REAL ALGEBRAIC GEOMETRY LECTURE NOTES (21: 29/06/15 - CORRECTED ON 11/07/19)

SALMA KUHLMANN

Contents

Chapter IV: Real closed exponential fields

1. Real closed exponential fields

Definition 1.1. Let K be a real closed field and

$$\exp : (K, +, 0, <) \to (K^{>0}, \cdot, 1, <)$$

such that exp is an order preserving isomorphism of ordered groups, i.e.

(i) $x < y \Rightarrow \exp(x) < \exp(y)$,

(ii) $\exp(x + y) = \exp(x) \exp(y)$.

Then $(K, +, 0, 1, <, \exp)$ is called a **real closed exponential field**.

Question: Is the theory $T_{\exp} = \mathrm{Th}(\mathbb{R}, +, \cdot, 0, 1, <, \exp)$ decidable?

- Osgood proved that $T_{\exp}$ does not admit quantifier-elimination.
- $\sim$ 1991 A. Wilkie showed that $T_{\exp}$ is o-minimal.
- In 1994 A. Wilkie and A. Macintyre showed that $T_{\exp}$ is decidable if Schanuel's conjecture is true. In fact they showed that $T_{\exp}$ is decidable, if and only if "a weak form of Schanuel's conjecture" is true.

2. Additive lexicographic decomposition

Remark 2.1. Let A, B be ordered abelian groups. The **lexicographic product** $A \sqcup B$ is the ordered abelian group defined as follows:
As a group it is just the direct sum $A \oplus B$. The total order is the lexicographic order on $A \oplus B$, i.e. for $a_i \in A$ and $b_i \in B$

$$a_1 + b_1 < a_2 + b_2 :\Leftrightarrow \text{either } a_1 < a_2 \text{ or } a_1 = a_2 \text{ and } b_1 < b_2.$$

Recall 2.2. A **complement** U of a subspace W of V is just a subspace such that $V = U \oplus W$. Moreover, U is unique up to isomorphism.

Theorem 2.3. *Let $(K, +, \cdot, 0, 1, <)$ be an ordered non-Archimedean field with value group G and residue field $\overline{K}$. Consider the ordered divisible abelian group $(K, +, 0, <)$.*

- *There exists a complement $\mathbb{A}$ of K_v in $(K, +, 0, <)$ and a complement $\mathbb{A}'$ of I_v in K_v such that $(K, +, 0, <) = \mathbb{A} \sqcup \mathbb{A}' \sqcup I_v$.*
- *Both $\mathbb{A}$ and $\mathbb{A}'$ are unique (up to isomorphism of ordered groups). Moreover, $\mathbb{A}'$ is isomorphic to $(\overline{K}, +, 0, <)$.*
- *Furthermore the value set of $\mathbb{A}$ is $G^{<0}$ and the value set of I_v is $G^{>0}$. The Archimedean components of $\mathbb{A}$ and I_v are all isomorphic to $(\overline{K}, +, 0, <)$.*

The proof of this theorem will be in the assignment. Consider

$$v : (K, +, 0, <) \to G.$$

Note that $v(I_v) = G^{>0}$, so $v(\mathbb{A}) = G^{<0}$.

Hilfslemma 2.4.

(*i*) Let M be an ordered $\mathbb{Q}$-vector space and C a convex subspace of M such that $M = C' \oplus C$, where C' is the vector space complement of C in M. Then $M = C' \sqcup C$.

(*ii*) Let $\eta : M \to N$ be a surjective homomorphism of ordered vector spaces. Then $\ker \eta$ is a convex subspace of M and $M \cong N \sqcup \ker \eta$.

(*iii*) Let M, N be ordered vector spaces with convex subspaces C and D, respectively. Assume that $\eta : M \to N$ is an isomorphism of ordered vector spaces such that $\eta(C) = D$. Then

$$\overline{\eta} : M/C \mapsto N/D, a + C \mapsto \eta(a) + D$$

is a well-defined isomorphism of ordered vector spaces.

Remark 2.5. Consider the divisible ordered abelian group $(K, +, 0, <)$ and $x = 1 \in K$. Compute $C_1 = (K_v, +, 0, <)$ and $D_1 = (I_v, +, 0, <)$. For the Archimedean component we have

$$B_1 \cong C_1/D_1 \cong (\overline{K}, +, 0, <).$$

We generalize this observation to the following:

Proposition 2.6. *All the Archimedean components of the divisible ordered abelian group* $(K, +, 0, <)$ *are isomorphic to the divisible ordered abelian group* $(\overline{K}, +, 0, <)$.

Proof. Let $a \in K, a > 0$. The map

$$\eta : C_a \mapsto (\overline{K}, +, 0, <),\ x \mapsto \overline{xa^{-1}}$$

(Recall: $G = \{x : v(x) \geqslant v(a)\}$) is a surjective homomorphism of ordered groups with kernel $D_a = \{x : v(x) > v(a)\} \subset C_a$. □

3. Multiplicative lexicographic decomposition

Theorem 3.1. *Let* $(K, +, \cdot, 0, 1, <)$ *be a totally ordered non-Archimedean field with natural valuation* v, $G = v(K^*)$ *and residue field* $\overline{K}$. *Assume that* K *is root closed for positive elements, i.e.* $(K^{>0}, \cdot, 1, <)$ *is a divisible ordered group.*

- *There exists a group complement* $\mathbb{B}$ *of* $U_v^{>0}$ *in* $(K^{>0}, \cdot, 1, <)$ *and a group complement* $\mathbb{B}'$ *of* $1 + I_v$ *in* $(U_v^{>0}, \cdot, 1, <)$ *such that*
$$(K^{>0}, \cdot, 1, <) = \mathbb{B} \sqcup \mathbb{B}' \sqcup (1 + I_v, \cdot, 1, <).$$
- *Every group complement* $\mathbb{B}$ *is isomorphic to* G.
- *Every group complement* $\mathbb{B}'$ *is isomorphic to* $(\overline{K}^{>0}, \cdot, 1, <)$.

The proof follows from the following two lemmas and the Hilfslemma.

Lemma 3.2. *The map*

$$(K^{>0}, \cdot, 1, <) \to G,\ a \mapsto -v(a) = v(a^{-1})$$

is a surjective homomorphism of ordered groups with kernel $U_v^{>0}$. *Thus,* $U_v^{>0}$ *is a convex subgroup of* $(K^{>0}, \cdot, 1, <)$ *and*

$$(K^{>0}, \cdot, 1, <)/U_v^{>0} \cong G.$$

Therefore $(K^{>0}, \cdot, 1, <) \cong \mathbb{B} \sqcup U_v^{>0}$ with $\mathbb{B} \cong G$.

Lemma 3.3. *The map*

$$(U_v^{>0}, \cdot, 1, <) \to (\overline{K}^{>0}, \cdot, 1, <),\ a \mapsto \overline{a},$$

is a surjective homomorphism of ordered groups with kernel $1 + I_v$. *Thus*

$$(U_v^{>0}, \cdot, 1, <)/(1 + I_v, \cdot, 1, <) \cong (\overline{K}^{>0}, \cdot, 1, <).$$

Therefore $U_v^{>0} \cong \mathbb{B}' \sqcup 1 + I_v$, where $\mathbb{B}' \cong (\overline{K}^{>0}, \cdot, 1, <)$.