \mathbb{R}[X]$, $g(X) = \sum_{k \in \mathbb{Z}_+^n} a_k X^k \in \mathbb{R}[X]$. Then $L(h^2 g) \geq 0$ for all $h \in \mathbb{R}[X]$ if and only if the multisequence $g(E)_\tau$ is psd.

**Proof.** Compute:

1. $L(X^l g) = \sum_{k \in \mathbb{Z}_+^n} a_k \tau(k + l) = g(E)_\tau(l); \text{ for all } l \in (\mathbb{Z}_+)^n.$

Thus if $h = \sum c_i X^{k_i} \in \mathbb{R}[X]$ then $h^2 = \sum_{i,j} c_i c_j X^{k_i + k_j}.$

2. So, $L(h^2 g) = L\left( \sum_{i,j} c_i c_j X^{k_i + k_j} g \right) = \sum_{i,j} c_i c_j L(X^{k_i + k_j} g) = \sum_{i,j} g(E)_\tau(k_i + k_j)c_i c_j.$

$\square$

1
Theorem 1.2. (Schmüdgen’s NNSS) (Reformulation in terms of moment sequences) Let $K = K_S$ compact, $S = \{g_1, \ldots, g_s\}$ and $\tau : (\mathbb{Z}^+)^n \to \mathbb{R}$ be a given multisequence. Then $\tau$ is a $K$-moment sequence if and only if the multisequences $(g_1^{e_1} \cdots g_s^{e_s})(E)_\tau : (\mathbb{Z}^+)^n \to \mathbb{R}$ are all psd for all $(e_1, \ldots, e_s) \in \{0, 1\}^s$.

Next we reformulate question (1) in 2.4 of Lecture 15 in terms of Hankel matrices:

2. SCHMÜDGEN’S NNSS AND HANKEL MATRICES

We want to understand $L(h^2g) \geq 0; h, g \in \mathbb{R}[X]$ in terms of Hankel matrices.

Definition 2.1. A real symmetric $n \times n$ matrix $A$ is psd if $x^T Ax \geq 0 \forall x \in \mathbb{R}^n$. An $N \times N$ symmetric matrix (say) $A$ is psd if $x^T Ax \geq 0 \forall x \in \mathbb{R}^n$ and $\forall n \in \mathbb{N}$.

Definition 2.2. Let $L \neq 0; L : \mathbb{R}[X] \longrightarrow \mathbb{R}$ be a given linear functional. Fix $g \in \mathbb{R}[X]$. Consider symmetric bilinear form:

$$\langle \cdot, \cdot \rangle_g : \mathbb{R}[X] \times \mathbb{R}[X] \to \mathbb{R}$$

$$\langle h, k \rangle_g := L(hkg) ; h, k \in \mathbb{R}[X]$$

Denote by $S_g$ the $N \times N$ symmetric matrix with $\alpha\beta$-entry $\langle X^\alpha, X^\beta \rangle_g \forall \alpha, \beta \in \mathbb{N}^n$, i.e. the $\alpha\beta$-entry of $S_g$ is $L(X^{\alpha+\beta} g)$.

Example. Let $g = 1$, then

$$\langle X^\alpha, X^\beta \rangle_1 = L(X^{\alpha+\beta}) := S_{\alpha+\beta}.$$ 

More generally, if $g = \sum a_\gamma X^\gamma$ then

$$\langle X^\alpha, X^\beta \rangle_g = L\left( \sum_\gamma a_\gamma X^{\alpha+\beta+\gamma} \right) = \sum_\gamma a_\gamma S_{\alpha+\beta+\gamma}.$$ 

Proposition 2.3. Let $L, g$ be fixed as above. Then the following are equivalent:

1. $L(\sigma g) \geq 0 \forall \sigma \in \mathbb{R}[X]^2$.
2. $L(h^2g) \geq 0 \forall h \in \mathbb{R}[X]$.
3. $\langle \cdot, \cdot \rangle_g$ is psd.
4. $S_g$ is psd.

Proof. (1) $\Leftrightarrow$ (2) is clear. Since $\langle h, h \rangle_g = L(h^2g)$, (2) $\Leftrightarrow$ (3) is clear. (3) $\Leftrightarrow$ (4) is also clear.
2.4. Example. (Hamburger) Let $n = 1$. A linear functional $L : \mathbb{R}[X] \to \mathbb{R}$ comes from a Borel measure on $\mathbb{R}$ if and only if $L(\sigma) \geq 0$ for every $\sigma \in \sum \mathbb{R}[X]^2$.

Proof. From Haviland we know $L$ comes from a Borel measure iff $L(f) \geq 0$ for every $f(X) \in \mathbb{R}[X], f \geq 0$ on $\mathbb{R}$. But $\text{Psd}(\mathbb{R}) = \sum \mathbb{R}[X]^2$ (by exercise in Real Algebraic Geometry course in WS 2009-10). So the condition is clear. \(\square\)

Remark 2.5. We can express Hamburgers’s Theorem via Hankel matrix $S_g$ with $g = 1$ the constant polynomial.

$n = 1$, so (for $i, j \in \mathbb{N}$) the $ij$\textsuperscript{th} coefficient of $S_1$ is $s_{i,j} = L(X^{i+j})$.

Hence, $S_1 = \begin{pmatrix} s_0 & s_1 & s_2 & \ldots \\ s_1 & s_2 & \ldots \\ s_2 & \ldots & \ddots \\ \vdots & \vdots & \ddots \end{pmatrix}$ is psd.

2.1. REFORMULATION OF SCHMÜDGEN’S SOLUTION TO THE MOMENT PROBLEM IN TERMS OF HANKEL MATRICES

2.6. Let $S = \{ g_1, \ldots, g_s \} \subseteq \mathbb{R}[X]$ and $K_S \subseteq \mathbb{R}^n$ is compact. A linear functional $L$ on $\mathbb{R}[X]$ is represented by a Borel measure on $K$ iff the $2^S$ $\mathbb{N} \times \mathbb{N}$ Hankel matrices $[S_{g_1^\alpha \ldots g_s^\beta}(e_1, \ldots, e_s) \in \{0,1\}^4]$ are psd, where $S_g := [L(X^{\alpha+\beta}g)]_{\alpha,\beta} ; \alpha, \beta \in \mathbb{N}^n$.

3. FINITE SOLVABILITY OF THE K-MOMENT PROBLEM

Definition 3.1. Let $K$ be a basic closed semi-algebraic subset of $\mathbb{R}^n$.

1. The $K$-moment problem (KMP) is **finitely solvable** if there exists $S$ finite, $S \subseteq \mathbb{R}[X]$ such that:

   (i) $K = K_S$, and

   (ii) $\forall$ linear functional $L$ on $\mathbb{R}[X]$ we have: $L(T_S) \geq 0 \Rightarrow L(\text{Psd}(K)) \geq 0$ (equivalently, (iii) $L(T_S) \geq 0 \Rightarrow \exists \mu : L = \int d\mu$).

2. We shall say $S$ solves the KMP if (i) and (ii) (equivalently (i) and (iii)) hold.

3.2. Schmüdgen’s solution to the KPM for $K$ compact b.c.s.a. Let $K \subseteq \mathbb{R}^n$ be a compact basic closed semi-algebraic set. Then $S$ solves the KMP for any finite description $S$ of $K$ (i.e. for all finite $S \subseteq \mathbb{R}[X]$ with $K = K_S$).
One can restate the condition “$S$ solves the $K$-Moment problem” via the equality of two preorderings. We shall adopt this approach throughout:

**Definition 3.3.** Let $T_S \subseteq \mathbb{R}[X]$ be a preordering. Define the dual cone of $T_S$:

$$T_S^\vee := \{ L | L : \mathbb{R}[X] \to \mathbb{R} \text{ is a linear functional; } L(T_S) \geq 0 \}$$

and the double dual cone:

$$T_S^{\vee\vee} := \{ f \mid f \in \mathbb{R}[X]; L(f) \geq 0 \ \forall \ L \in T_S^\vee \}.$$

**Lemma 3.4.** For $S \subseteq \mathbb{R}[X]$, $S$ finite:

(a) $T_S \subseteq T_S^{\vee\vee}$

(b) $T_S^{\vee\vee} \subseteq \text{Psd}(K_S)$.

**Proof.** (a) Immediate by definition.

(b) Let $f \in T_S^{\vee\vee}$. To show: $f(\bar{x}) \geq 0 \ \forall \ \bar{x} \in K_S$.

Now every $\bar{x} \in \mathbb{R}^n$ determines an $\mathbb{R}$-algebra homomorphism

$$e_{\bar{x}} := L_{\bar{x}} \in \text{Hom}(\mathbb{R}[X], \mathbb{R}); \quad L_{\bar{x}}(g) = e_{\bar{x}}(g) := g(\bar{x}) \ \forall \ g \in \mathbb{R}[X],$$

this $L_{\bar{x}}$ is in particular a linear functional.

Moreover we claim that $L_{\bar{x}}(T_S) \geq 0$ for $\bar{x} \in K_S$. Indeed if $g \in T_S$ then $L_{\bar{x}}(g) = g(\bar{x}) \geq 0$ for $\bar{x} \in K_S$.

So, by assumption on $f$ we must also have $L_{\bar{x}}(f) \geq 0$ for $\bar{x} \in K_S$, i.e. $f(\bar{x}) \geq 0$ for all $\bar{x} \in K_S$ as required.

□

We summarize as follows:

**Corollary 3.5.** For finite $S \subseteq \mathbb{R}[X]$:

$$T_S \subseteq T_S^{\vee\vee} \subseteq \text{Psd}(K_S).$$

**Corollary 3.6.** (Reformulation of finite solvability) Let $K \subseteq \mathbb{R}^n$ be a b.c.s.a. set and $S \subseteq \mathbb{R}[X]$ be finite. Then $S$ solves the KMP iff

(j) $K = K_S$, and

(jj) $T_S^{\vee\vee} = \text{Psd}(K)$. 
Proof. Assume (ii) of definition 3.1, i.e. $\forall L : L(T_S) \geq 0 \Rightarrow L(\text{Psd}(K)) \geq 0$, and show (jj) i.e. $T_S^{\vee} = \text{Psd}(K)$:

Let $f \in \text{Psd}(K)$. Show $f \in T_S^{\vee}$ i.e. show $L(f) \geq 0 \forall L \in T_S^{\vee}$.
Assume $L(T_S) \geq 0$. Then by assumption $L(\text{Psd}(K)) \geq 0$. So, $L(f) \geq 0$ as required.

Conversely, assume (jj) and show (ii):

Let $L(T_S) \geq 0$, i.e. $L \in T_S^{\vee}$. Show $L(\text{Psd}(K)) \geq 0$, i.e show $L(f) \geq 0 \forall f \in \text{Psd}(K)$.
Now [by assumption (jj)] $f \in \text{Psd}(K) \Rightarrow f \in T_S^{\vee} \Rightarrow L(f) \geq 0 \forall L \in T_S^{\vee}$. □

We shall come back later to $T_S^{\vee}$ and describe it as closure w.r.t. an appropriate topology.

4. HAVILAND’S THEOREM

For the proof of Haviland’s theorem (2.5 of lecture 15), we will recall Riesz Representation Theorem.

Definition 4.1. A topological space is said to be Hausdorff (or separated) if it satisfies

(H4): any two distinct points have disjoint neighbourhoods, or

(T2): two distinct points always lie in disjoint open sets.

Definition 4.2. A topological space $\chi$ is said to be locally compact if $\forall x \in \chi \exists$ an open neighbourhood $U \ni x$ such that $\overline{U}$ is compact.

Theorem 4.3. (Riesz Representation Theorem) Let $\chi$ be a locally compact Hausdorff space and $L : \text{Cont}_c(\chi, \mathbb{R}) \rightarrow \mathbb{R}$ be a positive linear functional i.e. $L(f) \geq 0 \forall f \geq 0$ on $\chi$. Then there exists a unique (positive regular) Borel measure $\mu$ on $\chi$ such that $L(f) = \int_{\chi} f d\mu \forall f \in \text{Cont}_c(\chi, \mathbb{R})$, where $\text{Cont}_c(\chi, \mathbb{R}) :=$ the ring ($\mathbb{R}$-algebra) of all continuous functions $f : \chi \rightarrow \mathbb{R}$ (addition and multiplication defined pointwise) with compact support i.e. such that the set $\text{supp}(f) := \{x \in \chi : f(x) \neq 0\}$ is compact.

Definition 4.4. $L$ positive means:

$L(f) \geq 0 \forall f \in \text{Cont}_c(\chi, \mathbb{R})$ with $f \geq 0$ on $\chi$. 