Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Dr. Maria Infusino
Dr. Charu Goel

REAL ALGEBRAIC GEOMETRY–WS 2014/15

Solution to the Christmas Assignment

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

a) The system $\mathcal{I}$ covers K since for any $x \in K$, $x \in]x-1, x+1[$.
To show that $\mathcal{I}$ is closed under finite intersections, it suffices to consider the intersection of two elements in $\mathcal{I}$. Let $A, B \in \mathcal{I}$. Then we can distinguish four main cases (draw a picture to help yourself to see the different cases):

- At least one between A and B is the empty set. Then $A \cap B = \emptyset \in \mathcal{I}$ since $\emptyset =]a, a[$ for any $a \in K$.
- $A, B \neq \emptyset$ and $A \cap B = \emptyset$. Then $A \cap B \in \mathcal{I}$.
- $A, B \neq \emptyset$ and either $A \subseteq B$ or $B \subseteq A$. Then $A \cap B \in \{A, B\} \in \mathcal{I}$.
- $A, B \neq \emptyset$ and $A \cap B \neq \emptyset$ and neither $A \subseteq B$ or $B \subseteq A$.
  Since $A, B \neq \emptyset$, let us denote them by $A =]a, b[$ and $B =]c, d[$ with $a < b \in K$ and $c < d \in K$. Then the other assumptions imply that we can have only two cases either $a < c < b < d$ or $c < a < d < b$. In the first case $A \cap B =]c, b[\in \mathcal{I}$ and in the second case $A \cap B =]a, d[\in \mathcal{I}$

b) Consider $a \in K^\times$ and any $\epsilon > 0$ in K. W.l.o.g. suppose that $\epsilon < \frac{1}{|a|}$. We need to find some $\delta > 0$ such that, whenever $x \in]|a| - \delta, |a| + \delta[$, we have $\frac{1}{x} \in \left] \frac{1}{|a|} - \epsilon, \frac{1}{|a|} + \epsilon \right[$.
The latter relation implies that

$$0 < \delta < \frac{\epsilon |a|^2}{1 + \epsilon |a|}.$$

Then it remains to show that this condition is also sufficient. This easily follows by noting that $\frac{\epsilon|a|^2}{1+\epsilon|a|} < \frac{\epsilon|a|^2}{1-\epsilon|a|}$ since $0 < 1 - \epsilon|a| < 1 + \epsilon|a|$.

c) Let $\mathcal{B}$ be the basis for the product topology on K^n given by the interval topology on K, i.e. the collection of all the hypercubes of the form

$$\prod_{i=1}^{n}]a_i, b_i[\text{ for any } n \in \mathbb{N},\ a_i, b_i \in K \text{ for } i = 1, \dots, n,$$

and $\mathcal{B}'$ be the basis for the euclidean topology on K^n, i.e. the collection of all the open balls of the form

$$B\big((a_1, \dots, a_n), r\big) := \left\{ (x_1, \dots, x_n) \in K^n \mid \sqrt{(x_1 - a_1)^2 + \dots + (x_n - a_n)^2} < r \right\}$$

for any $a_i, r \in K$ with $r > 0$.
It suffices to show that $\mathcal{B}$ and $\mathcal{B}'$ are equivalent bases. Thus, we need to show that, for any hypercube $H \in \mathcal{B}$, there exist two balls $B_1, B_2 \in \mathcal{B}'$ such that $B_1 \subseteq H \subseteq B_2$. Let $H := \prod_{i=1}^{n}]a_i, b_i[$ for some $n \in \mathbb{N}$, $a_i, b_i \in K$ for $i = 1, \dots, n$. Then we get our conclusion just by taking

$$B_1 := B\left(\left(\frac{a_1 + b_1}{2}, \dots, \frac{a_n + b_n}{2} \right), \min\left\{ \frac{b_i - a_i}{2} : i = 1, \dots, n \right\} \right)$$

and

$$B_2 := B\left(\left(\frac{a_1+b_1}{2},\ldots,\frac{a_n+b_n}{2}\right), \max\left\{\frac{b_i-a_i}{2} : i=1,\ldots,n\right\}\right).$$

2) Let $(R,\leq)$ be a real closed field. Consider $Pos(R) := \{x \in R \mid x > 0\}$.

a) Let us first show that the subset $Pos(R) \subset R^\times$ is a subgroup of $(R^\times,\cdot)$.

- $(Pos(R),\cdot)$ is closed under multiplication, since:

$$g_1, g_2 \in Pos(R) \overset{\text{def}}{\Longleftrightarrow} g_1 > 0,\ g_2 > 0 \overset{\text{R ord.field}}{\Longrightarrow} g_1 \cdot g_2 > 0 \overset{\text{def}}{\Longleftrightarrow} g_1 \cdot g_2 \in Pos(R)$$

- $(Pos(R),\cdot)$ is closed under inverse, since:

$$g \in Pos(R) \overset{\text{def}}{\Longleftrightarrow} g > 0 \overset{\text{R ord.field}}{\Longrightarrow} \frac{1}{g} > 0 \overset{\text{def}}{\Longleftrightarrow} \frac{1}{g} \in Pos(R)$$

Note that $(R^\times,\cdot)$ is an abelian group since R is a field. Therefore, $Pos(R)$ is an abelian subgroup of $(R^\times,\cdot)$. Moreover, since $(R,\leq)$ is a totally ordered set, the restriction of the ordering $\leq$ to $Pos(R)$ is also a total ordering on $Pos(R)$. Hence, $(Pos(R),\leq)$ is a totally ordered set.
By Definition 1, it remains to show only that the property (1) holds. Indeed, this is true since for any $g_1, g_2, h \in Pos(R)$ such that $g_1 \geq g_2$ we have that:

$$g_1 \geq g_2 > 0 \text{ and } h > 0 \overset{\text{R ord.field}}{\Longrightarrow} g_1 \cdot h = h \cdot g_1 \geq g_2 \cdot h = h \cdot g_2.$$

Hence, we have proved that $Pos(R)$ is an ordered abelian subgroup of $(R^\times,\cdot)$

b) Let us now show that $(Pos(R),\cdot)$ is divisible. Let $a \in Pos(R)$ and for any $n \in \mathbb{N}$ let $f_n(x) = x^n - a$. Then we have:

- $f_n(0) = -a < 0$ since $0 < a \in R$ and R is an ordered field
- $f_n(1+a) = (1+a)^n - a = \sum_{k=0}^{n} \binom{n}{k} a^k - a = 1 + na + \left(\sum_{k=2}^{n} \binom{n}{k} a^k\right) - a = 1 + a(n-1) + \left(\sum_{k=2}^{n} \binom{n}{k} a^k\right) > 0$

By the intermediate value theorem (applicable since R is a real closed field), $\exists\, c \in]0, 1+a[\subset R$ such that $f_n(c) = 0$. Thus we have showed that for any $n \in \mathbb{N}$, $\exists\, c = \sqrt[n]{a} \in R$ with $c > 0$, i.e. for any $n \in \mathbb{N}$, $\sqrt[n]{a} \in Pos(R)$. Then, since $(Pos(R),\cdot)$ is closed under multiplication, we have that for any $m \in \mathbb{N}_0$ and $n \in \mathbb{N}$, $a^{\frac{m}{n}} = (\sqrt[n]{a})^m \in Pos(R)$, i.e. for any $q \in \mathbb{Q}$, $a^q \in Pos(R)$.

3) a) Consider some polynomials $p_0, \ldots, p_n \in \mathbb{R}[X]$, and an infinite subset $U \subset \mathbb{R}$ s.t. for all $x \in U$

$$f(x) := p_n(x)(e^x)^n + p_{n-1}(x)(e^x)^{n-1} + \cdots + p_0(x) = 0.$$

Suppose that the p_i's are not all identically 0, and that n is the biggest exponent of e^x for which p_n is non-zero on U.

i) If U has no bound, then it contains an infinite subsequence $(x_k)_{k\in\mathbb{N}}$ tending to $\pm\infty$. For instance, consider the case $x_k \to +\infty$ as $k \to +\infty$. We can write $f(x)$ as follows

$$f(x) = (e^x)^n \left[p_n(x) + \frac{p_{n-1}}{e^x} + \cdots + \frac{p_0}{(e^x)^n}\right].$$

But, for any $l = 1, \ldots, n$, we have

$$\lim_{k\to\infty} \frac{p_{n-l}(x_k)}{(e^{x_k})^l} = 0.$$

Thus, we get

$$\lim_{k\to\infty} f(x_k) = \lim_{k\to\infty} (e^{x_k})^n p_n(x_k) = \pm\infty,$$

which contradicts the fact that for any k, $f(x_k) = 0$.

ii) If U is bounded, then it must have an accumulation point since it is infinite in $\mathbb{R}$. Consider $f(z)$ where z is a complex variable. Note that f is a holomorphic function on the whole complex plane $\mathbb{C}$ as sum and product of e^z, $p_0(z), \dots, p_n(z)$ which are holomorphic functions on $\mathbb{C}$. Now we know that $f(z) = 0$ for all $z \in U \subset \mathbb{R} \subset \mathbb{C}$ then, applying the Identity Theorem of Complex Analysis, we obtain that $f(z) = 0$ for any $z \in \mathbb{C}$. In particular, restricting to the real variable x, we get that $f(x) = 0$ for any $x \in \mathbb{R}$. Then, to get a contradiction, we can apply the same argument as in the preceding item i) by setting $U = \mathbb{R}$.
(For a reference the Identity Theorem of Complex Analysis see e.g. [1, Chapter 3, Theorem 1.2 (ii)] and [2, Chapter 10, Corollary to Theorem 10.18].)

b) Suppose that $\Gamma_{\exp}$ is semi-algebraic in $\mathbb{R}^2$. Then, by the proposition about the normal form of semi-algebraic sets of Lecture 11, we have that $\Gamma_{\exp}$ would be a finite union of basic semi-algebraic sets of the form

$$Z(g) \cap U(g_1, \dots, g_p).$$

for some $p \in \mathbb{N}$ and $g, g_1, \dots, g_p \in \mathbb{R}[X, Y]$.
Now, we proved in part a) of this exercise that for any $0 \not\equiv g \in \mathbb{R}[X, Y]$ the set $Z(g) = \{(x, e^x) \in \mathbb{R}^2 : g(x, e^x) = 0\}$ is finite. Therefore, $\Gamma_{\exp}$ would be a finite union of finite sets and so a finite set that is a contradiction. Hence, $g \equiv 0$ and so $Z(g) = \mathbb{R}^2$. As a consequence, $\Gamma_{\exp}$ would be a finite union of sets $U(g_1, \dots, g_p)$. But in Sheet 7, Exercise 3 b), we proved that for any $h \in \mathbb{R}[X, Y]$, $U(h)$ is open in $\mathbb{R}^2$. Hence, each $U(g_1, \dots, g_p)$ is open in $\mathbb{R}^2$. This would mean that $\Gamma_{\exp}$ contains an open square of $\mathbb{R}^2$, and thus has non-empty interior. As a consequence, $\Gamma_{\exp}$ would contain a vertical segment, which implies that some point in $\mathbb{R}$ has at least two distinct images, contradicting the fact that the exponential is a function.

4) We consider the Motzkin polynomial

$$m(X, Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2.$$

a) Let $a := 1$, $b := X^2Y^4$ and $c := X^4Y^2$. Then for any $(X, Y) \in \mathbb{R}^2$ we have $0 \leq a, b, c \in \mathbb{R}$. Therefore, using the inequality suggested in the hint, we get that for any $(X, Y) \in \mathbb{R}^2$

$$a + b + c \geq 3\sqrt[3]{abc} = 3\sqrt[3]{X^6Y^6} = 3X^2Y^2,$$

and thus $m(X, Y) = a + b + c - 3X^2Y^2 \geq 0$.

b) Suppose that the Motzkin polynomial can be written as $m = f_1^2 + \dots + f_k^2$ for some $k \in \mathbb{N}$ and $f_i(X, Y) \in \mathbb{R}[X, Y]$. Then w.l.o.g. we can take $f_1(X, Y) \not\equiv 0$ and so by Lemma 2 of Lecture 16 we have

$$6 = \deg(m) = 2 \max\{\deg(f_i),\ i = 1, \dots, k\},$$

which implies $\max\{\deg(f_i),\ i = 1, \dots, k\} = 3$ and so $\deg(f_i) \leq 3$ for $i = 1, \dots, k$. A base of the vector space of all the polynomials of degree ≤ 3 is given by

$$\{1,\ X,\ Y,\ X^2,\ XY,\ Y^2,\ X^3,\ X^2Y,\ XY^2,\ Y^3\}.$$

If X, X^2, X^3 respectively, appears in some f_i, then X^2, X^4, X^6 respectively, would appear in $m(X, Y)$ with positive coefficient, which is not the case. So X, X^2, X^3 do not appear in any of the f_i's. With the same argument, we can conclude that Y, Y^2, Y^3 do not appear either in any of the f_i's.

c) Suppose by contradiction that $m = f_1^2 + \dots + f_k^2$ for some $k \in \mathbb{N}$ and $f_i(X, Y) \in \mathbb{R}[X, Y]$. Then, by the part b) of this exercise, we know that for any $i \in \{1, \dots, k\}$:

$$f_i(X, Y) = a_i + b_iXY + c_iX^2Y + d_iXY^2, \text{ for some } a_i, b_i, c_i, d_i \in \mathbb{R}.$$

Then for any $i \in \{1,\dots,k\}$ we have $f_i^2(X,Y) = b_i^2 X^2 Y^2 +$ other terms, which gives that

$$m(X,Y) = \sum_{i=1}^{k} f_i^2(X,Y) = \sum_{i=1}^{k} b_i^2 X^2 Y^2 + \text{ other terms.}$$

Identifying the terms with same degree, we obtain that $\sum_{i=1}^{k} b_i^2 = -3$ which is clearly false in $\mathbb{R}$. Contradiction.

In conclusion, the Motzkin polynomial $m(X,Y)$ is non-negative on $\mathbb{R}^2$ but is not a s.o.s. in $\mathbb{R}[X,Y]$.

5) Let $n \in \mathbb{N}$, $\underline{X} := (X_1,\dots,X_n)$ and $d \in \mathbb{N}_0$.

a) Let us first consider the case of an arbitrary monic monomial of degree $\leq d$, i.e. we consider $g_{\underline{i}}(\underline{X}) := \underline{X}^{\underline{i}} = X_1^{i_1}\cdots X_n^{i_n}$, for some multi-index $\underline{i} = (i_1,\dots,i_n) \in \mathbb{N}_0^n$ such that $i_1+\cdots+i_n \leq d$. Then we have that

$$\bar{g}_{\underline{i}}(X_0,X_1,\dots,X_n) := X_0^d g_{\underline{i}}\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right) = X_0^d \frac{X_1^{i_1}\cdots X_n^{i_n}}{X_0^{i_1+\cdots+i_n}} = X_0^{d-(i_1+\cdots+i_n)} X_1^{i_1}\cdots X_n^{i_n}$$

and so $\deg(\bar{g}_{\underline{i}}) = d-(i_1+\cdots+i_n)+i_1+\cdots+i_n = d$.
Let us consider now some non-zero polynomial $f \in \mathbb{R}[\underline{X}]$ with $\deg(f) \leq d$, i.e.

$$f(\underline{X}) := \sum_{\substack{\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}_0^n \\ i_1+\cdots+i_n\leq d}} a_{\underline{i}}\, \underline{X}^{\underline{i}} = \sum_{\substack{\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}_0^n \\ i_1+\cdots+i_n\leq d}} a_{\underline{i}}\, g_{\underline{i}}(\underline{X}) \quad \text{with } a_{\underline{i}} \in \mathbb{R}.$$

Then we have have that

$$\begin{aligned}
\bar{f}(X_0,X_1,\dots,X_n) := X_0^d f\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right) &= X_0^d \sum_{\substack{\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}_0^n \\ i_1+\cdots+i_n\leq d}} a_{\underline{i}}\, g_{\underline{i}}\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right) \\
&= \sum_{\substack{\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}_0^n \\ i_1+\cdots+i_n\leq d}} a_{\underline{i}}\, X_0^d\, g_{\underline{i}}\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right) \\
&= \sum_{\substack{\underline{i}=(i_1,\dots,i_n)\in\mathbb{N}_0^n \\ i_1+\cdots+i_n\leq d}} a_{\underline{i}}\, \bar{g}_{\underline{i}}(X_0,X_1,\dots,X_n).
\end{aligned}$$

Hence, since we have already proved that $\deg(\bar{g}_{\underline{i}}) = d$ for any $\underline{i} = (i_1,\dots,i_n) \in \mathbb{N}_0^n$ such that $i_1+\cdots+i_n \leq d$, the polynomial $\bar{f}(X_0,X_1,\dots,X_n)$ is homogenous and $\deg(\bar{f}) = d$

b) Let us consider the homogenization map

$$\begin{array}{rccc}
h: & V_{d,n} & \to & F_{d,n+1} \\
 & f(X_1,\dots,X_n) & \mapsto & h(f) := \overline{f}(X_0,X_1,\dots,X_n).
\end{array}$$

To show that the map h is an isomorphism between vector spaces we need to show that h is an invertible linear map, i.e. there exists h^{-1} and both h and h^{-1} are linear.

- h is linear, since for any $\alpha,\beta \in \mathbb{R}$ and for any $f,g \in V_{d,n}$ we get:

$$\begin{aligned}
h(\alpha f(\underline{X}) + \beta g(\underline{X})) &= X_0^d\left(\alpha f\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right) + \beta g\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right)\right) \\
&= \alpha\left(X_0^d f\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right)\right) + \beta\left(X_0^d g\left(\frac{X_1}{X_0},\dots,\frac{X_n}{X_0}\right)\right) \\
&= \alpha\bar{f}(X_0,X_1,\dots,X_n) + \beta\bar{g}(X_0,X_1,\dots,X_n) \\
&= \alpha h(f(\underline{X})) + \beta h(g(\underline{X})).
\end{aligned}$$

- The compositional inverse h^{-1} of h is given by:

$$\begin{array}{cccc} h^{-1}: & F_{d,n+1} & \to & V_{d,n} \\ & \overline{f}(X_0, X_1, \ldots, X_n) & \mapsto & h^{-1}(\overline{f}) := \overline{f}(1, X_1, \ldots, X_n). \end{array}$$

  which is clearly linear.

c) Let $d \in \mathbb{N}_0$ be even. First we want to show that $f \geq 0$ on $\mathbb{R}^n$ implies $\overline{f} \geq 0$ on $\mathbb{R}^{n+1}$. Let $(x_0, x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ then we need to distinguish two cases:

Case 1: $x_0 \neq 0$. Then, by definition, $\overline{f}(x_0, x_1, \ldots, x_n) = x_0^d f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right)$. By assumption, $f\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \geq 0$ and, since d is even, $x_0^d > 0$. Hence, $\overline{f}(x_0, x_1, \ldots, x_n) \geq 0$.

Case 2: $x_0 = 0$. Since any polynomial is a continuous map, we have that $\overline{f}(0, x_1, \ldots, x_n) = \lim_{\epsilon \to 0} \overline{f}(\epsilon, x_1, \ldots, x_n)$. But for any $\epsilon \in \mathbb{R}^\times$, we have just showed that $\overline{f}(\epsilon, x_1, \ldots, x_n) \geq 0$. Thus, $\overline{f}(0, x_1, \ldots, x_n) \geq 0$.

Let us show now that $\overline{f} \geq 0$ on $\mathbb{R}^{n+1}$ implies $f \geq 0$ on $\mathbb{R}^n$. This follows just by noting that for any $(x_1, \ldots, x_n) \in \mathbb{R}^n$, we have $f(x_1, \ldots, x_n) = \overline{f}(1, x_1, \ldots, x_n)$, which is non-negative by assumption.

d) Suppose that $f = \sum_{i=1}^{k} f_i^2$ for some $k \in \mathbb{N}$ and some non-zero f_i's in $\mathbb{R}[X_1, \ldots, X_n]$. We have that $\deg(f_i) \leq d/2$, since $deg(f) \leq d$. Then

$$\overline{f}(X_0, X_1, \ldots, X_n) = X_0^d f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right) = \sum_{i=1}^{k} \left[X_0^{d/2} f_i\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)\right]^2 = \sum_{i=1}^{k} \bar{f_i}(X_0, X_1, \ldots, X_n)^2$$

Note that by the part a) of this exercise we know that each $\bar{f_i} \in \mathbb{R}[X_0, X_1, \ldots, X_n]$ is homogeneous of degree $= d/2$.

Conversely, suppose that $\overline{f}(X_0, X_1, \ldots, X_n) = \sum_{i=1}^{k} s_i(X_0, \ldots, X_n)^2$ for some $k \in \mathbb{N}$ and some non-zero s_i's in $\mathbb{R}[X_0, X_1, \ldots, X_n]$. Then

$$f(X_1, \ldots, X_n) = \overline{f}(1, X_1, \ldots, X_n) = \sum_{i=1}^{k} s_i(1, X_1, \ldots, X_n)^2 = \sum_{i=1}^{k} f_i(X_1, \ldots, X_n)^2,$$

where $f_i(\underline{X}) := s_i(1, X_1, \ldots, X_n) \in \mathbb{R}[X_1, \ldots, X_n]$.

e) The polynomial $\overline{m}$ is the homogenization of the Motzkin polynomial m introduced in Exercise 4. There we proved that m is PSD but not sum of squares in $\mathbb{R}[X, Y]$. Then by the parts c) and d) of this exercise we have also that the form $\overline{m}$ is PSD but not sum of squares in $\mathbb{R}[X, Y, Z]$.

References

[1] S. Lang. *Complex Analysis*. Springer-Verlag, New York, fourth edition, 1999.

[2] W. Rudin. *Real and Complex Analysis*. McGraw-Hill, New York, second edition, 1974.

f