Solutions to Sheet 4

Exercise 1

Let $M = X^2Y^2(X^2 + Y^2 - 3) + 1 \in \mathbb{R}[X, Y]$. We saw in class, that every non-negative polynomial is a sum of squares of rational functions (Hilbert's 17th problem). In this exercise, we will see that M is a non-negative polynomial that is not a sum of squares of polynomials.

(a) Show that $M(x, y) \geq 0$ for all $(x, y) \in \mathbb{R}^2$.

Hint: Use the arithmetic-geometric mean inequality on three variables.

Solution:
The arithmetic-geometric mean inequality for three variables states that

$$\sqrt[3]{abc} \leq \frac{a+b+c}{3}$$

and gives

$$X^4Y^2 + X^2Y^4 + 1 \geq 3\sqrt[3]{X^6Y^6} = 3X^2Y^2,$$

what we have to prove.

(b) Show that if $m \geq 1$ and $(f_1, \dots, f_m)$ are non-zero elements of $\mathbb{R}[X, Y]$, then

$$\deg(f_1^2 + \cdots + f_m^2) = 2\max(\deg(f_i)).$$

Solution:
Since $\deg(f^2) = 2\deg(f)$, it is clear that $\deg(f_1^2 + \cdots + f_m^2) \leq \max(\deg(f_i^2)) = 2\max(\deg(f_i))$. On the other hand we can be sure that no cancellation happens in the sum $f_1^2 + \cdots + f_m^2$, since the maximal degree terms all have positive coefficients (since the f_i are squared). Thus equality holds.

(c) Show that there is no finite family $(p_i)_{i \in I}$ in $\mathbb{R}[X, Y]$ such that $M = \sum p_i^2$.

Hint: Assume that there is such a family; show first that $\deg(p_i) \leq 3$*, then evaluate with* $X = 0$ *and* $Y = 0$ *to see that each* p_i *would have to be of the form* $a + bXY$ *for some* $a \in \mathbb{R}$ *and some* $b \in \mathbb{R}[X, Y]$ *with degree at most* 1*; compute then the coefficient of* $(XY)^2$.

Solution:
Let us assume that $M(X, Y) = \sum_i p_i(X, Y)^2$. Since $\deg(M) = 6$, by (b),

$$6 = \deg(M) = 2\max(\deg(p_i)),$$

we may conclude that $\deg(p_i) \leq 3$ for all i. Let p_i be given by

$$p_i(X,Y) = \sum_{k+\ell \leq 3} a^i_{k\ell} X^k Y^\ell$$

and note that when we plug in $X = 0$, we get

$$M(0,Y) = 1 = \sum_i p_i(0,Y)^2 = \sum_i \left(a^i_{00} + a^i_{01}Y + a^i_{02}Y^2 + a_{03}Y^3\right)^2,$$

hence $a^i_{0\ell} = 0$ for all $\ell \geq 1$. Similarly, we can plug in $Y = 0$ to get $a^i_{k0} = 0$ for $k \geq 1$. Thus the p_i have to be of the form

$$p_i(X,Y) = a^i_{00} + a^i_{11}XY + a^i_{21}X^2Y + a^i_{12}XY^2$$

and by multiplying out, we notice that the coefficient in front of X^2Y^2 in p_i^2 is $(a^i_{11})^2$. Hence

$$-3X^2Y^2 = \sum_i (a^i_{11})^2,$$

but the lefthandside is positive. This is a contradiction and thus M cannot be written as a sum of squares of polynomials.

Exercise 2

Let $\mathcal{L}$ be a language with a binary relation symbol $\leq$.

(a) Let M be an o-minimal $\mathcal{L}$-structure. Show that a non-empty subset $X \subset M$ with $X \neq M$ is definable if and only if the boundary $\partial X = \overline{X} \setminus \mathring{X}$ of X is finite and non-empty.

Solution:
If $X \subset M$ is definable, then the boundary is finite, by Lemma V.1(2) of the lecture. Since $X \neq M$, $\partial M \neq \emptyset$.

If the boundary is finite, let $-\infty = a_0 \leq a_1 \leq \ldots \leq a_n = \infty$ such that $\partial X = \{a_1, \ldots, a_{n-1}\}$. We can now define the following formula

$$\varphi(x) \quad = \quad \bigvee_{a_j \in X} x = a_j \vee \bigvee_{]a_j, a_j+1[\subseteq X} a_j < x \wedge x < a_{j+1}$$

and by the following Lemma we know that this is a valid description of X.

Lemma 0.1. For every $0 \leq j \leq n-1$, the open interval $]a_j, a_{j+1}[$ is contained in X, or disjoint from X.

Proof. Consider $]a_j, a_{j+1}[\subseteq M \setminus \partial X = \mathring{X} \cup (M \setminus \overline{X})$. Define the two open sets $A =]a_j, a_{j+1}[\cap \mathring{X}$, $B =]a_j, a_{j+1}[\cap (M \setminus \overline{X})$. Since $A \cup B =$

$]a_j, a_{j+1}[$ and $]a_j, a_{j+1}[$ is d-connected, we have $A = \emptyset$ or $B = \emptyset$. This shows the Lemma. □

(b) Let M be an $\mathcal{L}$-structure in which $\leq$ is interpreted as a total order which is dense without endpoints. Show that M is o-minimal if and only if every definable non-empty subset $X \subset M$ with $X \neq M$ has finite non-empty boundary $\partial X = \overline{X} \setminus \mathring{X}$, and for any $x < y$ in $\partial X \cup \{-\infty, +\infty\}$, if $]x, y[\cap \partial X$ is empty, then either $]x, y[\subset X$ or $]x, y[\cap X = \emptyset$.

Solution:
Assume first that M is o-minimal. By (a) X has finite non-empty boundary. Let $x < y$ for $x, y \in \partial X \cup \{-\infty, \infty\}$, such that $]x, y[\cap \partial X = \emptyset$. Interpreting this in the language of the solution to (a), there is a j, such that $x = a_j$ and $y = a_{j+1}$. By the Lemma in the solution to (a), $]x, y[\subseteq X$ or $]x, y[\cap X = \emptyset$.

Now assume the second part. To show o-minimality, we already know that $(M, \leq)$ forms a dense linear order without endpoints and hence only have to show that definable subsets of M are finite unions of points and open intervals. So let X be a definable subset of M. If $X = \emptyset$ or $X = M$, then it is clearly a finite union of points and open intervals, so we may assume that X has finite non-empty boundary. Let $-\infty = a_0 \leq a_1 \leq \ldots \leq a_n = \infty$ as in (a). By the assumption, we know that $]a_j, a_{j+1}[$ is either fully contained in X or disjoint from X. Hence X is the following finite union of points and open intervals

$$X = \bigcup_{p \in \partial X \cap X} \{p\} \cup \bigcup_{]a_j, a_{j+1}[\subseteq X}]a_j, a_{j+1}[.$$

Exercise 3

Let $\mathcal{L}_0 = (\cdot, e, \leq)$ be the language of ordered groups. Let M be an o-minimal $\mathcal{L}_0$-structure which is a model of the theory of ordered groups. (Which means that the order has the property that $x \leq y$ implies $xz \leq yz$ and $zx \leq zy$ for all $z \in M$.)

(a) Let $H \subset M$ be a definable subgroup of $(M, \cdot)$. Show that H is an interval, i.e., if $e < h$ for some $h \in H$, then $[e, h] \subset H$.

Hint: By contradiction, show that if this is false, then there is an infinite "discrete" definable set.

Solution:
Assume for contradiction that $e, h \in H$, but $g \in M \setminus H$ with $e \leq g \leq h$.

Since $e \leq h, h \leq h^2$. Since $e \leq g, h \leq gh$. Since $g \leq h, gh \leq h^2$. Now $h^2 \in H$ and $gh \notin H$, since otherwise $ghh^{-1} \in H$. Similarly we get

$$e \leq g \leq h \leq gh \leq h^2 \leq gh^2 \leq h^3 \leq gh^3 \leq \dots$$

Since M is o-minimal and H is a definable subgroup of M, H has to be a finite union of points and open intervals, but by the above sequence, we see that there are infinitely many elements $gh^k \in M \setminus H$ between the $h^k \in H$, which is a contradiction.

(b) Show that the only definable subgroups of $(M, \cdot)$ are $\{e\}$ and M.

Solution:
Let $H \neq \{e\}$ be a definable subgroup. By (a), H is open (Every element $h \in H$ is contained in an open interval $(h^{-2}, h^2) \subseteq H$). We claim that $M \setminus H$ is open too:

Let $e \leq k \in M \setminus H$. Since $e \leq h, k \leq hk$ and since $h^{-1} \leq e, h^{-1}k \leq k$. Both hk and $h^{-1}k$ are not in H and hence $k \subset]h^{-1}k, hk[\subseteq M \setminus H$.

Since M is d-connected and $H \neq \emptyset$, $M \setminus H$ has to be empty, hence $H = M$.

(c) Deduce that $(M, \cdot)$ is abelian and divisible, i.e. that for any $y \in M$ and $n \geq 1$ integer, there exists $x \in M$ such that $x^n = y$.

Solution:
The definable subgroups $\mathrm{Cent}_M(\{a\}) = \{g \in M \colon aga^{-1} = g\}$ for $a \in M \setminus \{e\}$ clearly contain $a \in \mathrm{Cent}_M(\{a\})$, and by (b) $\mathrm{Cent}_M(\{a\}) = M$. Hence everything commutes with a and M is abelian.

For every $n \geq 2$ we consider the definable subgroup

$$\Gamma_n = \{y \colon \exists x \colon x^n = y\},$$

which is not $\{e\}$, since $g^n \in \Gamma_n$ for every $g \in M \setminus \{e\}$. By (b) $\Gamma_n = M$, and hence M is divisible.

Exercise 4

Let $\mathcal{L} = (+, -, \cdot, 0, 1, \leq)$ be the language of ordered rings. Let M be an o-minimal $\mathcal{L}$-structure which is a model of the theory of ordered rings (not necessarily commutative; this means that $0 < 1$ in M, that $(M, +)$ is an ordered abelian group, and that the order has the property that whenever $x \leq y$ and $z \geq 0$, also $xz \leq yz$). *Hint: Use exercise 3.*

(a) Show that for every $x \in M \setminus \{0\}$, there is an inverse element $y \in M$ with $x \cdot y = 1$.

Solution:
For $x \in M \setminus \{0\}$, we consider the definable subgroup $x \cdot M = \{t \in M : \exists y \in M : t = x \cdot y\} < (M, +)$. By exercise 3 (c), $x \cdot M = M$ and hence there is an inverse $y \in M$ with $x \cdot y = 1$.

(b) Show that the positive elements of M form an ordered group with the multiplication.

Solution:
Clearly, $(M \setminus \{0\}, \cdot)$ is a group. To see that $\mathrm{Pos}(M) = \{x \in M : x > 0\}$ is a group, we have to check that it is closed under multiplication and taking inverses. Indeed when $0 \leq y$ and $z \geq 0$, then $0 = 0 \cdot z \leq y \cdot z \in \mathrm{Pos}(M)$ by the axioms of ordered rings. Moreover, if $y \geq 0$, then also $y^{-1} \geq 0$, since otherwise $1 = zz^{-1} \leq 0$. The group $\mathrm{Pos}(M)$ is an ordered group, since M is an ordered ring.

(c) Show that M is an ordered field.

Solution:
The ring M is a field, since it has an inverse by (a) and the multiplication is commutative by Exercise 3 (c) applied to the subgroup of positive elements (and multiplying by (-1) the negative elements).

(d) Show that positive elements in M have a square root.

Solution:
This follows from Exercise 3(c) applied to the group of positive elements. A square root is the special case $n = 2$ of divisibility.

(e) Show that addition and multiplication are continuous on M^2 (with the order topology on M and the product of the order topology on M^2).

Solution:
The open intervals form a basis of open sets in the topology on M. Thus it suffices to show that the preimages of open intervals is open. Consider the open set $]u, v[\subseteq M$ for $u < v \in M$.

Given $(a, b) \in +^{-1}(]u, v[)$, we consider the open set

$$B =]a + \Delta_-, a + \Delta_+[\times]b + \Delta_-, b + \Delta_+[\subseteq M^2 \quad \text{for}$$
$$\Delta_- = \frac{u - a - b}{2} < 0 \quad \text{and} \quad \Delta_+ = \frac{v - a - b}{2} > 0.$$

Clearly $(a,b) \in B$. For all $(x,y) \in B$ we have

$$u = a + b + 2\Delta_- < x + y < a + b + 2\Delta_+ = v$$

and hence $+(B) \subseteq]u,v[$, i.e. $+^{-1}(]u,v[)$ is open.

For the multiplication, we first restrict ourselves to the case $u,v > 0$, we let $(a,b) \in (\cdot)^{-1}(]u,v[)$, and in the case $a,b > 0$ consider the open set

$$B =]a \cdot \Delta_-, a \cdot \Delta_+[\times]b \cdot \Delta_-, b \cdot \Delta_+[\subseteq M^2 \quad \text{for}$$
$$\Delta_- = \sqrt{u/(ab)} < 1 \quad \text{and} \quad \Delta_+ = \sqrt{v/(ab)} > 1.$$

Again $(a,b) \in B$ and for all $(x,y) \in B$ we have

$$u = ab\Delta_-^2 < x \cdot y < ab\Delta_+^2 = v$$

and hence $(\cdot)(B) \subseteq]u,v[$.

In the case $a,b < 0$, we have instead $(a,b) \in -B$ and $(\cdot)(-B) = (\cdot)(B) \subseteq]u,v[$. In both cases $(\cdot)^{-1}(]u,v[)$ is open.

When u,v are not both positive we can do similar constructions.

(f) Show that for $f \in M[X]$, the polynomial function associated to f from M to M is a definable continuous function.

Solution:
A polynomial is a conjunction of additions and multiplications, both of which are continuous according to (e).

(g) Show that M is a real-closed field. *Hint: Use the criterion that a field F is real closed if and only if (1) for every $a \in F$, either a or $-a$ is a square and (2) every polynomial in $F[X]$ of odd degree has a root in F.*

Solution:
(1) Let $a \in M$. By (d), $|a| = \max\{a, -a\}$ has a square root.

(2) Let $f = \sum_{i=0}^{d} a_i X^i \in M[X]$ be a polynomial of odd degree d. We may assume without loss of generality that f is monic (otherwise take $f/(a_d)$ instead of f). The goal is to find $x, y \in M$ such that $f(x) < 0 < f(y)$ and to then use the intermediate value theorem for for o-minimal structures.

We let $y = \max_i\{d|a_i|, 1\}$. If $d|a_i| < 1$, for every $i = 1, \dots, d-1$, then

$$\left|\sum_{i=0}^{d-1} a_i y^i\right| \leq \sum_{i=1}^{d-1} |a_i| \leq d \cdot \max\{|a_i|\} < 1 = y = y^d$$

so $f(y) = y^d + \sum a_i y^i > 0$. If however there is a j, such that $y = d|a_j|$, then we have

$$\left| \sum_{i=0}^{d-1} a_i y^i \right| \leq \sum_{i=0}^{d-1} |a_i| d^i |a_j|^d < \sum_{i=0}^{d-1} d^{d-1} |a_j|^d = d^d |a_j|^d = y^d.$$

Thus $f(y) = y^d + \sum a_i y^i > 0$. A similar calculation shows that $x := -y$ satisfies $f(x) \leq 0$.

We now use the intermediate value theorem for o-minimal structures to find a 0.