# Algebra 3

Inofficial lecture notes
for the lecture held by Prof. Bürgisser, WS2016/17

geschrieben von Henning Seidler
henning.seidler@mailbox.tu-berlin.de

Henning Seidler

## Contents



# 1 Real Algebra

In previous lectures we focused on extension of $\mathbb{Q}$, or we took $\mathbb{C}$ when we needed an algebraically closed field. Now we regard $\mathbb{R}$ as basis.
Much is based on work of E.Artin, U. Schreyer. The standard textbook is "Real Algebraic Geometry" by Bochnak, Coste and Roy.

## 1.1 Real Fields

**Definition.** *An* ordered field *(angeordneter Körper) is a field $K$ together with a total order $\leq$ on $K$ such that*

*(1)* $\forall x, y, z \in K : x \leq y \implies x + z \leq y + z$

*(2)* $\forall x, y \in K : 0 \leq x, 0 \leq y \implies 0 \leq xy$

*We will use the notation $x < y :\Leftrightarrow x \leq y \wedge x \neq y$.*

**Example.**

- *Of course, $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields.*
- *For $f \in \mathbb{R}[X] \setminus \{0\}$, with $f = \sum_{i=m}^{d} a_i X^i$ and $a_m \neq 0$ we define $0 < f :\Leftrightarrow 0 < a_m$. This can be expanded to $\mathbb{R}(X)$, where we say $0 < \frac{f}{g} \Leftrightarrow 0 < f \cdot g$. To obtain a total order we define $q_1 \leq q_2 :\Leftrightarrow q_1 = q_2 \vee 0 < q_2 - q_1$.*

  *For any $r \in \mathbb{R}$ we have $0 < X < r$. So $X$ is like an infinitesimal.*

**Remark.** *Let $(K, \leq)$ be an ordered field. Then $\forall x \in K : 0 \leq x^2$. So we have $0 < 1^2 = 1$ and by induction $n < n+1$, which implies $\operatorname{char} K = 0$.*

*Proof.* If $0 \leq x$, then $0 \leq x \cdot x$ by the second axiom. Otherwise $x < 0$. So we have $0 < -x$ so we get $0 < (-x)(-x) = x^2$. □

**Definition.** *A* cone *(Kegel) of a field $K$ is a subset $P \subseteq K$ such that*

*(1) $\forall x, y \in P : x + y \in P$*

*(2) $\forall x, y \in P : xy \in P$*

*(3) $\forall x \in K : x^2 \in P$.*

*A cone is called* proper *is $-1 \notin P$.*

**Lemma.** *Let $(K, \leq)$ be an ordered field.*

*(1) Then $P := \{x \in K : x \geq 0\}$ is a proper cone, the positive cone of $(K, \leq)$, and we have $P \cup (-P) = K$.*

*(2) Conversely, if $P$ is a proper cone with $P \cup (-P) = K$, then $x \leq y :\Leftrightarrow y - x \in P$ defines a total order of $K$.*

*Proof.* The first is clear.
For the second we claim $P \cap (-P) = \{0\}$. Assume $0 \neq a \in P \cap (-P)$. Let $x \in K \setminus P$. Thus $-x \in P$. But then we get $x = (a^{-1})^2 \cdot a(-x)(-a) \in P$, which is a contradiction. □

**Remark.** *The set $\sum K^2 := \{x_1^2 + \ldots + x_n^2 : x_i \in K, n \in \mathbb{N}\}$ is a cone. It is contained in any cone of $K$.*

**1.1 Lemma.** *Let $P$ be a proper cone of $K$ and $a \in K$.*

1. *$-a \notin P$ implies $P[a] := \{x + ay : x, y \in P\}$ is a proper cone of $K$.*
2. *$P$ is contained in the positive cone of an ordering of $K$.*

*Proof.*

1. The first two axioms are calculation and use of $a^2 \in P$. The third follows from $P \subseteq P[a]$ (take $y = 0$). So $P[a]$ is a cone.

   Assume $-1 \in P[a]$ with $-1 = x + ay$. Then $y \neq 0$, because $-1 \notin P$. But in this case $-a = (x+1)y^{-1} = (x+1)y(y^{-1})^2 \in P$ we get a contradiction.

2. By applying the above construction, we get a chain, whose union forms an upper bound. By Zorn's Lemma there is a maximal proper cone $Q$ containing $P$. So we need to check $Q \cup (-Q) = K$: Let $-a \notin Q$. Then $a \in Q[a]$, but $Q[a]$ is a proper cone, so $Q[a] = Q$.

□

**Theorem.** *Let $K$ be a field. TFAE (The following are equivalent)*

1. *$K$ has an ordering.*
2. *$K$ has a proper cone.*
3. $-1 \notin \sum K^2$
4. $\forall x_1, \ldots, x_n \in K : \sum x_i^2 = 0 \implies \forall i : x_i = 0$

*Proof.* The chain (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is clear with the above.
Assume (3) and $\sum_{i=1}^n x_i^2 = 0$ with $x_1 \neq 0$. Then $-1 = \sum_{i=2}^n \left(\frac{x_i}{x_1}\right)^2$, which is a contradiction.
(4)$\Rightarrow$(3): Assume $-1 = \sum x_i^2 \in \sum K^2$. Then we can add $1^2$ on both sides, so $0 = 1^2 + \sum x_i^2$. By (4) this implies $1 = 0$. $\lightning$.
(3)$\Rightarrow$(1): Since $-1 \notin \sum K^2$, this cone is proper. By Lemma 1.1 the cone $\sum K^2$ is contained in the positive cone of an ordering of $K$. So in particular $K$ has an ordering. $\square$

**Definition.** *A field $K$ which has these properties is called* real field.

**Remark.** *Every real field contains a copy of $\mathbb{Q}$. This already follows from the characteristic.*

**Proposition.** *Let $K$ be a real field, $P$ a proper cone. Then $P$ is the intersection of the positive cones $Q$ of all orderings of $K$ where $P \subseteq Q$. In particular $\sum K^2$ is the intersection of positive cones of all orderings.*

*Proof.* Assume $-a \notin P$. By Lemma 1.1.(1) $P[a]$ is a proper cone of $K$. By Lemma 1.1.(2) $P[a]$ is contained on the positive cone $Q$ of some ordering of $K$. Then $a \in Q$, so $-a \notin Q$. so each element not contained in $P$ is cut off by some ordering. $\square$

**Example.**

- *Every subfield of $\mathbb{R}$ is a real field.*
- *Recall our ordering on $\mathbb{R}(X)$. Then this also becomes a real field.*

## 1.2 Real Closed Field (reell abgeschlossene Körper)

**Definition.** *A real field $K$ is called* real closed *if it does not have a proper real algebraic extension. That is: if $K \leq K_1$ is an algebraic extension and $K_1$ is a real field, then $K = K_1$.*

**Example.** $\mathbb{R}$ *is real closed: Let $\mathbb{R} \leq K_1$ be an algebraic extension. But we already know this allows only for $K_1 = \mathbb{R}$ or $K_1 = \mathbb{C}$. But $\mathbb{C}$ is not real, since $-1 \in \sum \mathbb{C}^2$.*

**Example.** $\mathbb{R}_{\text{alg}} := \{x \in \mathbb{R} : a \text{ alg. over } \mathbb{Q}\}$ *is a real closed field. The proof idea is $\mathbb{R}_{\text{alg}}(i) = \overline{\mathbb{Q}}$.*

More general we will show: If $K$ real and $K(i)$ alg. closed, then $K$ is real closed.

**1.2 Theorem.** *Let $K$ be a real field. TFAE*

1. *$K$ is real closed.*
2. *$K^2 = \{a \in K : a \geq 0\}$ and any polynomial of odd degree as a root in $K$.*
3. *$K(i) = K[X]/(X^2 + 1)$ is algebraically closed.*

*Proof.* **(1)⇒(2)** Put $Q := K^2$. We want to show $Q = \sum K^2$. Assume $a = \sum b_i^2 \notin Q$. Then $K < K(\sqrt{a})$ is a proper algebraic extension. Since $K$ is real closed, this is not a real field. By the above characterisation we can write $-1$ as a sum of squares:

$$\begin{aligned} -1 &= \sum_{i=1}^{m}(x_i + y_q\sqrt{a})^2 && \text{with } x_i, y_i \in K \\ &= \sum_{i=1}^{m}(x_i^2 + ay_i^2) + \lambda\sqrt{a} && \text{compare coefficients} \\ -1 &= \sum x_i^2 + a\sum y_i^2 \\ -a &= \left(1+\sum x_i^2\right)\left(\sum y_i^2\right)\left(\sum y_i^2\right)^{-2} \in \sum K^2 \\ \Rightarrow -a &=: \sum z_i^2 \end{aligned}$$

But then $\sum b_i^2 + \sum z_i^2 = 0$, which only is possible if $b_i = z_i = 0$, so $a = 0$. ↯

Next we claim $Q \cup -Q = K$: We just showed if $a \notin Q$, then $-a \in \sum K^2 = Q$. Therefore $Q$ is the positive cone of an ordering of $K$.

Claim 3: If $f \in K[X]$, $d := \deg f$ is odd, then $f$ has a root in $K$. To this end assume $f$ has no root and is of minimal degree. We know $f$ has an irreducible factor of odd degree, so wlog $f$ is irreducible. Then consider $K < K[X]/(f) =: L$, which cannot be a real field. Again $-1$ is a sum of squares $-1 = \sum \overline{h}_i = \sum h_i + gf$, so $h_i \in K[X]$ with $\deg h_i < d$ and $g \in K[X]$. Then we have $\deg\left(\sum h_i^2\right) = 2\max\{\deg h_i : i\} \leq 2(s-1)$. Note that we do not have any cancellation of the leading coefficients since they are sums of squares. From $\sum h_i^2 = -1 - gf$ we conclude

$$\deg g + d = \deg(gf) = \deg\left(\sum h_i^2\right) \leq 2d - 2$$

so $\deg g \leq d - 2$, but also $\deg g$ is odd. By minimality of $f$ we know $g$ has a root $x \in K$. But then $-1 = \sum h_i(x)$ in $K$, which is a contradiction.

**(2)⇒(3)** See Algebra II

**(3)⇒(1)** Take $K \leq K_1$ an algebraic field extension. Since any extension is contained in the algebraic closure, so $K_1 \leq K(i)$. That leaves only $K_1 = K$ and $K_1 = K(i)$. But the latter is not real, since $-1$ is a sum of squares. So $K_1 = K$, hence $K$ is real closed. □

**1.3 Proposition (Intermediate Value Theorem).** *Let $R$ be a rial closed field, $a, b \in R$ with $a < b$. Let $f \in R[X]$ such that $f(a)f(b) < 0$. Then there is some $\xi \in [a, b]$ with $f(\xi) = 0$.*

*Proof.* By Theorem 1.2 $R(i)$ is algebraically closed, so $f$ splits into linear factors. But as in $\mathbb{C}$, if $x = c + di$ is a root, then also the conjugate $\overline{x} = c - di$ is a root. So all factors of $f$ are of the form $X - e_i$ and $(X - c_i)^2 + d_i^2$. From $f(a)f(b) < 0$ we know that in the interval, one of the factors must have a sign change. But the quadratic ones always yields non-negative values. So one of the $e_i$ mus be in the interval. So $e_i \in [a, b]$ with $f(e_i) = 0$ as desired. □

**Definition.** *Let $(K, \leq)$ be an ordered field. A* real closure *of $(K, \leq)$ is a field extension $K \leq R$ such that*

1. *$R$ is real closed*

2. *The inclusion $K \leq R$ is order preserving. If $x \geq 0$ in $K$, then $x \geq 0$ in $R$ and $x = y^2$ for some $y \in R$.*

change subfield to $\subseteq$, because $\leq$ is taken

**1.4 Theorem.** *Every ordered field $(K, \leq)$ has a real closure. This is unique up to isomorphism: If $K \leq R$ and $K \leq R'$ are real closures, then there exists a unique order-preserving $K$-isomorphism $R \to R'$.*

*Proof.* Let $\overline{K}$ be an algebraic closure of $K$. Thus every algebraic extension of $K$ is a subfield of $\overline{K}$, so we just look at the real ones. Consider

$$\left\{(F, \leq)\text{ordered field} : K \leq F \leq \overline{K}, K \hookrightarrow F \text{ order preserving}\right\}$$

We say $(F, \leq) \preceq (F', \leq')$ iff $F \leq F'$ and $F \hookrightarrow F'$ preserves order. Thus the above set gets an order, so we can apply Zorn's Lemma. As is the proof for the algebraic closure, the union of a chain is an upper bound, so we have a maximal element $(R, \leq)$. It remains to show that $R$ is real closed. Put $P := \{x \in R : x \geq 0\}$ and $Q := \{y^2 : y \in R\}$. Clearly $Q \subseteq P$, by axioms. But we claim $P = Q$.
Assume $a \in P \setminus Q$. The set of elements

$$\sum_i b_i \left(c_i + d_i\sqrt{q}\right)^2 \qquad\qquad b_i, c_i, d_i \in R, b_i \geq 0$$

is the cone generated by $P$ and $\sqrt{a}$ in $R\left(\sqrt{a}\right)$. This cone $P'$ is proper, because otherwise we would have

$$-1 = \sum_i b_i \left(c_i + d_i\sqrt{a}\right)^2 = \sum_i b_i(c_i^2 + d_i^2) + (\ldots) \cdot \sqrt{a}$$

and by comparing coefficients, we get $-1 = \sum_i b_i(c_i^2 + d_i^2)$, which is an equation in $R$. But $R$ is ordered, so $-1$ is not positive, while the sum is. So $P'$ is proper.
Therefore there is an ordering of $R(\sqrt{a})$ whose positive cone is $P'$. But that is a contradiction to the maximality of $R$. Hence $P = Q$.
Let $R \leq E \leq \overline{K}$ be a field extension, with $E$ real. Let $\leq_E$ be an ordering of $E$. Since $\{x \in R : x \geq 0\} = \{y^2 : y \in R\}$ we know that $\leq_E$ extends he order of $R$: If $x \geq_R 0$, then $x = y^2$ for some $y \in R \subseteq E$. So $x = y^2$ in $E$, so $x \geq_E 0$. By the maximality of $R$, we get $R = E$. Hence $R$ is real closed. □

For the proof of uniqueness, we need the following

**Theorem.** *Let $(K, \leq)$ be an ordered field and $f \in K[X]$. Let $K \leq R$ be a real closure. The number of distinct zeros of $f$ in $R$ is the same for all real closures.*

*of Theorem 1.4 cont.* Assume we have the following picture Where $R, R'$ is real closed and $K \leq F$ is a finite algebraic extension. Then we claim every order-preserving morphism $\varphi : K \to R'$ can be extended to an order preserving morphism $\varphi' : F \to R'$.
Let $F = K(a)$ for a primitive element $a$. Let $f \in K[X]$ be the minimal polynomial of $a$. Let $a_1 < a_2 < \ldots < a_n$ be the zeros of $f$ in $R$, say $a = a_j$. By the above theorem, $f$ has exactly $n$ zeros in $R'$, say $b_1 < \ldots < b_n$. Define $\varphi' : F = K(a) \to R'$ via $a = a_j \mapsto b_j$. By our knowledge from Algebra, we know such a morphism exists. But it remain to show that $\varphi'$ actually preserves order.

$$\begin{tikzcd}
R & \\
F \arrow[u] \arrow[r, dashed] & R' \\
K \arrow[u] \arrow[ur, "\varphi"] &
\end{tikzcd}$$

Take $y \in K(a)$, with $y \geq 0$. Then $y$ is a square in $R$, say $y = z^2$ for some $z \in R$. Let $x_i^2 := a_{i+1} - a_i$ for some $x_i \in R$. Then there is a morphism $\psi : K(a_1, \ldots, a_n, x_1, \ldots, x_{n-1}, y, z) =: K(\alpha) \to R'$,which extends $\varphi$. Now we can say $\psi(a_{i+1}) - \psi(a_i) = \psi(x_i)^2 \geq 0$, and $\psi(a_i)$ are the zeros of $f$. Together with the order we get $\psi(a_i) = b_i$ and in particular $\psi(a_j) = b_j = \varphi'(a_j)$. Thus $\psi_{|K(a)} = \varphi'$, so $\varphi'(y) = \psi(y) = \psi(z)^2 \geq 0$, so $\varphi'$ is order preserving.
Let $K \leq R$ be an algebraic extension. Using Zorn's Lemma any $\varphi : K \to R$ has an order preserving extension $R \to R'$. This is unique, because if $a \in R$ is the $j$-th root of its minimal polynomial $f \in K[X]$, then $a$ has to be mapped to the $j$-th root of $f$ in $R'$. $\square$

**Definition.** *An ordered field $(K, \leq)$ is called* archimedian *if for any $\alpha \in K$ there is some $n \in \mathbb{N}$ such that $\alpha < n$.*

**Remark.** *Note that $1 + \ldots + 1 \neq 0$ in any ordered field, so every ordered field contains (a copy of) the natural numbers, so the above comparison actually makes sense.*

**Example.**

1. *Subfield of $\mathbb{R}$ are archimedian.*
2. *The field $\mathbb{R}(X), \leq)$ with infinitesimal $X > 0$ is not archimedian, because $X^{-1}$ is not bounded by any natural number.*

**1.5 Exercise.** Let $(K, \leq)$ be archimedian. Then $\mathbb{Q}$ is dense in $K$, which means for all $a, b \in K$ where is some $q \in \mathbb{Q}$ with $a < q < b$.

**1.6 Exercise.** Let $(K, \leq)$ be archimedian. Then there is an order preserving mophism $K \hookrightarrow \mathbb{R}$ of fields. Up to isomorphism, the archimedian fields are exactlythe subfield of $\mathbb{R}$.
See: "Real Algebra", by A. Prestel.

## 1.3 Counting real roots

Let $R$ be a real closed field.

**Proposition.** *Let $f \in K[X]$ and $a, b \in R$ with $a < b$.*

1. *(Rolle) If $f(a) = f(b) = 0$ then $f'(c) = 0$ for some $a < c < b$.*
2. *(Mean Value Theorem) There is some $c \in (a, b)$ with $f(b) - f(a) = f'(c)(b - a)$.*
3. *If for all $x \in (a, b)$ we have $f'(x) > 0$, then $f$ is strictly increasing in $(a, b)$.*

*Proof.* 1. Wlog $a, b$ are consecutive zeros of $f$, say $f = (X - a)^m (X - b)^m g$ with $n, m \geq 1$ and $g$ without root in $(a, b)$. By Proposition 1.3 $g$ has constant sign on $(a, b)$. Furthermore we have

$$f' = (X-a)^{m-1}(X-b)^{n-1}g_1 \text{ for } g_1 = m(X-b)g + n(X-a)g + (X-a)(X-b)g'$$

Then $g_1(a) = m(a-b)g(a) < 0$ and $g_1(b) = n(b-a)g(b) > 0$ have opposite sign. By Proposition 1.3 there is some $c \in (a,b)$ with $g_1(c) = 0$, so $f'(c) = 0$.

2. Apply 1 to $\widetilde{f} = f - f(a) - m(X-a)$, $m := \frac{f(b)-f(a)}{b-a}$.

3. Clear after 2.

□

For this section let $R$ be a real closed field.

**Definition.** *The* variation $\operatorname{var}(a_1, \dots, a_n)$ *of a sequence* $(a_1, \dots, a_n)$ *in* $R$ *is the number of its strict sign changes. For some polynomial* $f = \sum_{i=0}^{n} a_i X^i$ *we put* $\operatorname{vc}(f) := \operatorname{var}(a_0, \dots, a_n)$.

**Example.** $\operatorname{var}(1,-2,3,4) = 2$, *but* $\operatorname{var}(1,0,-2,0,3,0,0,4) = 2$, *because the zeroes are no strict changes.* $\operatorname{vc}(f)(X^n - 1) = \operatorname{var}(-1,0,\dots,0,1) = 1$; $\operatorname{vc}(X^n+1) = 0$.

**Remark.** *If* $f$ *hat* $t$ *terms, then* $\operatorname{vc}(f) \le t-1$.

Denote by $N_+(F)$ the number of positive roots in $R$, counted with multiplicity.

**1.7 Theorem (Décartes Rule,1637).** *For* $f \in R[X] \setminus R$ *we have* $N_+(f) \le \operatorname{vc}(f)$. *In particular, a polynomial with* $t$ *terms has at most* $t-1$ *positive roots.*

**Example.** *1. Let* $f = X^n - 1$, *so* $t = 2$ *terms and* $N_+(f) = 1$ *(only 1),so this bound is sharp.*

*2.* $f = \sum_{i=0}^{n-1} X^i = \frac{X^n-1}{X-1}$. *We have* $\operatorname{vc}(f) = 0 = N_+(f)$.

*3. For* $f = X^3 - X^2 + X - 1$ *we have* $\operatorname{vc}(f) = 3$ *but* $N_+(f) = 1$.

*of Theorem 1.7.* Induction over the number of terms: For the case $t = 1$ the polynomial has the form $f = a_n X^n$, which has no sign change and no positive root.
Now let $f = \sum_{i=m}^{n} a_i X^i$ with $m < n$ and $a_n a_m \neq 0$. This we rewrite as

$$f = X^m \left(a_n X^{n-m} + \ldots + a_m\right) =: X^m \cdot \widetilde{f},$$

so wlog we can assume $m = 0$. Then we look at the next coefficient after $a_0$ (note that we allow gaps), so $f = a_n X^n + \ldots + a_q X^q + a_0$ where $a_q a_0 \neq 0$ and $q > 1$. Regard the derivative $f' = n a_n X^{n-1} + \ldots + q a_q x^{q-1}$. Note that $f'$ has one term less, so we can apply our induction hypothesis. We have

$$\operatorname{vc}(f) = \begin{cases} \operatorname{vc}(f') & : a_q a_0 > 0 \\ \operatorname{vc}(f') + 1 & : a_q a_0 < 0 \end{cases}$$

It is sufficient to show

$$N_+(f) \le \begin{cases} N_+(f') & : a_q a_0 > 0 \\ N_+(f') + 1 & : a q a_0 < 0 \end{cases} \tag{1}$$

Let $0 < x_1 < \ldots < x_s$ be the positive roots of $f$ with multiplicities $\mu_i$. By Rolle, there are roots $y_1, \dots, y_{s-1}$ of $f'$ such that $0 < x_1 < y_1 < x_2 < \ldots < x_{s-1} < y_{s-1} < x_s$. Moreover $x_i$ is root if

$f'$ with multiplicity $\mu_i$. Note that $N_+(f) = \sum \mu_i$. Furthermore $N_+(f') \geq (s-1) + \sum(\mu_i - 1)$. Therefore eq. (1) follows in the case $a_q a_0 < 0$. So now assume $a_q a_0 > 0$, so wlog both are positive. Hence $f(0) > 0$ and $f'(0) > 0$, so we start positive and have a positive slope. Thus between 0 and $x_1$ there must be a maximum $y_0$ of $f$. But in that point we must have $f'(y_0) = 0$, so we have found another root of $f'$. So in this case we get $N_+(f') \geq 1 + (s-1) + \sum(\mu_i - 1) = N_+(f)$. □

**Remark (Supplement to Décartes Rule).** *For $f \in R[X] \setminus R$ we have $N_+(f) \equiv \mathrm{vc}(f) \mod 2$.*

**Example.** *Let $f = \sum_{k=0}^{n}(-1)^k X^{n-k}$, so $\mathrm{vc}(f) = n$. But also we have $N_+(f) = 0$ if $n$ is even, and $N_+(f) = 1$ if $n$ is odd.*

Generalisation: Let $f \in R[X]$ and $\xi \in R$. We define the variation of the derivatives of $f$ at $\xi$ via

$$\mathrm{vder}_\xi(f) := \mathrm{var}(f(\xi), f'(\xi), f''(\xi), \ldots)$$

For $-\infty \leq a < b \leq \infty$ denote by $N_{(a,b]}(f)$ the number of roots in $f$ in the interval $(a,b]$, counted with multiplicity. Earlier we had the special case $N_+(f) = N_{(0,\infty]}(f)$.

**1.8 Theorem (Budan (1807), Fourier (1820)).** *Let $f \in R[X] \setminus R$ and $-\infty \leq a < b \leq \infty$. Then*

$$N_{(a,b]}(f) \leq \mathrm{vder}_a(f) - \mathrm{vder}_b(f)$$
$$N_{(a,b]}(f) \equiv \mathrm{vder}_a(f) - \mathrm{vder}_b(f) \mod 2$$

**Remark.**
- *We have shown the special case $a = 0$ and $b = \infty$.*
- $\mathrm{vder}_0(f) = \mathrm{var}(f(0), f'(0), \ldots) = \mathrm{var}(k! \cdot a_k : k = 0, \ldots, n) = \mathrm{vc}(f)$
- $\mathrm{vder}_\infty(f) = 0$ *(that means $\mathrm{vder}_M(f)$ for some sufficiently large number $M$)*

Given $f \in R[X]$ square-free (i.e. $\gcd(f, f') = 1$). We apply the Euclidean Algorithm to $f$ and $f'$,putting $f_0 := f$ and $f_1 := f'$. The recursive steps are written as $f_{i-1} = q_i f_i - f_{i+1}$ for $i = 1, \ldots, l$. (We already know the final result, but we are interested in the $f_i$ we obtain during the computation.) Note that

$$\gcd(f_{i+1}, f_i) = \gcd(f_i, f_{i-1}) = \ldots = \gcd(f', f) = 1$$

For $\xi \in R$ we define $V_\xi(f) := \mathrm{var}(f_0(\xi), \ldots, x_l(\xi)$.

**1.9 Theorem (Sturm, 19th cent.).** *Let $f \in R[X]$ (be square-free), $a, b \in R$ with $a < b$ and $f(a) \neq 0 \neq f(b)$. Then*

$$\#\{\xi \in (a,b) : f(\xi) = 0\} = V_a(f) - V_b(f)$$

**Remark.** *The condition square-free can be removed, because that would just add the same factor in our sequence in the variation. But $\mathrm{var}(a_i : i) = \mathrm{var}(a_i \cdot b : i)$.*

**Example.** *Take $f = X^3 - X$=(X-1)X(X+1)=: $f_0$. Then $f_1 = f' = 3X^2 - 1$. The algorithm yields $f = \frac{1}{3}Xf' - \frac{2}{3}X$ and $f_1 = \frac{9}{2}f_2 - 1$, that is $f_2 = \frac{2}{3}X$ and $f_3 = 1$. So we get the following table*

| $\xi$ | $-2$ | $-\frac{1}{2}$ | $\frac{1}{2}$ | $2$ |
|---|---|---|---|---|
| $V_\xi(f)$ | 3 | 2 | 1 | 0 |

| | $f_0$ | $f_1$ |
|---|---|---|
| $\xi_-$ | - | + |
| $\xi$ | 0 | + |
| $\xi_+$ | + | + |

**Remark.** *Denote by* $\mathrm{lc}(f) := a_n$ *the leading coefficient for* $f = a_n X^n + \ldots$, *where* $a_0 \neq 0$. *Put* $V_\infty(f) := \mathrm{var}(\mathrm{lc}(f_0), \mathrm{lc}(f_1), \ldots)$ *and likewise* $V_{-\infty} := V_\infty(f(-X))$.
*If* $\xi$ *is the largest root of* $f$, *then* $f$ *has constant sign on the interval* $(\xi, \infty)$ *and this sign is the same one as* $\mathrm{lc}(f)$.

**Corollary.** *Sturm's theorem also holds for* $-\infty \leq a < b \leq \infty$. *In particular*

$$\#\{\xi \in R : f(\xi) = 0\} = V_{-\infty}(f) - V_\infty(f).$$

*Proof.* Assume as zeroes of $f_0, \ldots, f_l$ are contained in the interval $(-M, M)$. Then by the previous observation $\mathrm{sgn}(f_i(M)) = \mathrm{sgn}(\mathrm{lc}(f_i))$ for all $0 \leq i \leq l$. Hence $V_\infty(f) = V_M(f)$. Similarly $V_{-\infty}(f) = V_{-M}(f)$. Now we apply Sturm on the interval $(-M, M)$ and obtain the result. ☐

*of Theorem 1.9.* Let $\xi_1 < \ldots < \xi_s$ be the roots in $R$ of $f_0, \ldots, f_l$. In the open interval $(\xi_i, \xi_{i+1})$ all of the functions $f_0, \ldots, f_l$ have constant sign. In particular $\xi \mapsto V_\xi(f)$ is constant on these intervals.
Let $\xi \in \{\xi_1, \ldots, \xi_s\}$ and $\xi_-$ and $\xi_+$ are "close" to $\xi$ (i.e. $\xi = \xi_i$ and $\xi_{i-1} < \xi_- < \xi_i < \xi_+ < \xi_{i+1}$). It suffices to show

$$V_{\xi_-}(f) = \begin{cases} V_{\xi_+}(f) + 1 & : f(\xi) = 0 \\ V_{\xi_+}(f) & \text{else} \end{cases} \tag{2}$$

To that end we have the following observations

(A) $f_i(\xi) > 0$ implies $f_i(\xi_-) > 0$ and $f_i(\xi_+) > 0$ by intermediate value theorem. Likewise we have $f_i(\xi) < 0$ implies $f_i(\xi_-) < 0$ and $f_i(\xi_+) < 0$

(B) Let $f(\xi) = 0$, i.e. $f_0(\xi) = 0$. Since $f$ is square-free we get $f'(\xi) \neq 0$; wlog $f'(\xi) > 0$. Then for the sign we get the following table Therefore $\mathrm{var}(f_0(\xi_-), f_1(\xi_-) = 1$ and $\mathrm{var}(f_0(\xi_+), f_1(\xi_+) = 0$.

(C) Let $f_i(\xi) =$ for some $i > 0$. Since $\gcd(f_{i-1}, f_i) = 1$ we get $f_i(\xi) \cdot f_{i-1}(\xi) \neq 0$ (otherwise $X - \xi$ would be a common factor). From the above algorithm we have $f_{i-1}(\xi) = q_i(\xi) f_i(\xi) - f_{i+1}(\xi) = f_{i+1}(\xi)$. So these have different sign; wlog $f_{i-1}(\xi) < 0$ and $f_{i+1}(\xi) > 0$. Hence we obtain the sign table No mater which sign we have at the unknown places, we still have one sign change

| | $f_{i-1}$ | $f_i$ | $f_{i+1}$ |
|---|---|---|---|
| $\xi_-$ | - | ? | + |
| $\xi$ | - | 0 | + |
| $\xi_+$ | - | ? | + |

in every line. Therefore

$$\mathrm{var}(f_{i-1}(\xi_-) =, f_i(\xi_-), f_{i+1}(\xi_-)) = \mathrm{var}(f_{i-1}(\xi_+) =, f_i(\xi_+), f_{i+1}(\xi_+)) = 1$$

From item B and item C we get that eq. (2) is "locally true". There may be several $i$ such that $f_i(\xi) = 0$. But from that it is easy to see that eq. (2) holds in general. ☐

**Exercise.** *Show the statement still holds if you drop the condition* $\gcd(f, f') = 1$.

*Proof.* The main idea is $\mathrm{var}(f_0(\xi), \ldots, f_l(\xi)) = \mathrm{var}(f_0(\xi) \cdot g(\xi), \ldots, f_l(\xi), g(\xi))$ as long as $g(\xi) \neq 0$. ☐

# 2 Tarski-Seidenberg principles and applications

Let $R$ be a real closed field.
**Motivation:** We regard the quadratic equation, let $a, b, c \in R$.

$$\exists X \in R. aX^2 + bX + c = 0 \tag{3}$$

As over $\mathbb{R}$ we have $\exists X \in R. X^2 + pX + q = 0 \Leftrightarrow \frac{p^2}{4} - q \geq 0$. The important observation is that the left hand side has an existential quantifier, whereas the right hand side is quantifier-free. So we eliminated a quantifier, which makes the decision easier by far. Thus eq. (3) is equivalent to

$$(a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge b \neq 0) \wedge (a = b = c = 0) \tag{4}$$

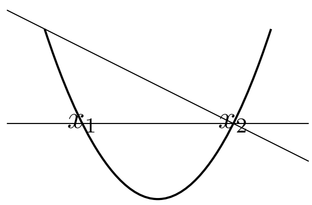
By Theorem 1.9 we have a way to check eq. (3) for arbitrary degree. For $f \in R[X]$ the question $\exists x \in R. f(X) = 0$ can be expressed by a quantifier-free formula.
Furthermore this can be generalised to an arbitrary number of variables. We iterate the single variable case and eliminate a quantifier in each step.
In particular the existence of a root of $f \in R[X_1, \ldots, X_n]$ is decidable. In contrast the question $\exists x \in \mathbb{Z}^n. f(x) = 0$ is undecidable. It was proven by Julia Robinson, Putnam, David and Matjasevich, which solved Hilbert's 10th problem.

**Definition.** *Let $R$ be a real closed field. Then we define the sign function* $\operatorname{sgn} : R \to \{+, 0, -\}$ *in the canonical way.*

Let $f_1, \ldots, f_r \in R[X]$ and let $x_1 < x_2 < \ldots < x_N$ be the roots of the $f_i \neq 0$. By intermediate value theorem the sign of the $f_i$ on each interval $(x_j, x_{j+1})$ is constant. Denote this by $\operatorname{sgn} f_i(x_j, x_{j+1})$. Define the *sign table* $\mathrm{SGN}(f_1, \ldots, f_r) \in \{-, 0, +\}^{r \times (2N+1)}$. For the number of columns we have $N + 1$ intervals and the $N$ roots.

$$\begin{matrix} \operatorname{sgn} f_1(-\infty, x_1) & \operatorname{sgn}(f_1(x)) & \ldots & \operatorname{sgn} f_1(x_N, \infty) \\ \vdots & & & \\ \operatorname{sgn} f_r(-\infty, x_1) & & \ldots & \operatorname{sgn} f_r(x_N, \infty) \end{matrix}$$

**Example.** *Assume we have the following picture. Thus we get the sign table*




$$\mathrm{SGN}(f_1, f_2) = \begin{pmatrix} + & 0 & - & 0 & + \\ + & + & + & 0 & - \end{pmatrix}$$

**2.1 Lemma.** *Let $f \in R[X]$ and $a, b \in R$ with $a < b$. Let $\varepsilon := \operatorname{sgn}(f')$ be constant on $(a, b)$. Then the sign table of $f$ on $[a, b]$ is determined by $\varepsilon_a := \operatorname{sgn} f(a), \varepsilon_b := \operatorname{sgn} f(b)$ and $\varepsilon$. If $b = \infty$, then the sign table of $f$ on $[a, \infty)$ is determined by $\varepsilon_a$ and $\varepsilon$. Similarly for $a = -\infty$.*

*Proof.* Wlog let $\varepsilon = +$. By Rolle $f$ has at most one root in $(a, b)$. Now we have some case distinctions.

**Case $\varepsilon_a = +$:** We start positive and go up, so it remains positive.

**Case $\varepsilon_a = 0$:** We start at zero, then go up.

**Case $\varepsilon_a = -$, $\varepsilon_b = +$:** We have some root.

**Case $\varepsilon_a = -$, $\varepsilon_b = 0$:** We end with a root.

**Case $\varepsilon_a = -$, $\varepsilon_b = -$:** We stay negative all the time.

□

**Corollary.** *Let $f \in R[X]$ with $f' \neq 0$. We compute the division $f = qf' + g$ with $\deg g < \deg f'$. Then the sign table of $f$ is determined by the sign table of $(f', g)$.*

*Proof.* Let $x_1 < \ldots < x_N$ be the zeroes of $f'$. So we have $f(x_i) = g(x_i)$, so we have the signs here. By Lemma 2.1 the sign of $f$ on $(x_i, x_{i+1})$ are determined by the signs of $f(x_i) = g(x_i)$ and $\operatorname{sgn} f'(x_i, x_{i+1})$. Similarly for $(-\infty, x_1)$ and $(x_N, \infty)$. □

Although this yields a recursive algorithm to compute the sign table of any polynomial, it has exponential complexity (Fibonacci).

**Example (Cubic Equation).** *We know we can restrict ourselves to the case $f = X^3 + pX + q$. Then we have $f' = 3X^2 + p$. The question is, when do we have the sign table $\mathrm{SGN}(f) = (-, 0, +, 0, -, 0, +)$? Computing the polynomial division we get $X^3 + pX + q = \frac{1}{3}X \cdot (3X^2 + q) + g$ with $g := \frac{2p}{3}X + q$. Let $x_1, x_3$ be the roots of $f'$ and $x_2$ be the root of $g$. If $f$ has 3 roots, then the picture of $f'$ and $g$ looks like the example above. For the sign table we get*

$$\mathrm{SGN}(f', g) = \begin{pmatrix} + & 0 & - & - & - & 0 & + \\ + & + & + & 0 & - & - & - \end{pmatrix}$$

*for this to happen we need $p < 0$, $f'(x_2) < 0$. Rewriting this we get $p < 0$ and $27q^2 + 4p^3 < 0$, which nicely turn out to be the discriminant. Actually we may drop the first condition.*
*But all computations are equivalences. So we get a simple criterion whether $f$ has 3 roots in $R$.*

Let $f_1, \ldots, f_r \in R[X]$ with $\deg f_i \leq m$. Then $\mathrm{SGN}(f_1, \ldots, f_r) \in \{-, 0, +\}^{r \times (2N+1)}$ where for the number of zeroes we have $N \leq r \cdot m$. Let $W_{r,m}$ be the set of all matrices of format $r \times (2N * 1)$ over $\{-, 0, +\}$ where $N \leq r \cdot m$.

**2.2 Lemma.** *There is a map $\varphi : W_{2r,m} \to W_{r,m}$ such that for all real closed fields $R$ and all lists $f_1, \ldots, f_r \in R[X]$ with $\deg f_i \leq m$, $f_r \notin R$ we have*

$$\mathrm{SGN}(f_1, \ldots, f_{r-1}, f_r) = \varphi\left(\mathrm{SGN}(f_1, \ldots, f_{r-1}, f_r', g_1, \ldots, g_r)\right)$$

*where for $i < r$ we put $g_i := f_r \bmod f_i$ and $g_r := f_r \bmod f_r'$.*

*Proof sketch.* We show that $\mathrm{SGN}(f_1, \ldots, f_r)$ is completely determined by $\mathrm{SGN}(f_1, \ldots, f_{r-1}, f_r', g_1, \ldots, g_r)$. Let $x_1 < \ldots < x_N$ be he zeroes in $R$ of $f_1, \ldots, f_{r-1}, f_r'$. From the table of $(f_1, \ldots, f_{r-1}, f_r')$ we obtain a function $\Theta : \{1, \ldots, N\} \to \{1, \ldots, r\}$ such that

$$\begin{aligned} f_{\Theta(i)}(x_i) = 0 &: \Theta(i) \neq r \\ f_r'(x_i) = 0 &: \Theta(i) = r \end{aligned}$$

Then $f_r(x_i) = g_{\Theta(i)}(x_i)$ for all $i$ (since $g_{\Theta(i)} = f_r \bmod f_{\Theta(i)}$). From the sign table of $(f_1, \ldots, f_{r-1}, f_r', g_1, \ldots, g_r)$ we can derive the sign of $f_r(x_i)$ for $i = 1, \ldots, N$. Moreover we know the sign of $f_r'$ on the intervals $(x_i, x_{i+1})$. Thus by Lemma 2.1 we obtain the sign of $f_r$ on each of these intervals. □

**Remark.** *In Lemma 2.2, for $r = 1$ we get the above corollary.*

**2.3 Theorem.** *Let $f_1, \dots, f_r \in \mathbb{Z}[X, Y_1, \dots, Y_n]$. We put $m := \max\{\deg_X f_i : i\}$ and let $W' \subseteq W_{r,n}$ (the set of "allowed" tables). Then there is a Boolean combination $B(Y)$ of polynomial equations and inequalities in $Y_1, \dots, Y_n$ over $\mathbb{Z}$ such that for all real closed fields $R$ and for all $y \in R^n$ we have*

$$\mathrm{SGN}(f_1(X, y), \dots, f_r(X, y)) \in W' \Leftrightarrow B(y)$$

**Example.** *We look at the simple case $r = 1$, where $f = \sum_{i=0}^{n} Y_i X^i \in \mathbb{Z}[X, Y_0, \dots, Y_n]$. For any $y \in R^{n+1}$ we get $f(X, y) \in R[X]$. Then there are some conditions $B : R^{n+1} \to \mathrm{bool}$ such that $\exists x. f(x, y) = 0 \Leftrightarrow B(y)$.*

*Proof of Theorem 2.3.* Induction on $m$:

**IB $m = 0$:** Then all polynomials contain no $X$. So in this case take

$$B(Y) := \bigvee_{(\varepsilon_1, \dots, \varepsilon_r)^T \in W'} \bigwedge_{i=1}^{r} (\mathrm{sgn}\, f_i(y) = \varepsilon_i)$$

**IS $m > 0$:** Wlog let $m = \deg f_r$. Write $f_i := h_{i,m_i}(Y) X^{m_i} + \ldots + h_{i,0}(Y)$ where $h_{i,m_i}(Y) \neq 0$. Claim: It is sufficient to find a quantifier-free formula for

$$\underbrace{m_r \cdot \prod_{i=1}^{r} h_{i,m_i}}_{=:h(y)} \neq 0 \wedge (\mathrm{SGN}(f_1(X, y), \dots, f_r(X, y)) \in W')$$

So we have one case where all leading coefficients are non-zero.

$$f_1(X, y) = \underbrace{h_{1,m_1}(y) X^{m_1}}_{\overset{?}{=}0} + \underbrace{h_{1,m_1-1}(y) X^{m_1-1}}_{\neq 0} + \dots$$

The idea is that if leading coefficients vanish, we may apply the IH.

Let $g_1, \dots, g_r \in \mathbb{Z}(Y)[x]$ be the remainders of the division of $f_r$ by $f_1, .., f_{r-1}, f_r'$. More precisely $h^{2e} f_r = q f_i + \widetilde{g}_i$ where $q, g_i \in \mathbb{Q}[X, Y]$ and $\deg g_i < m = \deg f_r$, $g_i = \frac{\widetilde{g}_i}{h^{2e}}$. In particular $h(y) \neq 0$ implies $g_1(X, y) = f_r(X, y) \bmod f_1(X, y)$. Note that $g_1$ and $\widetilde{g}_1$ have the same sign, so they can be exchanged in the table. Now we use Lemma 2.2. Let $W''$ be the inverse image of $W'$ under $\varphi : W_{2r,m} \to W_{r,m}$. For all $R$ and all $y \in R^n$ we have

$$h(y) \neq 0 \wedge \mathrm{SGN}(f_1(X, y), \dots, f_r(X, y)) \in W' \Leftrightarrow h(y) \neq 0 \wedge \mathrm{SGN}(f_1(X, y), \dots, f_r'(X, y), g_1(X, y), \dots, g$$

The new polynomials $f_r'(X, y), g_1(X, y), \dots, g_r(X, y)$ have degree $< m$. If degree $m$ appeared $\mu$ times among $f_1(X, y), \dots, f_r(X, y)$ then we have eliminated one occurrence, so it appears $\mu - 1$ times now. By repeating that procedure we can achieve that the maximum of the degrees is $m - 1$. Thus we can apply the IH.

□

**2.4 Corollary.** *Let $K$ be a real field and $f_1, \dots, r_f \in K[X, Y_1, \dots, Y_n]$, $(\varepsilon_1, \dots, \varepsilon_r) \in \{-, 0, +\}^r$. Then there is a boolean combination $B(Y)$ of polynomial equations and inequalities in $Y_1, \dots, Y_n$ with coefficients in $K$ such that for all real closed field extensions $K \subseteq R$ and all $y \in R^n$ we have*

$$\exists x \in R. \bigwedge_{i=1}^{r} \mathrm{sgn}\, f_i(x, y) = \varepsilon_i \Leftrightarrow B(y)$$

*Proof.* In the $f_i$ replace the coefficients in $K$ by indeterminants $T_1, \dots, T_p$, thus obtaining polynomial $F_i \in \mathbb{Z}[X, Y, T]$. Then apply Theorem 2.3 to $F_1, \dots, F_r$ and $W'$ where $W'$ consists of the tables containing the column $\varepsilon^T$. In the resulting boolean formula $B(Y, T)$ we replace the $T_j$ by the original coefficients of the $f_i$. $\square$

## Notions from logic

Let $K$ be a real field. We regard the signature $\sigma = \{0, 1, +, \cdot, -, (\cdot)^{-1}, \leq\}$. A first order formula in the language of ordered field is obtained by the above signature, i.e. using variables, quantification over elements of $K$, using the elements of $\sigma$ and boolean combinations. Denote by $\mathcal{L}(K)$ the set of these formulas. A formula without free variable is called a sentence. But even a sentence is neither true nor false on its own. It requires a field to be evaluated. As example regard $\forall y.\exists x.0 \leq y \to y = x^2$, which holds in $\mathbb{R}$ but not in $\mathbb{Q}$. For a formula with free variables we need an additional assignment.

## 2.1 Quantifier elimination

**2.5 Theorem (Tarski '31, Seidenberg '54).** *Let $K$ be a real field and $\varphi \in \mathcal{L}(K)$ with free variables $x_1, \dots, x_n$. Then there is a quantifier-free formula $\psi \in \mathcal{L}(K)$ with the same free variables such that for all real closed extensions $K \subseteq R$ and all $x \in R^n$ we have*

$$R \models \varphi(x) \Leftrightarrow R \models \psi(x)$$

*Proof.* Induction on $\varphi$, where $\wedge, \neg, \exists$ is sufficient. The base case is clear (choose $\psi := \varphi$), similarly $\neg$ and $\wedge$. Additionally any atomic formula (created by $=$ and $\leq$) can be stated via the sgn-function. Wlog we can regard any boolean combination in disjunctive normal form

$$\begin{aligned} B(X, Y) &= \bigvee_i \bigwedge_j (\operatorname{sgn} f_{ij}(X, Y) = \varepsilon_{ij}) \\ \xRightarrow{2.4} \exists X.B(X, Y) &\equiv \bigvee_i \Big( \exists X. \bigwedge (\operatorname{sgn} f_{ij}(X, Y) = \varepsilon_{ij}) \Big) \equiv \bigvee_i B'(X, Y) \equiv B''(X, Y) \end{aligned}$$ $\square$

**2.6 Corollary (Transfer priciple).** *Let $R_1 \subseteq R_2$ be extensions of real closed field. Let $\varphi \in \mathcal{L}(R_1)$ be a sentence. Then $R_1 \models \varphi \Leftrightarrow R_2 \models \varphi$.*

**2.7 Corollary (Artin-Lang-Theorem).** *Let $R \subseteq R_1$ be real closed fields, $A$ a finitely generated $R$-algebra and $\varphi : A \to R_1$ be an $R$-homomorphism. Then there exists an $R$-algebra morphism $\psi : A \to R$.*

*Proof.* We can write $A = R[X_1, \dots, X_n]/I$ where $I = \langle f_1, \dots, f_r \rangle$ (note $A$ is the homomorphic image of a polynomial ring). Put $\xi_i := \varphi(X_i) \in R_1$. Then $\xi := (\xi_1, \dots, \xi_n) \in R_1^n$ satisfies $f_i(\xi) = \varphi(f_i(X)) = 0$. The statement

$$\exists X_1 . \exists X_n . \bigwedge_i f_i(x_1, \dots, x_n) = 0$$

is true over $R_1$. By transfer principle (Corollary 2.6) this formula is true over $R$ as well. Hence there exist $\xi_i' \in R$ (and putting $\xi' := (\xi_1', \dots, \xi_n')$) such that $f_i(\xi) = 0$ for $i = 1, \dots, r$. Thus evaluation at $\xi'$ gives an $R$-algebra morphism $\psi : A \to R$.
We can evaluate $R[X_1, \dots, X_n] \to R$ via $X_i \mapsto \xi_i'$. But under that evaluation $f_i \mapsto f_i(\xi') = 0$. so $\psi(I) = 0$ and we get the diagramme $\square$

$$
\begin{tikzcd}
R[X_1,\dots,X_n] \arrow[r] \arrow[d, dash] & R \\
A = R[X_1,\dots,X_n]/I \arrow[ur] &
\end{tikzcd}
$$

Compare this with the following theorem from Algebra 2:

**Theorem.** *Let $L \subseteq K_1$ be algebraically closed field and $A$ a finitely generated $K$-algebra with $K$-algebra morphism $\varphi : A \to K_1$. Then there exists a $K$-algebra morphism $A \to K$.*

This was used to prove Hilbert's Nullstellensatz. So it is reasonable that we use Artin-Lang to show the real Nullstellensatz.

## 2.2 Hilbert's 17-th problem

Let $f \in \mathbb{R}[X_1, \dots, X_n]$ be such that $\forall x \in \mathbb{R}^n . f(x) \geq 0$.
**Question:** Is $f$ a sum of squares?
The degree must be even, so out $2d = \deg f$. Some easy answers we know from Linear Algebra:

- true for $n = 1$
- true for $d = 1$ and $n \geq 1$.
- true for $n = 2$ and $d = 2$, bivariate quartics

Hilbert: The answer is "no" in all other cases.

**Example (Motzkin's counter-example).** *Define $f := Z^6 + x^4Y^2 + X^4Y^2 - 3X^2Y^2Z^2$. Then by AM-GM-inequality we have*

$$\frac{1}{3}\left(Z^6 + X^4Y^2 + X^2Y^4\right) \geq \sqrt[3]{Z^6 \cdot X^4Y^2 \cdot X^2Y^4} = X^2Y^2Z^2$$

*Thus $f(x, y, z) \geq 0$ for all $x, y, z \in \mathbb{R}$.*
*Now suppose $f = g_1^2 + \ldots + g_t^2$ with $g_i \in \mathbb{R}[X, Y, Z]$. Note that $f$ is homogeneous of degree 6, so wlog the $g_i$ are homogeneous of degree 3. None of the $g_i$ may contain $X^3$ or higher, since the leading coefficient of $X^6$ would be a sum of squares, hence positive. Neither do they contain $Y^3, X^2Z, Y^2Z, XZ^2, YZ^2$. Hence they are linear combinations of $X^2Y, XY^2, XYZ, Z^3$. Therefore the only way to obtain $X^2Y^2Z^2$ is to square $XYZ$, but this always yields a positive coefficient.*

**Remark (Barvinok, Blekkerman).** *Let $P_{n,d} := \{f \in \mathbb{R}[X_1, \dots, X_n]_{2d} : f \geq 0\}$. This is a convex cone. But*

$$\Sigma_{n,d} = \left\{ \sum_{i=1}^{k} g_i^2 : g_i \in \mathbb{R}[X_1, \dots, X_n]_d \right\} \subseteq P_{n,d}$$

*is a convex cone as well. It can be shown that this is a proper cone, but even more, if we restrict to the unit ball in $\mathbb{R}^n$, then*

$$\frac{\operatorname{vol}(\Sigma_{n,d})}{\operatorname{vol}(P_{n,d})} \xrightarrow{n \to \infty} 0$$

*with an exponential decrease (d fixed).*

**2.8 Theorem (Hilbert's 17-th problem, Artin 1927).** *Let $f \in \mathbb{R}[X_1, \dots, X_n]$ be such that $\forall x \in \mathbb{R}^n . f(x) \geq 0$. Then $f$ is a sum of squares of rational functions.*

*Proof.* Put $K := \mathbb{R}(X_1, \dots, X_n)$. Suppose $f \notin \Sigma K^2$. By chapter 1 there is an ordering $\leq$ on $K$ such that $f < 0$. Let $R$ be the real closure of $(K, \leq)$. We have $-f > 0$, so there is some $z \in R$ such that $-f = z^2$. Consider the following statement in $\mathcal{L}(\mathbb{R})$: ref

$$\varphi := \exists X_1 \dots \exists X_n . \exists z . f(X_1, \dots, X_n) + z^2 = 0 \wedge z \neq 0$$

We know that $\varphi$ holds over $R$, but it also is a statement over $\mathbb{R}$. By Corollary 2.6 we have $\exists x_1, \dots, x_n, z \in \mathbb{R} . f(x_1, \dots, x_n) + z^2 = 0 \wedge z \neq 0$. So $f(x_1, \dots, x_n) < 0$ which is a contradiction. $\square$

**Remark (Supplement).** *Let $k \subseteq \mathbb{R}$ be some subfield (e.g. $k = \mathbb{Q}$) and $f \in k[X_1, \dots, X_n]$ such that $\forall \xi \in k^n . f(\xi) \geq 0$. Then there are $a_1, \dots, a_t \in k$ with $a_i > 0$ and $g_1, \dots, g_t \in k(X_1, \dots, X_n)$ such that $f = \sum a_i g_i^2$.*

*Proof.* Look at

$$P := \left\{ \sum_{i=1}^{t} a_i g_i^2 : a_i \in k, a_i > 0, g_i \in k(X_1, \dots, X_n) \right\}$$

This is the cone in $k(X_1, \dots, X_n)$ generated by $\{a \in k : a > 0\}$. So $P$ is the intersection of all positive cones of orderings of $k(X_1, \dots, X_n)$ containing $\{a \in k : a > 0\}$. Now suppose $f \notin P$. Then there is an ordering $\leq$ of $k(X_1, \dots, X_n)$ such that $f < 0$. Let $R$ be the real closure of $(k(X_1, \dots, X_n), \leq)$ and let $\widetilde{k}$ denote the real closure of $k$, so $\widetilde{k} \subseteq R$. By Corollary 2.6 we have $\exists \xi \in \widetilde{k}^n . f(\xi) < 0$. But $\mathbb{Q} \subseteq k$ and $\mathbb{Q}$ is dense in $\mathbb{R}$. By assumption we have $\forall \xi \in \mathbb{R}^n . f(\xi) \geq 0$ ↯

check

$\square$

# 3 Real Algebra

## 3.1 Digression on commutative Algebra

Let $A$ be a commutative ring, $I \subset A$ an ideal.

**Definition.** *A* minimal prime ideal *over $I$ is a prime ideal $p$ of $A$ such that $I \subseteq p$ and $p$ is minimal with that property. That is if $p'$ is a prime ideal with $I \subseteq p' \subseteq p$, then $p = p'$.*

**Definition.** *The* radical *of $I$ is the ideal $\sqrt{I} := \{a \in A : \exists n \in \mathbb{N} . a^n \in I\}$.*

Note that $I \subseteq \sqrt{I}$.

**Example.** *Let $A = \mathbb{Z}$, so every ideal is principal. Let $I = (a)$ for $a = p_1^{e_1} \dots p_r^{e_r}$. Then $\sqrt{(a)} = (p_1 \dots p_r) = \bigcap_{i=1}^{r} (p_i)$.*

**Theorem.** *1. Every proper ideal has a minimal prime ideal.*

*2. $\sqrt{I}$ is the intersection of the minimal prime ideals over $I$.*

*3. (E.Noether) If $A$ is noetherian, then there are only finitely many minimal primes.*

*Proof.* 1. The set $\{p \text{ prime ideal} : I \subseteq p\}$ is non-empty, since $I$ can be extended to a maximal ideal. With Zorn's Lemma we can show that this set has a minimal element.

2. Note that if $p$ is prime and $I \subseteq p$, then $\sqrt{I} \subseteq p$. (If $a \in \sqrt{I}$, then $a^n \in I$, so $a \in I$.) Hence $\sqrt{I}$ is contained in the intersection. To show equality we assume wlog $I = 0$ (otherwise go to $A/I$). Assume $a \notin \sqrt{0}$, so $a$ is not nilpotent, which means $\forall n. a^n \neq 0$. Thus $S := \{a^n : n \in \mathbb{N}\}$ does no intersect 0. (Then $S$ is muliplicative, and we can work in $S^{-1}A$.) There is a maximal ideal $J$ not intersection $S$ (Zorn's Lemma).

   Claim: $J$ is a prime ideal.
   Suppose $a, b \in A \setminus J$, but $ab \in J$. Then by maximality $((a)+J) \cap S \neq 0$ and $((b)+J) \cap S \neq 0$. Therefore we get $s = ca + x$ and $s' = c'b + y$ for some $c, c' \in A$, $s, s' \in S$ and $x, y \in J$. Thus $S \ni ss' = cc'ab + z \in J$ for some $z \in J$. But $S$ and $J$ do not intersect. ↯

3. Suppose there is an ideal $I$ of $A$ with infinitely many minimal primes. Since $A$ is noetherian, we can assume that $I$ is maximal with this property. Then $I$ is not prime. Hence there are $a, b \in A \setminus I$ such that $ab \in I$. For any prime $p \supseteq I$ we must have $a \in p$ or $b \in p$. So $I + (a) \subseteq p$ or $I + (b) \subseteq b$. So if $p_1, p_2, \dots$ are infinitely many minimal primes over $I$, there is a partition $\mathbb{N}_+ = C_1 \oplus C_2$ such that $i \in C_1 \implies I + (a) \subseteq p_i$ and $j \in C_2 \implies I + (b) \subseteq p_j$. Wlog $C_1$ is infinite, so $I + (a)$ has infinitely many minimal primes, contradicting the maximality of $I$. □

## 3.2 Real Nullstellensatz

**Definition.** *An ideal $I \subseteq A$ is called* real *if*

$$\forall n. \forall a_1, \dots, a_n \in A. a_1^2 + \dots + a_n^2 \in I \implies a_1, \dots, a_n \in I$$

Compare this to $\mathbb{R}$ where $\sum a_i^2 = 0 \implies a_i = 0$, which holds in any real field.

**Remark.** *Assume $I$ is a prime ideal of $A$. Let $K$ be the quotient field of $A/I$. Then $I$ is real iff $K$ is a real field.*

As a motivation we recall from Algebra 2

**Theorem (Hilbert's Nullstellensatz, weak version).** *Let $K$ be an algebraically closed field and $f_1, \dots, f_s \in K[X_1, \dots, X_n]$ such that $f_1(x) = 0, \dots, f_s(x) = 0$ has no solution in $K^n$. Then there are $g_1, \dots, g_s \in K[X_1, \dots, X_n]$ such that $\sum_{i=1}^s g_i f_i = 1$.*

Now we replace "algebraically closed" by "real closed".

**3.1 Theorem (Real Nullstellensatz).** *Let $R$ be a real close field, $f_1, \dots, f_s \in R[X_1, \dots, X_n]$ be such that $f_1(x) = 0, \dots, f_s(x) = 0$ has no solution in $R^n$. Then there are $g_1, \dots, g_s, p_1, \dots, p_t \in R[X_1, \dots, X_n]$ such that*

$$\sum_{i=1}^{s} g_i f_i = 1 + \sum_{j=1}^{t} p_j^2 \tag{5}$$

**Remark.** *Again, as in Hilbert's case, the converse holds as well. If we had the above representation and $\xi$ were a common solution, then $0 = \sum g_i f_i(\xi) = 1 + \sum p_j^2(\xi) \geq 1$ is a contradiction.*

**3.2 Lemma.** *Assume $A$ is a noetherian commutative ring and $I \subseteq A$ is a real ideal. Then we have:*

1. *I is a radical ideal.*

2. *All minimal prime ideals of I are real.*

*Proof.* 1. Let $a^n \in I$. We do induction on $n$. For $n = 1$ we have $a \in I$, so let $n > 1$. If $n$ is even, we have $\left(a^{\frac{n}{2}}\right)^2 = a^n \in I$, but the left part is a (sum of) square(s). So $a^{\frac{n}{2}} \in I$. If $n$ is odd, we get $\left(a^{\frac{n+1}{2}}\right)^2 = a^{n+1} \in I$, so $a^{\frac{n+1}{2}} \in I$. In both cases we are done by induction hypothesis.

2. By item 1 $I$ is redical. Let $p_1, \dots, p_t$ be the minimal prime ideals of $I$. Suppose $p_1$ is not real and assume $a_1^2 + \dots + a_n^2 \in p_1$ for some $a_1, \dots, a_n \in A \setminus p_1$ (we do not have to regard squares which lie in $p_1$, since those get absorbed anyway). Let $b_i \in p_i \setminus p_i$ for $i = 2, \dots, t$. Then $b := b_2 \dots b_t \notin p_1$, since it is a prime ideal, but $b \in p_2 \cap \dots \cap b_t$. Now we multiply the above sum with $b^2$ and obtain

$$(a_1 b)^2 + \dots + (a_n b)^2 \in p_1 \cap \dots \cap p_t = \sqrt{I} = I$$

Since $I$ is real, we get $a_1 b \in I \subseteq p_1$, which is a contradiction. $\square$

**Notation.** *Let $V \subseteq R^n$, $F \subseteq R[X_1, \dots, X_n]$ and $R$ be real closed. Then we define*

$$J(V) := \{f \in R[X_1, \dots, X_n] : \forall \xi \in V. f(\xi) = 0\} \qquad \text{the vanishing ideal}$$
$$Z(F) := \{\xi \in R^n : \forall f \in F. f(\xi) = 0\} \qquad \text{the zero set}$$

*For $F = \{f_1, \dots, f_n\}$ we also write $Z(F) = Z(f_1, \dots, f_n)$.*

**Remark.**

- *Let $I := \langle F \rangle$ be the generated ideal. Then $Z(I) = Z(F)$.*
- *$\overline{V} := Z(J(V))$ is the Zariski-closure of $V$, by definition.*
- *Suppose $V = Z(F)$. Then $\overline{V} = V$, i.e. $V$ is Zariski-closed.*

**Remark.** *$J(V)$ is a real ideal.*

*Proof.* Suppose $f_1^2 + \dots + f_s^2 \in J(V)$ for some $f_i \in R[X_1, \dots, X_n]$. Take $\xi \in V$ and evaluate, then $f_1(\xi)^2 + \dots + f_s(\xi)^2 = 0$, which is an equality in the real field $R$. Therefore $f_1(\xi) = \dots = f_s(\xi) = 0$, which means $f_1, \dots, f_s \in J(V)$. $\square$

Now we can reformulate the real Nullstellensatz.

**3.3 Theorem (Real Nullstellensatz, (Dubois '69, Risler '70)).** *Let $R$ be a real closed field and $I \subseteq R[X_1, \dots, X_n]$ a real ideal. Then*

$$J(Z(I)) = I$$

*Proof.* **$J(Z(I)) \supseteq I$:** Let $f \in I$ and $\xi \in Z(I)$. Then by definition $f(\xi) = 0$, so $f \in J(Z(I))$.

**$J(Z(I)) \subseteq I$:** For $f \in R[X_1, \dots, X_n] \setminus I$ there exists some $x \in Z(I)$ such that $f(x) \neq 0$. If $f \notin I$, then there is some minimal prime ideal $p$ such that $I \subseteq P$ and $f \notin p$. By Lemma 3.2 $p$ is real. Assume $g_1, \dots, g_t$ generate the ideal $p$ (finitely many, since noetherian). The quotient field $K$ of $R[X]/p$ is real. Let $R_1$ be the real closure of $K$. Then we obtain a canonical morphism

$$\varphi : R[X] \to R[X]/p \rightsquigarrow K \rightsquigarrow R_1 \text{ denoted } X_i \mapsto \overline{X_i}$$

We have $f(\overline{X_1}, \dots, \overline{X_n}) \neq 0$ and $g_i(\overline{X_1}, \dots, \overline{X_n}) = 0$ for $i = 1, \dots, t$ (as polynomials). By transfer principle there are $x_1, \dots, x_n \in R$ such that $f(x_1, \dots, x_n) \neq 0$ and $g_i(x_1, \dots, x_n) = 0$ for $i = 1, \dots, t$. So $x := (x_1, \dots, x_n) \in R^n$ satisfies $x \in Z(\{g_1, \dots, g_t\}) = Z(p) \subseteq Z(I)$, since $I \subseteq p$. So $x \in Z(I)$ but $f(x) \neq 0$. $\square$

**Definition.** *Let $A$ be a commutative ring, $I \subseteq A$ an ideal. The* real radical $\sqrt[R]{I}$ *is defined as the smallest real ideal containing $I$.*

**Proposition.** *We have the explicit form*

$$\sqrt[R]{I} = \left\{a \in A : \exists m \in \mathbb{N}.\exists b_1, \ldots, b_t \in A. a^{2m} + b_1^2 + \ldots + b_t^2 \in I\right\}$$

*Proof.* **RHS is an ideal:** Let $a \in$ RHS and $c \in A$. Then

$$(ac)^{2m} + (b_1 c^m)^2 + \ldots + (b_t c^m)^2 = c^{2m} \cdot (\ldots) \in I \implies ac \in \text{RHS}$$

Let $a, a' \in$ RHS, say $a^{2m} + \sum b_i^2 \in I$ and $(a')^{2m'} + \sum b_i'^2 \in I$. We use the trick

$$(a + a')^{2(m+m')} + (a - a')^{2(m+m')} = a^{2m} \cdot c + (a')^{2m'} \cdot c'$$

for some $c, c'$, which are sums of squares, since all the odd powers cancel out and at least one of $a, a'$ has sufficiently high power. Finally this yields

$$\begin{aligned}(a + a')^{2(m+m')} &+ (a - a')^{2(m+m')} + c(b_1^2 + \ldots + b_t^2) + c'(b_1'^2 + \ldots + b_t'^2) \\ &= c\left(a^{2m} + \sum b_i^2\right) + c'\left((a')^{2m'} + \sum b_i'^2\right) \in I\end{aligned}$$

and on the left hand side we in fact have a sum of squares.

**RHS is real ideal:** Let $a_1^2 + \ldots + a_n^2 \in$ RHS. We have

$$a_1^{4m} + \text{s.sq.} = (a_1^2 + \ldots + a_n^2)^{2m} + \text{s.sq.} \in I$$

so $a_1 \in$ RHS, the same for all $a_i$.

**minimal:** Let $I \subseteq J$, $J$ a real ideal. Let $a \in$ RHS via $(a^m)^2 + b_1^2 + \ldots + b_t^2 \in I \subseteq J$. Since $J$ is real we get $a^m \in J$ and since $J$ is radical, this means $a \in J$. □

**Remark.** *1. We have $I \subseteq \sqrt{I} \subseteq \sqrt[R]{I}$ for any ideal $I$ in a commutative ring.*

*2. Let $I \subseteq R[X_1, \ldots, X_n]$ for some real field $R$, then $Z(\sqrt[R]{I}) = Z(I)$.*

*Proof.* 1. Let $a \in \sqrt{I}$, via $a^m \in I$. Then $a^{2m} \in I$, so $a \in \sqrt[R]{I}$.

2. $Z(\cdot)$ has inverse inclusion, so $Z(I) \subseteq Z(\sqrt[R]{I})$ is clear with the above. For the other way, let $\xi \in Z(I)$ and $f \in \sqrt[R]{I}$, say $f^{2m} + g_1^2 + \ldots + g_t^2 \in I$. This we evaluate at $\xi$ and obtain

$$f(\xi)^{2m} + g_1(\xi)^2 + \ldots + g_t(\xi)^2 = 0 \text{ in } R$$

Thus $f(\xi)^m = 0$, so $f(\xi) = 0$. Hence $(\xi) \in Z(\sqrt[R]{I}$. □

**3.4 Theorem (Real Nullstellensatz').** *Let $R$ be a real closed field, $I \subseteq R[X_1, \ldots, X_n]$ an ideal. Then $J(Z(I)) = \sqrt[R]{I}$.*

*Proof.* We have $Z(\sqrt[R]{I}) = Z(I)$. Now apply the Real Nullstellensatz (Theorem 3.3) to the real ideal $\sqrt[R]{I}$. □

**Theorem.** *Let $R$ be real closed, $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$ such that the system $f_1(X) = 0, \ldots, f_s(X) = 0$ has no solution in $R^n$. Then there are polynomials $g_1, \ldots, g_s, p_1, \ldots, p_t \in R[X_1, \ldots, X_n]$ such that*

$$\sum_{i=1}^{s} g_i f_i = 1 + \sum_{i=1}^{t} p_i^2$$

*Proof.* Put $I := \langle f_1, \ldots, f_s \rangle$. Since we do not have a solution, we have $Z(I) = \emptyset$. Thus $J(Z(I)) = R[X_1, \ldots, X_n]$. By Theorem 3.4 we have $1 \in \sqrt[R]{I}$. Using the characterisation, there exist $p_1, \ldots, p_t$ such that $1^{2m} + p_1^2 + \ldots + p_t^2 \in I$. $\square$

**Example.** *Consider* $\mathbb{R}[X,Y]$ *with* $I = (X^2 + Y^2 + 1)$. *Then* $Z(I) = \emptyset$ *and thus* $J(Z(I)) = (1) = \mathbb{R}[X,Y] = \sqrt[R]{I}$. *However, if we lift the definition to* $\mathbb{C}$, *then* $\sqrt[R]{I} = I$.
*Now we alter the ideal to* $I = (X^2 + Y^2)$. *Then* $Z(I) = \{(0,0)\}$, *and* $J(Z(I)) = (X,Y)$.
*Check* $(X,Y) = \sqrt[R]{X^2+Y^2}$: *Clearly* $X^2 + Y^2 \in (X,Y)$ *and by the characterisation of real ideals we have equality.*

## 3.3 Cones in Commutative Rings

In section 1.1 we defined cones in fields.

**Definition.** *A* cone $P$ *of* $A$ *is a subset* $P \subseteq A$ *such that*

1. $\forall a, b \in P. a + b \in P$
2. $\forall a, b \in P. ab \in P$
3. $\forall a \in A. a^2 \in P$.

*The cone* $P$ *is called* proper *if* $-1 \notin P$.

**Remark.** *The set*

$$\Sigma A^2 = \left\{ \sum_{i=1}^{n} a_i^2 : n \in \mathbb{N}, a_1, \ldots, a_n \in A \right\}$$

*is a cone of* $A$. *It is contained in all cones of* $A$.

**Example.** *Let* $M \subseteq R^n$, *for some real closed field* $R$. *Then* $\{f \in R[X_1, \ldots, X_n] : \forall \xi \in M. f(\xi) \geq 0\}$ *is a cone of* $A$. *Basically, we just took* $J(M)$ *and replaced "$=$" by "$\geq$".*

**Remark.** *The intersection of a family of cones of* $A$ *is a cone of* $A$.

**Definition.** *Let* $a_1, \ldots, a_r \in A$. *Denote by* $P[a_1, \ldots, a_r]$ *the smallest cone of* $A$ *containing* $a_1, \ldots, a_r$.

**Example.**

1. $P[a] = \{x + ya : x, y \in \Sigma A^2\}$, *because any powers of* $a$ *get absorbed in* $x$ *and* $y$.
2. $P[a_1, a_2] = \{x_{00} + x_{10}a_1 + x_{01}a_2 + x_{11}a_1a_2 : x_{ij} \in \Sigma A^2\}$.

*So technically, we just have* $P[a_1, \ldots, a_r] = (\Sigma A^2)[a_1, \ldots, a_r]$ *in the sense of adjoining elements and every adjunction is of degree 2.* check word

**Definition.** *A* prime cone $P$ *of* $A$ *is a proper cone* $P$ *of* $A$ *such that*

$$\forall a, b \in A. ab \in P \implies a \in P \vee -b \in P$$

**Example.** *Let* $A = K$ *be a field and* $P = \{x \in K : x \geq 0\}$ *be the positive cone of some ordering. Then* $P$ *is a prime cone:*
*Assume* $ab \in P$, *i.e.* $ab \geq 0$. *If* $a \geq 0$ *we're fine. Otherwise* $a < 0$. *But then* $b \leq 0$, *so* $-b \geq 0$.

**3.5 Proposition.** *Let* $P$ *be a prime cone of* $A$ *and put* $-P := \{-a : a \in P\}$. *Then*

1. $P \cup -P = A$
2. $P \cap -P$ *is a prime ideal of* $A$*, called the* support*,* $\operatorname{supp} P$*.*

*Proof.* 1. Let $a \in A$, then $a \cdot a = a^2 \in P$, so $a \in P$ or $-a \in P$, which means $a \in -P$.

2. $P$ and $-P$ are closed under addition and negation, so it is an additive subgroup. Let $a \in P \cap -P$ and $b \in A$. Then $b \in P$ or $b \in -P$. Assume $b \in P$. Then $ab \in P$ and $(-a)b \in P$, so $ab \in P \cap -P$. Similarly for $b \in -P$, so $P \cap -P$ is an ideal.

   Check prime: Let $ab \in P \cap -P$ and $a \notin P \cap -P$. If $a \notin P$, then from the above $ab \in P$ implies $-b \in P$. But we also have $a(-b) \in P$, which implies $b \in P$, so $b \in P \cap -P$. Analogous for $-a \notin P$. □

**Example (cont.).** *We have* $P = \{x \in K : x \geq 0\}$*. Then* $P \cap -P = \{0\}$*, by computation or because it is the only prime ideal of a field.*

**Remark.** *Prime cones of a field* $K$ *are the positive cones of orderings of* $K$*.*

**3.6 Proposition.** *A subset* $P$ *of* $A$ *is a prime cone of* $A$ *iff there is an ordered field* $(K, \leq)$ *and a ring homomorphism* $\varphi : A \to K$ *such that*

$$P = \{a \in A : \varphi(a) \geq 0\} \tag{6}$$

*Proof.* Suppose we have $\varphi : A \to K$ with eq. (6). Then clearly$P$ is a proper cone, just use the properties of the cone of $K$. To show that $P$ is prime suppose $ab \in P$. Then $\varphi(a)\varphi(b) = \varphi(ab) \geq 0$. Then either $\varphi(a) \geq 0$, which means $a \in P$ or $\varphi(a) < 0$. But then $\varphi(b) \leq 0$,so $\varphi(-b) \geq 0$, which means $-b \in P$.
For the other direction, if we had $\varphi$, we would have

$$\ker \varphi = \{a \in A : \varphi(a) \geq 0 \wedge \varphi(-a) \geq 0\} = P \cap -P = \operatorname{supp} P$$

Let $P$ be some prime cone. Then we put $I := \operatorname{supp} P$, which is a prime ideal. Then we take the canonical morphism $\varphi : A \to A/I \hookrightarrow \operatorname{Fr}(A/I) =: K$. For $K$ we define the cone $Q := \left\{\frac{\varphi(a)}{\varphi(b)} : a, b \in P, b \notin\right\}$, which induces an ordering of $K$. □

**3.7 Theorem.** *Let* $A$ *be a commutative ring. TFAE*

1. *A has a proper cone.*
2. *A has a prime cone.*
3. *There is a morphism* $\varphi : A \to K$ *for some real field* $K$*.*
4. *A has a real prime ideal.*
5. $-1 \notin \Sigma A^2$

gap

**Definition.** *A* Real algebraic set $V \subseteq R^n$ *is the zero set of polynomials* $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$*.*

$$V = \{\xi + R^n : f_i(\xi) = \ldots = f_m(\xi) = 0\}$$

*The* coordinate ring $R[V]$ *consists of the restrictions of the polynomial functions to* $V$*.*

$$V \to R \quad \xi \mapsto p(\xi)$$

$R[X_1, \ldots, X_n]$ $\quad$ $R[V]$

$R[X_1, \ldots, X_n]/I(V)$

This gives the picture

**Corollary (Variants of the Positivstellensatz).** *Let $V \subseteq R^n$ be a real algebraic set, $R$ some real closed field. Let $g_1, \ldots, g_s \in R[V]$ and*

$$W := \{\xi \in V : g(\xi) \geq 0, \ldots, g_s(\xi) \geq 0\}$$

*Let $P \subseteq R[V]$ denote the cone generated by $g_1, \ldots, g_s$. Let $f \in R[V]$. Then*

1. $\forall \xi \in W. f(\xi) \geq 0$ *iff* $\exists e \in \mathbb{N}. \exists p, q \in P. fp = f^{2e} + q$
2. $\forall \xi \in W. f(\xi) > 0$ *iff* $\exists p, q \in P. fp = 1 + q$
3. $\forall \xi \in W. f(\xi) = 0$ *iff* $\exists e \in \mathbb{N}. \exists p \in P. f^{2e} + p = 0$

*Proof.* Let $I(V) = \langle h_1, \ldots, h_r \rangle$ for some $h_i \in R[V]$ (these exist since the ideal is finitely generated).

1. $\forall \xi \in W. f(\xi) \geq 0$ means $S := \{\xi \in R^n : h_i(\xi) = 0, g_j(\xi) \geq 0, -f(\xi) \geq 0, f(\xi) \neq 0\}$ is empty. The elements of the cone generated by $g_1, \ldots, g_s, -f$ are of the form $p(-f) + q$ with $p, q \in P$. By theorem 2we get $S = \emptyset \Leftrightarrow \exists p, q \in P. \exists e \in \mathbb{N}. p(-f) + q + f^{2e} \in \langle h_1, \ldots, h_r \rangle$. So in $R[V]$ we get the equality $q + f^{2e} = fp$. ref
2. The LHS-condition means $S := \{\xi \in R^n : h_i(\xi) = 0, g_j(\xi) \geq 0, -f(\xi) \geq 0\}$ is empty. By theorem 2$S = \emptyset \Leftrightarrow \exists p, q \in P. p(-f) + q + 1^2 \in \langle h_1, \ldots, h_r \rangle$. So in $R[V]$ this becomes $fp = 1 + q$. ref
3. The LHS-condition means $S := \{\xi \in R^n : h_i(\xi) = 0, g_j(\xi) \geq 0, -f(\xi) \neq 0\}$ is empty. By theorem 2$S = \emptyset \Leftrightarrow \exists p \in P. \exists e \in \mathbb{N}. p + f^{2e} \in \langle h_1, \ldots, h_r \rangle$. So in $R[V]$ this becomes $p + f^{2e} = 0$. ref

$\square$

**Example (Blekherman, Parillo, Thomas; SIAM).** *Let $f = X_1^2 + X_2^2 - 1$ be the circle, $g_1 := 3X_2 - X_1^3 - 2$ and $g_2 := X_1 - 8X_2^3$. We consider the system $f(x) = 0$,$g_1(X) \geq 0$ and $g_2(X) \geq 0$.*

*draw the $g_i$*

*By drawing you see that the system has no solution. By theorem 2this means that there exists some $p \in P[g_1, g_2]$ such that $p + 1 \in \langle f \rangle$. In other words, there exist $s_0, s_1, s_2, s_{12} \in \sum \mathbb{R}[X_1, X_2]^2$ and $t \in \mathbb{R}[X_1, X_2]$ such that* ref

$$s_0 + s_1 g_1 + s_2 g_2 + s_{12} g_1 g_2 + tf = -1$$

*The problem is, that the theory does not tell us how to find these values. One can take*

$$\begin{aligned}
s_0 &= \frac{5}{43}X_1^2 + \frac{387}{44}\left(X_1X_2 - \frac{32}{129}X_1\right)^2 + \frac{11}{5}\left(-X_1^2 - \frac{1}{22}X_1X_2 - \frac{5}{1}X_1 + X_2^2\right)^2 \\
&\quad + \frac{1}{20}\left(-X_1^2 + 2X_1X_2 + X_2^2 + 5X_2\right)^2 + \frac{3}{4}\left(2 - X_1^2 - X_2^2 - X_2\right)^2 \\
s_1 &= 3 \\
s_2 &= 1 \\
s_{12} &= 0 \\
t &= -3X_1^2 + X_1 - 3X_2^2 + 6X_2 - 2
\end{aligned}$$

*It turns out there is a nice connection to optimisation.*

## 3.4 Link to semidefinite optimisation

Linear programming deals with optimising a linear function over a polyhedra.

$$\begin{aligned} \text{minimise } & c^T x \\ \text{subject to } & Ax = b \\ & x \geq 0 \end{aligned}$$

For the *feasibility problem* we only ask whether there is some $x \in \mathbb{R}^n_+$ such that $Ax = b$. There are efficient (polynomial time) algorithms for both of the problems.

- Simplex method: Start somewhere, in each step go to a neighbouring node of the polytope with higher target value; exponential worst-case, but best average case
- interior-point method: going through the inner part of the polytope, using Newton method
- Semidefinie Programming: $S_+ := \{X \in \mathbb{R}^{n \times n} : X^T = X, \text{ positive semidefinite}\}$, that is $\forall v \in \mathbb{R}^n . v^T X v \geq 0$.