Table of Contents: Real Algebraic Geometry II

Prof. Dr. Salma Kuhlmann, Katharina Dupont, Gabriel Lehéricy

SS 2015

REAL ALGEBRAIC GEOMETRY II LECTURE NOTES (01: 13/04/15 - CORRECTED ON 02/05/2019)

SALMA KUHLMANN

Contents

Chapter I: Valued vector spaces

1. Valued modules

All modules M considered are left Z-modules for a fixed ring Z with 1 (we are mainly interested in $Z = \mathbb{Z}$, i.e. in valued abelian groups).

Definition 1.1. Let Γ be a totally ordered set and ∞ an element greater than each element of Γ (Notation: $\infty > \Gamma$). A surjective map

$$v \colon M \longrightarrow \Gamma \cup \{\infty\}$$

is a **valuation** on M (and (M, v) is a **valued module**) if $\forall\, x, y \in M$ and $\forall\, r \in Z$:

(*i*) $v(x) = \infty \;\Leftrightarrow\; x = 0$,

(*ii*) $v(rx) = v(x)$, if $r \neq 0$ (value preserving scalar multiplication),

(*iii*) $v(x - y) \geqslant \min\{v(x), v(y)\}$ (ultrametric Δ-inequality).

Remark 1.2. $(i) + (ii) \;\Rightarrow\; M$ is torsion-free.

Remark 1.3. Consequences of the ultrametric Δ-inequality:

(*i*) $v(x) \neq v(y) \;\Rightarrow\; v(x + y) = \min\{v(x), v(y)\}$,

(*ii*) $v(x + y) > v(x) \;\Rightarrow\; v(x) = v(y)$.

Definition 1.4. $v(M) := \Gamma = \{v(x) : 0 \neq x \in M\}$ is called the **value set** of M.

Definition 1.5.

(i) Let (M_1, v_1), (M_2, v_2) be valued Z-modules with value sets Γ_1 and Γ_2 respectively. Let
$$h\colon M_1 \longrightarrow M_2$$
be an isomorphism of Z-modules. We say that h **preserves the valuation** if there is an isomorphism of ordered sets
$$\varphi\colon \Gamma_1 \longrightarrow \Gamma_2$$
such that $\forall\, x \in M_1 :\ \varphi(v_1(x)) = v_2(h(x))$.

(ii) Two valuations v_1 and v_2 on M are **equivalent** if the identity map on M preserves the valuation.

Definition 1.6.

(1) An **ordered system of Z-modules** is a pair
$$[\,\Gamma,\ \{B(\gamma) : \gamma \in \Gamma\}\,],$$
where $\{B(\gamma) : \gamma \in \Gamma\}$ is a family of Z-modules indexed by a totally ordered set Γ.

(2) Two ordered systems
$$S_i = [\,\Gamma_i,\ \{B_i(\gamma) : \gamma \in \Gamma_i\}\,] \qquad i = 1, 2$$
are **isomorphic** (we write $S_1 \cong S_2$) if and only if there is an isomorphism
$$\varphi\colon \Gamma_1 \longrightarrow \Gamma_2$$
of totally ordered sets, and $\forall\, \gamma \in \Gamma_1$ an isomorphism of Z-modules
$$\varphi_\gamma\colon B_1(\gamma) \longrightarrow B_2(\varphi(\gamma)).$$

(3) Let (M, v) be a valued Z-module, $\Gamma := v(M)$. For $\gamma \in \Gamma$ set
$$M^\gamma := \{x \in M : v(x) \geqslant \gamma\}$$
$$M_\gamma := \{x \in M : v(x) > \gamma\}.$$
Then $M_\gamma \subsetneq M^\gamma \subsetneq M$. Set
$$B(M, \gamma) := M^\gamma / M_\gamma.$$
$B(M, \gamma)$ is called **the (homogeneous) component corresponding to γ**. **The skeleton** (*das Skelett*) of the valued module (M, v) is the ordered system
$$S(M) := [\,v(M),\ \{B(M, \gamma) : \gamma \in v(M)\}\,].$$
We write $B(\gamma)$ for $B(M, \gamma)$ if the context is clear.

(4) For every $\gamma \in \Gamma$, the **coefficient map** (*Koeffizient Abbildung*)

$$\begin{aligned} \pi^M(\gamma,-)\colon M^\gamma &\longrightarrow B(\gamma) \\ x &\mapsto x + M_\gamma \end{aligned}$$

is the canonical projection.

We write $\pi(\gamma,-)$ instead of $\pi^M(\gamma,-)$ if the context is clear.

Lemma 1.7. *The skeleton is an isomorphism invariant, i.e.*

$$\begin{aligned} \textit{if} \quad (M_1,v_1) &\cong (M_2,v_2), \\ \textit{then} \quad S(M_1) &\cong S(M_2). \end{aligned}$$

Proof. Let $h\colon M_1 \to M_2$ be an isomorphism which preserves the valuation. Then

$$\tilde{h}\colon v_1(M_1) \longrightarrow v_2(M_2)$$

defined by

$$\tilde{h}(v_1(x)) := v_2(h(x))$$

is a well-defined map and an isomorphism of totally ordered sets.
For each $\gamma \in v_1(M_1)$, the map

$$h_\gamma\colon B_1(\gamma) \longrightarrow B_2(\tilde{h}(\gamma))$$

defined by

$$\pi^{M_1}(\gamma,x) \mapsto \pi^{M_2}(\tilde{h}(\gamma),h(x))$$

is well-defined and an isomorphism of modules. $\square$

2. Hahn valued modules

A system $[\Gamma,\ \{B(\gamma) : \gamma \in \Gamma\}]$ of torsion-free modules can be realized as the skeleton of a valued module through the following canonical construction:

Consider $\prod_{\gamma\in\Gamma} B(\gamma)$ the product module. For $s \in \prod_{\gamma\in\Gamma} B(\gamma)$ define

$$\operatorname{support}(s) = \{\gamma \in \Gamma : s(\gamma) \neq 0\}.$$

REAL ALGEBRAIC GEOMETRY II LECTURE NOTES (02: 16/04/15 - CORRECTED ON 02/05/2019)

SALMA KUHLMANN

Contents

1. Hahn valued modules

The **Hahn sum** is the Z-submodule of $\prod_{\gamma\in\Gamma} B(\gamma)$ consisting of all elements with finite support. We denote it by

$$\bigsqcup_{\gamma\in\Gamma} B(\gamma) := \left\{ s \in \prod_{\gamma\in\Gamma} B(\gamma) : |\mathrm{supp}(s)| < \infty \right\}$$

We endow $\bigsqcup_{\gamma\in\Gamma} B(\gamma)$ with the valuation

$$\begin{aligned} v_{\min}\colon \bigsqcup_{\gamma\in\Gamma} B(\gamma) &\longrightarrow \Gamma\cup\{\infty\} \\ v_{\min}(s) &= \min \mathrm{support}(s). \end{aligned}$$

(convention: $\min\emptyset = \infty$).

The **Hahn product** is the Z-submodule of $\prod_{\gamma\in\Gamma} B(\gamma)$ consisting of all elements with well-ordered support in Γ. We denote it by

$$\mathrm{H}_{\gamma\in\Gamma} B(\gamma) := \left\{ s \in \prod_{\gamma\in\Gamma} B(\gamma) : \mathrm{supp}(s) \text{ is a well-ordered subset of } \Gamma \right\}$$

We endow $\mathrm{H}_{\gamma\in\Gamma} B(\gamma)$ with the valuation $v_{\min}$ as well.

2. Well-ordered sets

We recall that a totally ordered set Γ is **well-ordered** if every non-empty subset of Γ has a least element, or equivalently if every strictly descending sequence of elements from Γ is finite.

Example 2.1.

(1) $Z = \mathbb{Z}$, assume $\Gamma = \{1, \ldots, n\},\ B(\gamma) = \mathbb{Z}$. Then

$$\coprod_{\gamma=1,\ldots,n} B(\gamma) = \mathrm{H}_{\gamma=1,\ldots,n}\, B(\gamma)$$

(2) $Z = \mathbb{Q}$, assume $\Gamma = \mathbb{N}$ (with natural order).
order type $\mathbb{N}$ = the first infinite ordinal number ω.

Let $B(\gamma) := \begin{cases} \mathbb{Q} & \text{if } \gamma \text{ is odd} \\ \mathbb{R} & \text{if } \gamma \text{ is even} \end{cases}$
Then

$$\mathrm{H}_{\gamma\in\mathbb{N}}\, B(\gamma) = \prod_{\gamma\in\mathbb{N}} B(\gamma).$$

More generally this holds whenever Γ is a well-ordered set, i.e. whenever Γ is an ordinal.

(3) $\Gamma = -\mathbb{N}$ with natural order.

$$\coprod_{\gamma\in-\mathbb{N}} B(\gamma) = \mathrm{H}_{\gamma\in-\mathbb{N}}\, B(\gamma)$$

More generally this holds whenever Γ is an anti well-ordered set, i.e. well-ordered under the order relation

$$\gamma_1 \leqslant^* \gamma_2 \Leftrightarrow \gamma_2 \leqslant \gamma_1.$$

(4) $\Gamma = \mathbb{Q}$. Then

$$\coprod_{\gamma\in\mathbb{Q}} B(\gamma) \subsetneq \mathrm{H}_{\gamma\in\mathbb{Q}}\, B(\gamma) \subsetneq \prod_{\gamma\in\mathbb{Q}} B(\gamma).$$

Note that every countable ordinal is the order type of a well-ordered subset of $\mathbb{Q}$.

Theorem 2.2. *(Cantor)*
Every countable dense linear order without endpoints is isomorphic to $\mathbb{Q}$.

Definition 2.3.

(i) A linear order Q is **dense** if

$$\forall q_1 < q_2 \in Q\ \exists q_3 \in Q \text{ such that } q_1 < q_3 < q_2.$$

(ii) A linear order has **no endpoints** if it has no least element and no last element.

Example 2.4.

(i) $\mathbb{Q}$ is dense because for $q_1 < q_2$ define $q_3 := \frac{q_1+q_2}{2}$.
$\mathbb{R}$ is dense.

(ii) $\mathbb{Q}$ and $\mathbb{R}$ have no endpoints.

Example 2.5.

(5) $\coprod_{\gamma\in\mathbb{Q}^{<0}} B(\gamma) \subsetneq \mathrm{H}_{\gamma\in\mathbb{Q}^{<0}} B(\gamma)$

$q \mapsto -q \quad q \mapsto \frac{1}{-q}(q \neq 0) \quad 0 \mapsto 0$. Note that $\mathbb{Q}^{<0} := \{q \in \mathbb{Q} : q < 0\}$ has no endpoints.

$$\coprod_{\gamma\in\mathbb{Q}^{<0}} B(\gamma) \cong \coprod_{\gamma\in\mathbb{Q}} B(\gamma) \cong \coprod_{\gamma\in\mathbb{Q}^{>0}} B(\gamma).$$

More generally let us now take $\Gamma = (q_1, q_2)$, the open intervall in $\mathbb{Q}$ determined by $q_1 < q_2$. Note that $(q_1, q_2) \cong \mathbb{Q}$.

(6) $\Gamma = \mathbb{R}$. Then

$$\coprod_{\gamma\in\mathbb{R}} B(\gamma) \subsetneq \mathrm{H}_{\gamma\in\mathbb{R}} B(\gamma) \subsetneq \prod_{\gamma\in\mathbb{R}} B(\gamma).$$

What are the well-ordered subsets of $\mathbb{R}$?

(i) all well-ordered subsets of $\mathbb{Q}$!

(ii) all countable ordinals are the order type of some well-ordered subset of $\mathbb{R}$.

Now: Are there more?

Discussion: What is the cardinality of $\mathbb{R}$?

$$|\mathbb{R}| = \left|\{0,1\}^{\mathbb{N}}\right| = |\{0,1\}|^{\mathbb{N}} = 2^{\aleph_0} = c := \text{ the continuum}$$

Therefore

$$c = |\mathfrak{P}(\mathbb{N})| > |\mathbb{N}| = \aleph_0.$$

More precisely: are there uncountable well-ordered subsets of $\mathbb{R}$?

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (03: 20/04/15 - CORRECTED ON 02/05/2019)

SALMA KUHLMANN

Contents

1. Hahn Sandwich Proposition

Lemma 1.1.

(i) $\coprod_{\gamma\in\Gamma} B(\gamma) \subseteq \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$.

(ii)

$$\begin{aligned} S(\coprod_{\gamma\in\Gamma} B(\gamma)) &\cong [\,\Gamma, \{B(\gamma) : \gamma\in\Gamma\}\,] \\ &\cong S(\mathrm{H}_{\gamma\in\Gamma} B(\gamma)). \end{aligned}$$

We shall show that if $Z = Q$ is a field and (V, v) is a valued Q-vector space with skeleton $S(V) = [\,\Gamma, \{B(\gamma) : \gamma \in \Gamma\,]$, then

$$\left(\coprod_{\gamma\in\Gamma} B(\gamma), v_{\min}\right) \hookrightarrow (V, v) \hookrightarrow (\mathrm{H}_{\gamma\in\Gamma} B(\gamma), v_{\min}).$$

2. Immediate extensions

Definition 2.1. Let (V_i, v_i) be valued Q-vector spaces ($i = 1, 2$).

(1) Let $V_1 \subseteq V_2$ be a Q-subspace with $v_1(V_1) \subseteq v_2(V_2)$. We say that (V_2, v_2) is an **extension** of (V_1, v_1), and we write

$$(V_1, v_1) \subseteq (V_2, v_2),$$

if $v_{2|_{V_1}} = v_1$.

(2) If $(V_1, v_1) \subseteq (V_2, v_2)$ and $\gamma \in v_1(V_1)$, the map

$$\begin{array}{rcl} B_1(\gamma) & \longrightarrow & B_2(\gamma) \\ x + (V_1)_\gamma & \mapsto & x + (V_2)_\gamma \end{array}$$

is a natural identification of $B_1(\gamma)$ as a Q-subspace of $B_2(\gamma)$. The extension $(V_1, v_1) \subseteq (V_2, v_2)$ is **immediate** if $\Gamma := v_1(V_1) = v_2(V_2)$ and $\forall\, \gamma \in v_1(V_1)$

$$B_1(\gamma) = B_2(\gamma).$$

Equivalently, $(V_1, v_1) \subseteq (V_2, v_2)$ is immediate if $S(V_1) = S(V_2)$.

Lemma 2.2. *(Characterization of immediate extensions)*
The extension $(V_1, v_1) \subseteq (V_2, v_2)$ is immediate if and only if

$$\forall\, x \in V_2,\ x \neq 0,\ \exists\, y \in V_1 \ \ \textit{such that} \ \ v_2(x-y) > v_2(x).$$

Proof. We show that in a valued Q-vector space (V, v), for every $x, y \in V$

$$v(x-y) > v(x) \iff \begin{cases} (i) & \gamma = v(x) = v(y) \ \text{ and} \\ (ii) & \pi(\gamma, x) = \pi(\gamma, y). \end{cases}$$

($\Leftarrow$) Suppose (i) and (ii). So $x, y \in V^\gamma$ and $x - y \in V_\gamma$.
Then $v(x-y) > \gamma = v(x)$.

($\Rightarrow$) Suppose $v(x-y) > v(x)$. We show (i) and (ii).
Assume for a contradiction that $v(x) \neq v(y)$. Then $v(x-y) = \min\{v(x), v(y)\}$. So if $v(x) > v(y)$, then $v(y) = v(x-y) > v(x)$ and if $v(y) > v(x)$, then $v(x) = v(x-y) > v(x)$. Both is obviously a contradiction. Thus, $v(x) = v(y)$. (ii) is analogue.

□

Example 2.3. $(\coprod_{\gamma\in\Gamma} B(\gamma),\ v_{\min}) \ \subseteq \ (\mathrm{H}_{\gamma\in\Gamma} B(\gamma),\ v_{\min})$
is an immediate extension.

Proof. Given $x \in \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$, $x \neq 0$, set

$$\gamma_0 := \min \operatorname{support}(x) \qquad \text{and} \qquad x(\gamma_0) := b_0 \in B(\gamma_0).$$

Let $y \in \coprod_{\gamma\in\Gamma} B(\gamma)$ such that

$$y(\gamma) = \begin{cases} 0 & \text{if } \gamma \neq \gamma_0 \\ b_0 & \text{if } \gamma = \gamma_0. \end{cases}$$

Namely $y = b_0 \chi_{\gamma_0}$, where

$$\chi_{\gamma_0} \colon \Gamma \longrightarrow Q$$

$$\chi_{\gamma_0}(\gamma) = \begin{cases} 1 & \text{if } \gamma = \gamma_0 \\ 0 & \text{if } \gamma \neq \gamma_0. \end{cases}$$

Then $v_{\min}(x-y) > \gamma_0 = v_{\min}(x)$ (because $(x-y)(\gamma_0) = x(\gamma_0) - y(\gamma_0) = b_0 - b_0 = 0$).

□

3. Valuation independence

Definition 3.1. $\mathcal{B} = \{x_i : i \in I\} \subseteq V \setminus \{0\}$ is **Q-valuation independent** if for $q_i \in Q$ with $q_i = 0$ for all but finitely many $i \in I$, we have

$$v\left(\sum_{i \in I} q_i x_i\right) = \min_{i \in I, q_i \neq 0} \{v(x_i)\}.$$

Remark 3.2.

(1) Q-linear independence $\not\Rightarrow$ Q-valuation independence.
Consider $(\coprod_2 \mathbb{Q}, v_{\min})$ and the elements $x_1 = (1,1),\ x_2 = (1,0)$.

(2) $\mathcal{B} \subseteq V \backslash \{0\}$ is Q-valuation independent $\Rightarrow$ $\mathcal{B}$ is Q-linear independent.
Else $\exists\ q_i \neq 0$ with $\sum q_i x_i = 0$ and $\min\{v(x_i)\} = v(\sum q_i x_i) = \infty$, a contradiction.

Proposition 3.3. *(Characterization of valuation independence)*
Let $\mathcal{B} \subseteq V \setminus \{0\}$. Then $\mathcal{B}$ is Q-valuation independent if and only if $\forall\, n \in \mathbb{N}$ and $\forall\, b_1, \ldots, b_n \in \mathcal{B}$ pairwise distinct with $v(b_1) = \cdots = v(b_n) = \gamma$, the coefficients

$$\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n) \in B(\gamma)$$

are Q-linear independent in the Q-vector space $B(\gamma)$.

Proof.

($\Rightarrow$) Let $b_1, \ldots, b_n \in \mathcal{B}$ with $v(b_1) = \cdots = v(b_n) = \gamma$ and suppose for a contradiction that

$$\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n) \in B(\gamma)$$

are not Q-linear independent. So there are $q_1, \ldots, q_n \in Q$ non-zero such that $\pi(\gamma, \sum q_i b_i) = 0$, so $v(\sum q_i b_i) > \gamma$. This contradicts the valuation independence.

($\Leftarrow$) We show that

$$v\left(\sum q_i b_i\right) = \min\{v(b_i)\} = \gamma.$$

Since $\pi(\gamma, b_1), \ldots, \pi(\gamma, b_n)$ are Q-linear independent in $B(\gamma)$,

$$\pi\left(\gamma, \sum q_i b_i\right) \neq 0,$$

i.e. $v(\sum q_i b_i) \leqslant \gamma$.
On the other hand $v(\sum q_i b_i) \geqslant \gamma$, so $v(\sum q_i b_i) = \gamma = \min\{v(b_i)\}$.

□

4. Maximal valuation independence

By Zorn's lemma, maximal valuation independent sets exist:

Corollary 4.1. *(Characterization of maximal valuation independent sets)* $\mathcal{B} \subseteq V \setminus \{0\}$ *is maximal valuation independent if and only if* $\forall\, \gamma \in v(V)$

$$\mathcal{B}_\gamma := \{\pi(\gamma, b) : b \in \mathcal{B}, v(b) = \gamma\}$$

is a Q*-vector space basis of* $B(\gamma)$.

Corollary 4.2. *Let* $\mathcal{B} \subseteq V \setminus \{0\}$ *be valuation independent in* (V, v). *Then* $\mathcal{B}$ *is maximal valuation independent if and only if the extension*

$$\langle\, \mathcal{B}\, \rangle := (V_0, v_{|V_0}) \ \subseteq\ (V, v)$$

is an immediate extension.

Proof.

($\Rightarrow$) Assume $\mathcal{B} \subseteq V$ is maximal valuation independent. We show $V_0 \subseteq V$ is immediate.

If not $\exists\ x \in V$, $x \neq 0$, such that

$$\forall\, y \in V_0 : \ v(x - y) \leqslant v(x).$$

We will show that in this case $\mathcal{B} \cup \{x\}$ is valuation independent (which will contradict our maximality assumption). Consider $v(y_0 + qx)$, $q \in Q$, $q \neq 0$, $y_0 \in V_0$. Set $y := -y_0/q$. We claim that

$$v(y_0 + qx) = v(x - y) = \min\{v(x), v(y)\} = \min\{v(x), v(y_0)\}.$$

This follows immediately from

Fact: $v(x - y) \leqslant v(x) \iff v(x - y) = \min\{v(x), v(y)\}$.

Proof of the fact. The implication ($\Leftarrow$) is trivial. To see ($\Rightarrow$), assume that $v(x - y) > \min\{v(x), v(y)\}$.

If $\min\{v(x), v(y)\} = v(x)$, then we have the contradiction

$$v(x) \geqslant v(x - y) > \min\{v(x), v(y)\} = v(x).$$

If $\min\{v(x), v(y)\} = v(y) < v(x)$, then $v(y) = v(x - y) > v(y)$, again a contradiction.

($\Leftarrow$) Now assume that $(V_0, v_{|V_0}) \subseteq (V, v)$ is immediate. We show that $\mathcal{B}$ is maximal valuation independent.

If not, $\mathcal{B} \cup \{x\}$ is valuation independent for some $x \in V \setminus \{0\}$ with $x \notin \mathcal{B}$. So $\forall y \in V_0$ we get $v(x - y) \leqslant v(x)$ by the fact above. This contradicts that $(V_0, v_{|V_0}) \subseteq (V, v)$ is immediate.

$\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (04: 20/04/15 - CORRECTED ON 02/05/2019)

SALMA KUHLMANN

Contents

Additional lecture on Ordinals

1. Preliminaries

Theorem 1.1. *(transfinite induction)*
If $(A, <)$ is a well-ordered set and $P(x)$ a property such that

$$\forall a \in A(\forall b < a \ P(b) \Rightarrow P(a)),$$

then $P(a)$ holds for all $a \in A$.

Proof. Consider the set

$$B := \{b \in A : P(b) \text{ is false}\}.$$

If $B \neq \emptyset$, let $b = \min B$. Then $\forall c < b \ P(c)$ is true but $P(b)$ is false, a contradiction. □

Definition 1.2. Let A be a well-ordered set. An **initial segment** of A is a set of the form $A_a := \{b \in A : b \leqslant a\}$.

Proposition 1.3. *No proper initial segment of a well-ordered set $(A, \leqslant)$ is $\cong A$.*

Proof. Assume $f : A \to A_a$ is an isomorphism of ordered sets. Prove by induction

$$\forall x \in A : f(x) \geqslant x.$$

Since $A_a \subsetneq A$ we find some $b \in A \backslash A_a$, i.e. $b > a$. Therefore

$$f(b) \geqslant b > a,$$

contradicting $f(b) \in A_a$. □

Definition 1.4. A set A is **transitive**, if $\forall a \in A \ \forall b \in a : b \in A$ (or equivalently $\forall a \in A : a \subseteq A$).

Lemma 1.5. *Let A be a transitive set. Then $\in$ is transitive on A if and only if a is transitive for all $a \in A$.*

Lemma 1.6. *A union of transitive sets is transitive.*

2. Ordinals

Definition 2.1. A set α is an **ordinal** if

(i) α is transitive,
(ii) $(\alpha, \in)$ is a well-ordered set.

Notation 2.2. $\mathrm{Ord} = \{\text{ordinals}\}$

Remark 2.3. *$\in$ is an order on $\alpha \Rightarrow \in$ is transitive, i.e. $\forall a \in \alpha : a$ is transitive.*

Proposition 2.4. *$\in$ is a strict order on* Ord.

Proof. If $\alpha \in \beta \in \gamma$, then $\alpha \in \gamma$ by transitivity of γ. Therefore $\in$ is transitive on Ord. Now let $\alpha \in \beta$. We claim $\beta \notin \alpha$. Otherwise $\alpha \in \beta \in \alpha$ and therefore $\alpha, \beta \in \alpha, \alpha \in \beta, \beta \in \alpha$, a contradiction. $\square$

We write $\alpha < \beta$ instead of $\alpha \in \beta$.

Example 2.5. Each $n \in \mathbb{N} = \{0, 1, \ldots\}$ is an ordinal

$$\begin{aligned} 0 &= \emptyset, \\ 1 &= \{0\}, \\ 2 &= \{0, 1\}, \\ 3 &= \{0, 1, 2\}, \\ &\vdots \\ n &= \{0, 1, \ldots, n-1\}. \end{aligned}$$

Moreover, $\mathbb{N} =: \omega$ is an ordinal.

Proposition 2.6. $\forall \alpha \in \mathrm{Ord} : \alpha = \{\beta \in \mathrm{Ord} : \beta < \alpha\}$.

Proof. Let $\beta \in \alpha$. Then β is transitive. Thus $\beta \subseteq \alpha$ and $(\beta, \in) = (\alpha, \in)_\beta$. $\square$

Lemma 2.7. *Let $\alpha, \beta \in \mathrm{Ord}$ such that $\alpha \subsetneq \beta$. Then $\min(\beta \backslash \alpha)$ exists and is $= \alpha$, so $\alpha \in \beta$.*

Proof. Since $\beta \backslash \alpha \neq \emptyset$, $\gamma := \min(\beta \backslash \alpha)$ exists. To show: $\gamma = \alpha$.
First let $\delta \in \gamma$, i.e. $\delta < \gamma$. Then $\delta \notin \beta \backslash \alpha$. Since $\delta \in \gamma \in \beta$, we have $\delta \in \beta$. Hence $\delta \in \alpha$.
Now let $\delta \in \alpha$. If $\delta > \gamma$, then $\alpha > \gamma$, i.e. $\gamma \in \alpha$, a contradiction. Therefore $\delta < \gamma$, i.e. $\delta \in \gamma$. $\square$

Lemma 2.8. $\alpha \leqslant \beta \Leftrightarrow \alpha \subseteq \beta$.

Proof.

$\Rightarrow$ Clear if $\alpha = \beta$. Otherwise $\alpha < \beta$, i.e. $\alpha \in \beta$ and therefore $\alpha \subseteq \beta$ by transitivity.

$\Leftarrow$ $\alpha \subsetneq \beta \Rightarrow \alpha \in \beta \Rightarrow \alpha < \beta$.

□

Proposition 2.9. $<$ *(which is* $\in$*) is a total order on* Ord.

Proof. Assume $\alpha \nleqslant \beta$. Then $\alpha \nsubseteq \beta$. Hence $\beta \in \alpha$, i.e. $\beta < \alpha$. □

Proposition 2.10. *If* $\alpha \neq \beta$, *then* $\alpha \ncong \beta$.

Proof. Without loss of generality $\alpha < \beta$, so α is an initial segment of β. □

Proposition 2.11. $(\mathrm{Ord}, <)$ *is well-ordered.*

Proof. Assume $\alpha_0 > \alpha_1 > \alpha_2 > \dots$ then $(\alpha_0, <)$ is not well-ordered, a contradiction. □

Proposition 2.12.

(*i*) *If* $\alpha \in \mathrm{Ord}$, *then* $\alpha \cup \{\alpha\} \in \mathrm{Ord}$.
($\alpha + 1 := \alpha \cup \{\alpha\}$ is called the ***successor*** *of* α*.)*

(*ii*) *If* A *is a set of ordinals, then* $\bigcup A \in \mathrm{Ord}$.
($\sup A := \bigcup A$ is the ***supremum*** *of* A*.)*

Remark 2.13.

(*i*) $n + 1 = \{0, \dots, n\} = \{0, \dots, n-1\} \cup \{n\}$.

(*ii*) $\sup A$ is not always a max, e.g. $A = \{2n : n \in \omega\}$. Then $\sup A = \omega$, but A has no max.

(*iii*) If $\alpha \in \mathrm{Ord}$, then $\sup \alpha = \alpha$.

Definition 2.14. An ordinal, which is not a succesor, is called a **limit ordinal**.

Proposition 2.15. *If* $\alpha \in \mathrm{Ord}$ *and* $P(x)$ *is a property such that*

(1) $P(0)$ *is true,*

(2) $\forall \beta \in \alpha (P(\beta) \Rightarrow P(\beta + 1))$,

(3) *if* $\beta \in \alpha$ *is a limit ordinal, then* $\forall \gamma < \beta \; P(\gamma) \Rightarrow P(\beta)$,

Then $P(\beta)$ *holds for all* $\beta \in \alpha$.

Theorem 2.16. *If* $(A, <)$ *is a well-ordered set,* $\exists! \alpha \in \mathrm{Ord}, \exists! \pi : A \to \alpha$ *an isomorphism.*

Definition 2.17. This unique ordinal α is called the **order type** of A, written $\alpha = \mathrm{ot}(A)$.

Lemma 2.18. *If* $\exists \alpha \in Ord$ *such that* $A \hookrightarrow \alpha$, *then the theorem holds.*

Proof. Let $\alpha = \min\{\beta \in \mathrm{Ord} : A \hookrightarrow \beta\}$.

(1) $\pi(0) = \min A$.
(2) If $\pi(\beta)$ has been defined, either $\beta + 1 = \alpha$ (and we are done) or $\beta + 1 < \alpha$ and $A_{\pi(\beta)} \subsetneq A$. Set $\pi(\beta+1) = \min(A \backslash A_{\pi(\beta)})$.
(3) If β is a limit ordinal and if $\pi(\gamma)$ has already been defined for all $\gamma < \beta$, we distinguish two cases:
    If $\beta = \alpha$ we are done.
    If $\beta < \alpha$, set $B = \{\pi(\gamma) : \gamma < \beta\}$ and set $\pi(\beta) = \min(A \backslash B)$.

□

3. Arithmetic of ordinals

Definition 3.1. We define the **ordinal sum** $\alpha + \beta$ by induction on β :

(i) $\alpha + 0 = \alpha$,

(ii) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$,

(iii) if β is a limit ordinal, then $\alpha + \beta = \sup\limits_{\gamma < \beta} (\alpha + \gamma)$.

Proposition 3.2.

(i) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

(ii) *If* $\beta < \gamma$, *then* $\alpha + \beta < \alpha + \gamma$.

Proof. We prove (i) by induction on γ.

- $\alpha + (\beta + 0) = \alpha + \beta = (\alpha + \beta) + 0$
-
$$\begin{aligned} \alpha + (\beta + (\gamma + 1)) &= \alpha + ((\beta + \gamma) + 1) \\ &= (\alpha + (\beta + \gamma)) + 1 \\ &= ((\alpha + \beta) + \gamma) + 1 \\ &= (\alpha + \beta) + (\gamma + 1). \end{aligned}$$
-
$$\begin{aligned} \alpha + (\beta + \gamma) &= \alpha + \sup_{\delta < \gamma} (\beta + \delta) \\ &= \sup_{\delta < \gamma} (\alpha + (\beta + \delta)) \\ &= \sup_{\delta < \gamma} ((\alpha + \beta) + \delta) \\ &= (\alpha + \beta) + \gamma. \end{aligned}$$

□

Remark 3.3. *$+$ is not commutative, e.g.* $1+\omega \neq \omega+1$.

Definition 3.4. We define the **ordinal product** $\alpha \cdot \beta$ by induction on β :

(*i*) $\alpha \cdot 0 = 0$,

(*ii*) $\alpha \cdot (\beta+1) = (\alpha \cdot \beta) + \alpha$,

(*iii*) if β is a limit ordinal, then $\alpha \cdot \beta = \sup\limits_{\gamma<\beta}(\alpha \cdot \gamma)$.

Definition 3.5. We define the **ordinal exponentiation** α^β by induction on β :

(*i*) $\alpha^0 = 1$,

(*ii*) $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$,

(*iii*) if β is a limit ordinal, then $\alpha^\beta = \sup\limits_{\gamma<\beta} \alpha^\gamma$.

Proposition 3.6. *Let F be the set of functions $\beta \to \alpha$ with finite support. Define*

$$f < g :\Leftrightarrow f(\gamma) < g(\gamma),$$

where $\gamma = \max\{\delta : f(\delta) \neq g(\delta)\}$. *Then* $\mathrm{ot}((F,<)) = \alpha^\beta$.

Proposition 3.7.

(*i*) $\alpha(\beta+\gamma) = \alpha\beta + \alpha\gamma$,

(*ii*) $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$,

(*iii*) $\left(\alpha^\beta\right)^\gamma = \alpha^{\beta\cdot\gamma}$.

Remark 3.8.

(*i*) $(\omega+1)\cdot 2 \neq \omega \cdot 2 + 1 \cdot 2$,

(*ii*) $(\omega \cdot 2)^2 \neq \omega^2 \cdot 2^2$.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (05: 23/04/15)

SALMA KUHLMANN

Contents

1. Valuation basis

Definition 1.1. $\mathcal{B} \subseteq V \backslash \{0\}$ is a Q**-valuation basis** of (V, v) if

(1) $\mathcal{B}$ is a Q-linear basis for V,
(2) $\mathcal{B}$ is Q-valuation independent.

Remark 1.2. $\mathcal{B}$ is a Q-valuation basis $\Rightarrow$ $\mathcal{B}$ is maximal valuation independent.

(This is because valuation independence $\Rightarrow$ linear independence).

Warning 1.3.

(i) a maximal valuation independent set needs not to be a valuation basis.
Example: $\mathrm{H}_{\mathbb{N}}\,\mathbb{Q}$ is a $\mathbb{Q}$-vector space, with $v_{\min}$ valuation. Consider

$$\mathcal{B} = \{(1, 0, \ldots), (0, 1, \ldots), \ldots\} \subseteq \mathrm{H}_{\mathbb{N}}\,\mathbb{Q} \backslash \{0\}.$$

Then $\forall \gamma \in \mathbb{N} : \mathcal{B}_\gamma = \{1\}$, which is a $\mathbb{Q}$-basis of $B(\gamma)$. Hence, $\mathcal{B}$ is maximal valuation independent. However, note that $\mathcal{B}$ is not a $\mathbb{Q}$-linear basis of $\mathrm{H}_{\mathbb{N}}\,\mathbb{Q}$.

(ii) a valued vector space needs not to admit a valuation basis.

Example 1.4. $(\coprod_{\gamma \in \Gamma} B(\gamma),\ v_{\min})$ admits a valuation basis.

Proof. Let $\mathcal{B}_\gamma$ be a Q-basis of $B(\gamma)$ for all $\gamma \in \Gamma$ and consider

$$\mathcal{B} := \bigcup_{\gamma \in \Gamma} \{b\chi_\gamma;\ b \in \mathcal{B}_\gamma\},$$

where $\forall\, \gamma \in \Gamma$

$$\chi_\gamma \colon \Gamma \longrightarrow Q$$

$$\chi_\gamma(\gamma') = \begin{cases} 1 & \text{if } \gamma = \gamma' \\ 0 & \text{if } \gamma \neq \gamma'. \end{cases}$$

$\square$

Corollary 1.5. *Let (V,v) be a valued Q-vector space with skeleton $S(V) = [\,\Gamma, \{B(\gamma) : \gamma \in \Gamma\}\,]$. Then (V,v) admits a valuation basis if and only if*

$$(V,v) \ \cong \ (\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}).$$

Proof.

($\Leftarrow$) ÜA.

($\Rightarrow$) Let $\mathcal{B} := \{b_i : i \in I\}$ be a valuation basis for (V,v). Then $\mathcal{B}$ is maximal valuation independent. For every $b_i \in \mathcal{B}$ with $v(b_i) = \gamma$ define

$$h(b_i) = \pi(\gamma, b_i)\chi_\gamma \in \bigsqcup_{\gamma\in\Gamma} B(\gamma)$$

and then extend h to all of V by linearity, i.e. for $x \in V$ such that $x = \sum_{b_i\in\mathcal{B}} q_{b_i} b_i$ define

$$h(x) := \sum_{b_i\in\mathcal{B}} q_{b_i} h(b_i).$$

Verify that h is valuation preserving, i.e. verify that

$$v_{\min}(h(x)) = v(x) \ (= \mathrm{id}(v(x))) \quad \forall x \in V$$

First consider the case $x = b_i$. Then it holds by construction $v(b_i) = v_{\min}(h(b_i))$.

For arbitrary x we have $h(x) = \sum q_{b_i} h(b_i)$, and therefore

$$\begin{aligned} v(x) &= \min\{v(b_i) : b_i \in \mathcal{B}\} \\ &= \min\{v_{\min}(h(b_i)) : b_i \in \mathcal{B}\} \\ &= v_{\min}(h(x)). \end{aligned}$$

□

Corollary 1.6. *Let (V,v) be a valued Q-vector space with skeleton $S(V) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. Then*

$$(\bigsqcup_{\gamma\in\Gamma} B(\gamma),\ v_{\min}) \ \hookrightarrow \ (V,v),$$

i.e. there exists a valued subspace (V_0, v_0) of (V,v) such that $(V_0,v_0) \subseteq (V,v)$ is immediate and

$$(V_0, v_0) \cong (\bigsqcup B(\gamma, v_{\min})).$$

Proof. By Zorn's lemma, let $\mathcal{B} \subset V \setminus \{0\}$ be maximal valuation independent. Set

$$V_0 := \langle\, \mathcal{B}\,\rangle_Q.$$

Then $\mathcal{B}$ is a valuation basis of V_0 and the extension $V_0 \subseteq V$ is immediate by maximality. By definition $S(V_0) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. So $(V_0, v_{|V_0})$ admits a valuation basis and has skeleton $S(V_0) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. By the previous corollary $(V_0, v_{|V_0}) \cong (\bigsqcup B(\gamma), v_{\min})$. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (06: 27/04/15 - CORRECTED ON 06/05/2019)

SALMA KUHLMANN

Contents

1. Introduction

Our aim for this and next lecture is to complete the proof of Hahn's embedding Theorem:

Let (V, v) be a Q-valued vector space with $S(V) = [\,\Gamma, B(\gamma)\,]$.
Let $\{x_i : i \in I\} \subset V$ be maximal valuation independent and

$$h\colon V_0 = (\langle\{x_i : i \in I\}\rangle,\ v)\ \xrightarrow{\sim}\ (\coprod_{\gamma\in\Gamma} B(\gamma),\ v_{\min}).$$

Then h extends to a valuation preserving embedding (i.e. an isomorphism onto a valued subspace)

$$\tilde{h}\colon (V, v)\ \hookrightarrow\ (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma),\ v_{\min}).$$

The picture is the following:

$$\begin{tikzcd}
(V,\, v) \arrow[r, hook, "\tilde{h}"] \arrow[d, dash, "\text{immediate}"'] & (\mathrm{H}_{\gamma\in\Gamma}\, B(\gamma),\ v_{\min}) \arrow[d, dash, "\text{immediate}"] \\
(V_0,\, v) \arrow[r, "h", "\sim"'] & (\coprod_{\gamma\in\Gamma} B(\gamma),\ v_{\min})
\end{tikzcd}$$

2. Pseudo-convergence and maximality

Definition 2.1. A valued Q-vector space (V, v) is said to be **maximally valued** if it admits no proper immediate extension.

Definition 2.2. Let $S = \{a_\rho : \rho \in \lambda\} \subset V$ for some limit ordinal λ. Then S is said to be **pseudo-convergent** (or **pseudo-Cauchy**) if for every $\rho < \sigma < \tau$ we have

$$v(a_\sigma - a_\rho) \ < \ v(a_\tau - a_\sigma).$$

Example 2.3.

(*a*) Let $V = (\mathrm{H}_{\mathbb{N}_0}\,\mathbb{R},\, v_{\min})$, where $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. An element $s \in V$ can be viewed as a function $s\colon \mathbb{N}_0 \to \mathbb{R}$. Consider

$$\begin{aligned} a_0 &= (1, 0, 0, 0, 0 \dots) \\ a_1 &= (1, 1, 0, 0, 0 \dots) \\ a_2 &= (1, 1, 1, 0, 0 \dots) \\ &\ \vdots \end{aligned}$$

The sequence $\{a_n : n \in \mathbb{N}_0\} \subset V$ is pseudo-Cauchy.

(*b*) Take (V, v) as above and $s \in V$ with

$$\mathrm{support}(s) = \mathbb{N}_0,$$

i.e. $s_i := s(i) \neq 0\ \forall\, i \in \mathbb{N}_0$. Define the sequence

$$\begin{aligned} b_0 &= (s_0, 0, 0, 0, 0 \dots) \\ b_1 &= (s_0, s_1, 0, 0, 0 \dots) \\ b_2 &= (s_0, s_1, s_2, 0, 0 \dots) \\ &\ \vdots \end{aligned}$$

For every $l < m < n \in \mathbb{N}_0$, we have

$$l + 1 = v_{\min}(b_m - b_l) < v_{\min}(b_n - b_m) = m + 1.$$

Therefore $\{b_n : n \in \mathbb{N}_0\} \subset V$ is pseudo-Cauchy.

Lemma 2.4. *If $S = \{a_\rho\}_{\rho\in\lambda}$ is pseudo-convergent then*

(*i*) *either $v(a_\rho) < v(a_\sigma)$ for all $\rho < \sigma \in \lambda$,*

(*ii*) *or $\exists\, \rho_0 \in \lambda$ such that $v(a_\rho) = v(a_\sigma)\ \ \forall\, \rho, \sigma \geqslant \rho_0$.*

Proof. Assume (*i*) does not hold, i.e. $v(a_\rho) \geqslant v(a_\sigma)$ for some $\rho < \sigma \in \lambda$. Then we claim that

$$v(a_\tau) = v(a_\sigma) \qquad \forall\, \tau > \sigma.$$

Otherwise, $v(a_\tau - a_\sigma) = \min\{v(a_\tau), v(a_\sigma)\} \leqslant v(a_\sigma)$.

But $v(a_\sigma - a_\rho) \geqslant v(a_\sigma)$, contradicting pseudo-convergence for $\rho < \sigma < \tau$. $\square$

Notation 2.5. In case (ii) define

$$\operatorname{Ult} S := v(a_{\rho_0}) = v(a_\rho) \qquad \forall \rho \geqslant \rho_0.$$

Lemma 2.6. *If $\{a_\rho\}_{\rho\in\lambda}$ is pseudo-convergent, then for all $\rho < \sigma \in \lambda$ we have*

$$v(a_\sigma - a_\rho) = v(a_{\rho+1} - a_\rho).$$

Proof. We may assume $\sigma > \rho + 1$ (so $\rho < \rho + 1 < \sigma$). From

$$v(a_{\rho+1} - a_\rho) < v(a_\sigma - a_{\rho+1})$$

and the identity

$$a_\sigma - a_\rho = (a_\sigma - a_{\rho+1}) + (a_{\rho+1} - a_\rho),$$

we deduce that

$$\begin{aligned} v(a_\sigma - a_\rho) &= \min\{v(a_\sigma - a_{\rho+1}), v(a_{\rho+1} - a_\rho)\} \\ &= v(a_{\rho+1} - a_\rho). \end{aligned}$$

□

Notation 2.7.

$$\begin{aligned} \gamma_\rho :&= v(a_{\rho+1} - a_\rho) \\ &= v(a_\sigma - a_\rho) \qquad \forall\, \sigma > \rho. \end{aligned}$$

Remark 2.8. Since $\rho < \rho + 1 < \rho + 2$, we have $\gamma_\rho < \gamma_{\rho+1}$ for all $\rho \in \lambda$.

3. Pseudo-limits

Definition 3.1. Let $S = \{a_\rho\}_{\rho\in\lambda}$ be a pseudo-convergent set. We say that $x \in V$ is a **pseudo-limit** of S if

$$v(x - a_\rho) = \gamma_\rho \qquad \text{for all } \rho \in \lambda.$$

Remark 3.2.

(i) If $v(a_\rho) < v(a_\sigma)$ for $\rho < \sigma$, then $x = 0$ is a pseudo-limit.

(ii) If 0 is not a pseudo-limit and x is a pseudo-limit, then $v(x) = \operatorname{Ult} S$.

Example 3.3.

(a) In Example 2.3(a), the constant function 1:

$$a = (1, 1, \dots)$$

is a pseudo-limit of the sequence $\{a_n\}_{n\in\mathbb{N}_0}$.

(*b*) In Example 2.3(*b*), s is a pseudo-limit of $\{b_n\}_{n\in\mathbb{N}_0}$.

Definition 3.4. (V, v) is **pseudo-complete** if every pseudo-convergent sequence in V has a pseudo-limit in V.

We will analyse the set of pseudo-limits of a given pseudo-Cauchy sequence (this set can be empty, a singleton, or infinite).

Definition 3.5. Let $S = \{a_\rho\}_{\rho\in\lambda}$ be a pseudo-convergent set. The **breadth** (*Breite*) B of S is defined to be the following subset of V:

$$B = B(S) := \{y \in V : v(y) > \gamma_\rho \ \forall\, \rho \in \lambda\}.$$

Lemma 3.6. *Let $S = \{a_\rho\}_{\rho\in\lambda}$ be pseudo-convergent with breadth B and let $x \in V$ be a pseudo-limit of S. Then an element of V is a pseudo-limit of S if and only if it is of the form $x + y$ with $y \in B$.*

Proof.

($\Rightarrow$) Let z be another pseudo-limit of S. It follows from

$$x - z = (x - a_\rho) - (z - a_\rho)$$

that

$$v(x - z) \geqslant \min\{v(x - a_\rho), v(z - a_\rho)\} = \gamma_\rho \qquad \forall\, \rho \in \lambda.$$

Since γ_ρ is strictly increasing, it follows $v(x-z) > \gamma_\rho$ for all $\rho \in \lambda$. So $x - z \in B$ is as required.

($\Leftarrow$) If $y \in B$ then $v(y) > \gamma_\rho = v(x - a_\rho)$ for all $\rho \in \lambda$. Then

$$v((x + y) - a_\rho) = v((x - a_\rho) + y) = \min\{v(x - a_\rho), v(y)\} = \gamma_\rho \qquad \forall\, \rho \in \lambda.$$

□

4. Cofinality

Definition 4.1. Let Γ be a totally ordered set. A subset $A \subset \Gamma$ is cofinal in Γ if

$$\forall\, \gamma \in \Gamma\ \exists\, a \in A \text{ with } \gamma \leqslant a.$$

Example 4.2. If $\Gamma = [0, 1] \subset \mathbb{R}$, then $A = \{1\}$ is cofinal in Γ.

Lemma 4.3. *Let $\emptyset \neq \Gamma$ be a totally ordered set. Then there is a well-ordered cofinal subset $A \subset \Gamma$. Moreover if Γ has no last element, then A has also no last element, i.e. the order type of A is a limit ordinal.*

Remark 4.4. Note that if $\{a_\rho\}_{\rho\in\lambda}$ is pseudo-Cauchy in (V, v), $x \in V$ is a pseudo-limit and $\{\gamma_\rho\}_{\rho\in\lambda}$ is cofinal in $\Gamma = v(V)$, then it follows by Lemma 3.6 that the limit is unique. This is because if $\{\gamma_\rho\}_{\rho\in\lambda}$ is cofinal in Γ, then $B(S) = \{0\}$.

Warning: $\{\gamma_\rho\}_{\rho\in\lambda}$ is cofinal in $\Gamma \not\Rightarrow S$ has no limit.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (07: 30/04/15 - CORRECTED ON 13/05/2019)

SALMA KUHLMANN

Contents

1. Pseudo-completeness

Let (V, v) be a valued Q-vector space. We recall that

- (V, v) is **maximally valued** if (V, v) admits no proper immediate extension.
- (V, v) is **pseudo-complete** if every pseudo-convergent sequence in V has a pseudo-limit in V.

Theorem 1.1. *(V, v) is maximally valued if and only if (V, v) is pseudo-complete.*

Today we will prove the implication:

(V, v) pseudo-complete $\Rightarrow$ (V, v) maximally valued.

It follows from the following proposition:

Proposition 1.2. *Let (V, v) be an immediate extension of (V_0, v). Then any element in V which is not in V_0 is a pseudo-limit of a pseudo-Cauchy sequence of elements of V_0, without a pseudo-limit in V_0.*

Note that once the proposition is established we have pseudo complete $\Rightarrow$ maximally valued. If not, assume that (V, v) is not maximally valued. Then there is a proper immediate extension (V', v') of (V, v). Let $y \in V' \backslash V$. By the proposition y is a pseudo-limit of a pseudo-Cauchy sequence in V without pseudo-limit in (V, v), a contradiction.

Proof. (of the proposition)
Let $z \in V \setminus V_0$. Consider the set

$$X = \{v(z - a) : a \in V_0\} \subset \Gamma.$$

Since $z \notin V_0$, $\infty \notin X$. We show that X can not have a maximal element. Otherwise, let $a_0 \in V_0$ be such that $v(z - a_0)$ is maximal in X. By the characterization of immediate extensions (Lecture 3, Lemma 2.2), there exists some $a_1 \in V_0$ such that $v((z-a_0)-a_1) > v(z-a_0)$. So $a_0 + a_1 \in V_0$ and $v(z-(a_0+a_1)) > v(z-a_0)$, a contradiction. Thus, X has no greatest element.

Select from X a well-ordered cofinal subset $\{\alpha_\rho\}_{\rho\in\lambda}$. Note that $\{\alpha_\rho\}_{\rho\in\lambda}$ has no last element, as λ is a limit ordinal.

For every $\rho \in \lambda$ choose an element $a_\rho \in V_0$ with

$$v(z - a_\rho) = \alpha_\rho.$$

The identity

$$a_\sigma - a_\rho = (z - a_\rho) - (z - a_\sigma)$$

and the inequality

$$v(z - a_\rho) < v(z - a_\sigma) \qquad\qquad (\forall\, \rho < \sigma \in \lambda)$$

imply

$$(*) \qquad\qquad v(a_\sigma - a_\rho) = v(z - a_\rho).$$

Thus, $\{a_\rho\}_{\rho\in\lambda}$ is pseudo-convergent with z as a pseudo-limit.

Finally suppose that $\{a_\rho\}_{\rho\in\lambda}$ has a further limit $z_1 \in V_0$.

By a result from the last lecture we have

$$v(z - z_1) > v(a_\sigma - a_\rho).$$

Combining this with $(*)$ we get

$$v(z - z_1) > v(z - a_\rho) = \alpha_\rho \qquad \forall\, \rho \in \lambda$$

and this is a contradiction, since $\{\alpha_\rho\}_{\rho\in\lambda}$ is cofinal in X. □

Theorem 1.3. *Suppose that*

(*i*) *V_i and V_i' are Q-valued vector spaces and V_i' is an immediate extension of V_i for $i = 1, 2$.*

(*ii*) *$h : V_1 \to V_2$ is an isomorphism of valued vector spaces.*

(*iii*) *V_2' is pseudo-complete.*

Then there exists an embedding $h' : V_1' \to V_2'$ such that h' extends h. Moreover h' is an isomorphism of valued vector spaces if and only if V_1' is pseudo-complete.

Proof. The picture is the following:

$$\begin{tikzcd}
V_1' \arrow[r, hook, "h'"] \arrow[d, dash, "\text{immediate}"'] & V_2' \arrow[d, dash, "\text{immediate}"] \\
V_1 \arrow[r, "h", "\sim"'] & V_2
\end{tikzcd}$$

Consider the collection of triples (M_1, M_2, g), where

$$V_1 \subseteq M_1 \subseteq V_1',$$
$$V_2 \subseteq M_2 \subseteq V_2',$$

and g a valuation preserving isomorphism of M_1 onto M_2 extending h.

This collection is non-empty, because (V_1, V_2, h) belongs to it. Moreover, one can show that every chain has an upper bound (ÜA). Therefore the conditions of Zorn's lemma are satisfied, i.e. there exists a maximal such triple (M_1, M_2, g). We claim that $M_1 = V_1'$. Assume for a contradiction there exists some $y_1 \in V_1' \setminus M_1$.

(**Note:** If $V_0 \subset V_1 \subset V_2$ are extensions of valued vector spaces and $V_2|V_0$ is immediate, then $V_2|V_1$ and $V_1|V_0$ are immediate)

Since V_1' is an immediate extension of M_1, there exists a pseudo-convergent sequence $S = \{a_\rho\}_{\rho\in\lambda}$ of M_1 without a pseudo-limit in M_1, but with a pseudo-limit $y_1 \in V_1'$. Consider $g(S) = \{g(a_\rho)\}_{\rho\in\lambda}$.

(**Facts/ÜA:**

- (i) the image of a pseudo-convergent sequence under a valuation preserving isomorphism is pseudo-convergent.
- (ii) the image of a pseudo-limit of a pseudo-convergent sequence under a valuation preserving isomorphism is a pseudo-limit of the image of the pseudo-convergent sequence.
- (iii) the image of a pseudo-complete vector space under a valuation preserving isomorphism is pseudo-complete.)

Since g is a valuation preserving isomorphism, $g(S)$ is a pseudo-convergent sequence of M_2 without a pseudo-limit in M_2 but with a pseudo-limit $y_2 \in V_2'$, because V_2' is pseudo-complete.

Let $M_i' = \langle M_i, y_i\rangle_Q$ for $i = 1, 2$, and denote by g' the unique Q-vector space isomorphism of the linear space M_1' onto the linear space M_2' extending g such that $g'(y_1) = y_2$.

We show that g' is valuation preserving: let

$$y = x + qy_1 \qquad x \in M_1 \quad (q \in Q \setminus \{0\})$$

be an arbitrary element of $M_1' \setminus M$. The sequence

$$S(y) = \{x + qa_\rho\}_{\rho\in\lambda}$$

is pseudo-convergent in M_1 with pseudo-limit $y \in M_1'$ and 0 is not a pseudo-limit (otherwise $-x/q \in M_1$ would be a pseudo-limit of S).

It follows that (since $y = x + qy_1$ is a pseudo-limit for the sequence $x + qa_\rho$ which does not have 0 as a pseudo-limit)

$$v(y) = \operatorname{Ult} S(y)$$

and similarly

$$v(g'(y)) = \operatorname{Ult} S(g'(y)),$$

where

$$S(g'(y)) = \{g'(x) + qg'(a_\rho)\}_{\rho \in \lambda}$$

is a pseudo-convergent sequence of M_2 with pseudo-limit $g'(y) \in M_2'$. Now $g'_{|M_1} = g$ is valuation preserving from M_1 to M_2. So we have

$$\mathrm{Ult}(S(y)) = \mathrm{Ult}(S(g'(y))),$$

hence

$$v(y) = v(g'(y))$$

as required.

Now if h' is onto, then V_1' is pseudo-complete. Conversely, if V_1' is pseudo-complete, then $h'(V_1')$ is also pseudo-complete and hence maximally valued. So the immediate extension $V_2'|h'(V_1')$ cannot be proper, i.e. $h'(V_1') = V_2'$. Thus, h' is onto as claimed. $\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (08: 04/05/15 - CORRECTED ON 13/05/2019)

SALMA KUHLMANN

Contents

1. Pseudo-completeness

In the last lecture we showed that pseudo complete implies maximally valued. Today, we prove the converse implication.

Proposition 1.1. *The Hahn product* $(\mathrm{H}_{\gamma\in\Gamma} B(\gamma), v_{\min})$ *is pseudo-complete.*

Proof. Let $\{a_\rho\}_{\rho\in\lambda}$ be pseudo-Cauchy. Recall that $\gamma_\rho = v(a_\rho - a_{\rho+1})$ is a strictly increasing sequence. Define $x \in \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$ by

$$x(\gamma) = \begin{cases} a_\rho(\gamma) & \text{if } \gamma < \gamma_\rho \text{ for some } \rho. \\ 0 & \text{otherwise.} \end{cases}$$

This is well-defined because if $\rho_1 < \rho_2 \in \lambda$, $\gamma < \gamma_{\rho_1}$ and $\gamma < \gamma_{\rho_2}$, then $v(a_{\rho_1} - a_{\rho_2}) = \gamma_{\rho_1}$
and therefore

$$a_{\rho_1}(\gamma) = a_{\rho_2}(\gamma)$$

(note that $v_{\min}(a-b)$ is the first spot where a and b differ).

Now we show that support(x) is well-ordered.
Let $A \subseteq \text{support}(x)$, $A \neq \emptyset$ and $\gamma_0 \in A$. Then $\exists\, \rho$ such that $\gamma_0 < \gamma_\rho$ and $x(\gamma_0) = a_\rho(\gamma_0)$ with $\gamma_0 \in \text{support}(a_\rho)$. Consider

$$A_0 := \{\gamma \in A : \gamma \leqslant \gamma_0\}.$$

Note that since $x(\gamma) = a_\rho(\gamma)$ for $\gamma \leqslant \gamma_0$ it follows that $A_0 \subseteq \text{support}(a_\rho)$ which is well-ordered, so $\min A_0$ exists in A_0 and it is the least element of A.
We conclude by showing that x is a pseudo-limit. By definition of x follows

$$v(x - a_\rho) \geqslant \gamma_\rho = v(a_{\rho+1} - a_\rho) \quad \forall\, \rho \in \lambda.$$

If $v(x - a_\rho) > v(a_\rho - a_{\rho+1})$, then

$$v(x - a_{\rho+1}) = v(x - a_\rho + a_\rho - a_{\rho+1}) = v(a_\rho - a_{\rho+1}) = \gamma_\rho,$$

but on the other hand we have

$$v(x - a_{\rho+1}) \geqslant \gamma_{\rho+1} > \gamma_\rho,$$

a contradiction. $\square$

Corollary 1.2. *Let (V, v) be a valued vector space with $S(V) = [\Gamma, \{B(\gamma), \gamma \in \Gamma\}]$. Then there exists a valuation preserving embedding*

$$(V, v) \hookrightarrow (\mathrm{H}_{\gamma\in\Gamma} B(\gamma), v_{\min})$$

Proof. The picture is the following:

$$\begin{tikzcd} V_1' = V \arrow[r, hook, "h'"] & \mathrm{H}_{\gamma\in\Gamma} B(\gamma) = V_2' \\ V_1 \arrow[u, dash, "\text{immediate}"] \arrow[r, "h", "\sim"'] & \coprod_{\gamma\in\Gamma} B(\gamma) = V_2 \arrow[u, dash, "\text{immediate}"'] \end{tikzcd}$$

Let $\mathcal{B}$ be a maximal valuation independent set in V and set $V_1 = \langle \mathcal{B} \rangle_Q$. Then V_1 has a valuation basis and therefore h exists and $V|V_1$ is immediate. □

Hilfslemma 1.3. *Let (V_1, v_1) be maximally valued, (V_2, v_2) a valued vector space and $h : V_1 \to V_2$ a valuation preserving isomorphism. Then (V_2, v_2) is maximally valued.*

Proof. Let $S(V_1) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. Assume that V_2 is not maximally valued, so $\exists V_2'$ a proper immediate extension. By our main theorem there exists an embedding h' of immediate extensions V_2' into $\mathrm{H}_{\gamma\in\Gamma} B(\gamma)$. This is impossible, since h' cannot be injective. □

Corollary 1.4. *Let (V, v) be a maximally valued vector space. Then it is pseudo complete. In fact*

$$(V, v) \simeq (\mathrm{H}_{\gamma\in\Gamma} B(\gamma), v_{\min}),$$

where $S(V) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$.

Proof. By the first corollary, the picture is the following

$$\begin{tikzcd} & \mathrm{H}\, B(\gamma) \\ V \arrow[r, "h", "\sim"'] & V_2. \arrow[u, dash, "\text{immediate}"'] \end{tikzcd}$$

Since V is maximally valued, it follows from the Hifslemma that V_2 is maximally valued. Therefore the extension $\mathrm{H}\, B(\gamma)|V_2$ is not proper, i.e. $V_2 = \mathrm{H}\, B(\gamma)$. Thus h is surjective, i.e. h is an isomorphism of valued vector spaces $V \to \mathrm{H}_{\gamma\in\Gamma} B(\gamma)$. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES
(09: 07/05/15 - CORRECTED ON 16/05/19)

SALMA KUHLMANN

Contents

1. Ordered abelian groups

Definition 1.1. $(G,+,0,<)$ is a (totally) **ordered abelian group** if $(G,+,0)$ is an abelian group and $<$ a total order on G, such that for all $a,b,c \in G$

$$a \leqslant b \ \Rightarrow \ a+c \leqslant b+c \quad (*).$$

Definition 1.2. A subgroup C of an ordered abelian group G is **convex** if $\forall\, c_1, c_2 \in C$ and $\forall\, x \in G$

$$c_1 < x < c_2 \ \Rightarrow \ x \in C.$$

Note that because of $(*)$ this is equivalent to requiring $\forall\, c \in C$ and $\forall\, x \in G$

$$0 < x < c \Rightarrow x \in C.$$

Example 1.3. $C = \{0\}$ and $C = G$ are convex subgroups.

Lemma 1.4. *Let G be an ordered abelian group and C a convex subgroup of G. Then*

(i) *G/C is an ordered abelian group by defining $g_1+C \leqslant g_2+C$ if $g_1 \leqslant g_2$.*

(ii) *There is a bijective correspondence between convex subgroups $C \subseteq C' \subseteq G$ and convex subgroups of G/C.*

(iii) *In particular, if D and C are convex subgroups of G such that $D \subset C$ and there are no further subgroups between D and C, then C/D has no non-trivial convex subgroups.*

(iv) *If an ordered abelian group has only the trivial convex subgroups, then it is an Archimedean group.*

Definition 1.5. Let G be an ordered abelian group, $x \in G$, $x \neq 0$.
We define:

$$C_x := \bigcap \{C : C \text{ is a convex subgroup of } G \text{ and } x \in C\}.$$

$$D_x := \bigcup \{D : D \text{ is a convex subgroup of } G \text{ and } x \notin D\}.$$

A convex subgroup C of G is said to be **principal** if there is some $x \in G$ such that $C = C_x$.

Lemma 1.6.

(*i*) *C_x and D_x are convex subgroups of G.*

(*ii*) *$D_x \subsetneq C_x$.*

(*iii*) *D_x is the largest proper convex subgroup of C_x, i.e. if C is a convex subgroup such that*

$$D_x \subseteq C \subseteq C_x$$

then $C = D_x$ or $C = C_x$.

(*iv*) *It follows that the ordered abelian group C_x/D_x has no non-trivial proper convex subgroup.*

2. Archimedean groups

Definition 2.1. Let $(G, +, 0, <)$ be an ordered abelian group. We say that G is **Archimedean** if for all non-zero $x, y \in G$:

$$\exists\, n \in \mathbb{N} : \quad n|x| > |y| \;\text{ and }\; n|y| > |x|,$$

where for every $g \in G$, $|g| := \max\{g, -g\}$.

Proposition 2.2. *(Hölder) Every Archimedean group is isomorphic to a subgroup of* $(\mathbb{R}, +, 0, <)$.

Proposition 2.3. *G is Archimedean if and only if G has no non-trivial proper convex subgroup.*

Therefore if G is an ordered group and $x \in G$ with $x \neq 0$, the quotient C_x/D_x is Archimedean (by 2.3) and can be embedded in $(\mathbb{R}, +, 0, <)$ (by 2.2).

Definition 2.4. Let G be an ordered group, $x \in G$, $x \neq 0$. We say that

$$B_x := C_x/D_x$$

is **the Archimedean component** associated to x.

3. Archimedean equivalence

Definition 3.1. An abelian group G is **divisible** if for every $x \in G$ and for every $n \in \mathbb{N}$ there is some $y \in G$ such that $x = ny$.

Remark 3.2. Any ordered divisible abelian group G is an ordered $\mathbb{Q}$-vector space and G can be viewed as a valued $\mathbb{Q}$-vector space in a natural way.

Definition 3.3. (Archimedean equivalence) Let G be an ordered abelian group. For every $0 \neq x, y \in G$ we define

$$\begin{aligned} x \ \sim^+ \ y \quad &:\Leftrightarrow \quad \exists\, n \in \mathbb{N} \quad n|x| \geqslant |y| \ \text{ and } \ n|y| \geqslant |x|. \\ x \ <<^+ \ y \quad &:\Leftrightarrow \quad \forall\, n \in \mathbb{N} \quad n|x| < |y|. \end{aligned}$$

Proposition 3.4.

(1) $\sim^+$ *is an equivalence relation.*

(2) $\sim^+$ *is compatible with* $<<^+$*:*

$$\begin{aligned} x <<^+ y \quad \textit{and} \quad x \sim^+ z \quad &\Rightarrow \quad z <<^+ y, \\ x <<^+ y \quad \textit{and} \quad y \sim^+ z \quad &\Rightarrow \quad x <<^+ z. \end{aligned}$$

Because of the last proposition we can define a linear order $<_\Gamma$ on $\Gamma := G/\sim^+$, the set of equivalence classes $\{[x] : x \in G\}$, as follows:

$$\forall x, y \in G\backslash\{0\} : \ [y] <_\Gamma [x] \quad \Leftrightarrow \quad x <<^+ y \quad (\text{and } \infty > \Gamma)$$

(convention: $[0] = \infty$)

Proposition 3.5.

(1) Γ *is a totally ordered set under* $<_\Gamma$.

(2) *The map*

$$\begin{aligned} v \colon G \ &\longrightarrow \ \Gamma \cup \{\infty\} \\ 0 \ &\mapsto \ \infty \\ x \ &\mapsto \ [x] \quad (\textit{if } x \neq 0) \end{aligned}$$

is a valuation on G *as a* $\mathbb{Z}$*-module, called the* ***natural valuation****:*

For every $x, y \in G$*:*

- $v(x) = \infty$ *iff* $x = 0$,
- $v(nx) = v(x) \quad \forall\, n \in \mathbb{Z},\ n \neq 0$,
- $v(x + y) \geqslant \min\{v(x), v(y)\}$.

(3) *if* $x \in G$, $x \neq 0$, $v(x) = \gamma$, *then*

$$G^{\gamma} := \{a \in G : v(a) \geqslant \gamma\} = C_x.$$
$$G_{\gamma} := \{a \in G : v(a) > \gamma\} = D_x.$$

So

$$B_x = C_x/D_x = G^{\gamma}/G_{\gamma} = B(\gamma)$$

is the Archimedean component associated to γ. *By Hölder's Theorem, the homogeneous components* $B(\gamma)$ *are all (isomorphic to) subgroups of* $(\mathbb{R}, +, 0, <)$.

Example 3.6. Let $[\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$ be an ordered family of Archimedean groups. Consider $\coprod_{\gamma\in\Gamma} B(\gamma)$ endowed with the lexicographic order $<_{\mathrm{lex}}$: for $0 \neq g \in \coprod_{\gamma\in\Gamma} B(\gamma)$ let $\gamma := \min \operatorname{support} g$. Then declare $g > 0 :\Leftrightarrow g(\gamma) > 0$.

Then $(\coprod B(\gamma), <_{\mathrm{lex}})$ is an ordered abelian group. Moreover, the natural valuation is the $v_{\min}$ valuation. Similarly for the Hahn product.

Theorem 3.7. *(Hahn's embedding theorem for divisible ordered abelian groups) Let* G *be a divisible ordered abelian group with skeleton* $S(G) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. *Then*

$$\left(\coprod B(\gamma), <_{\mathrm{lex}}\right) \hookrightarrow (G, <) \hookrightarrow (\mathrm{H}\, B(\gamma), <_{\mathrm{lex}}).$$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (10: 11/05/15 - CORRECTED ON 20/05/2019)

SALMA KUHLMANN

Contents

Chapter II: Valuations on ordered fields (particularly real closed fields)

1. Valued fields

Definition 1.1. Let K be a field, G an ordered abelian group and ∞ an element greater than every element of G. A surjective map

$$w\colon K \longrightarrow G \cup \{\infty\}$$

is a **valuation** if and only if $\forall\, a, b \in K$:

(*i*) $w(a) = \infty \;\Leftrightarrow\; a = 0$,

(*ii*) $w(ab) = w(a) + w(b)$,

(*iii*) $w(a - b) \geqslant \min\{w(a), w(b)\}$.

Immediate consequences:

- $w(1) = 0$,
- $w(a) = w(-a)$,
- $w(a^{-1}) = -w(a)$ if $a \neq 0$,
- $w(a) \neq w(b) \;\Rightarrow\; w(a + b) = \min\{w(a), w(b)\}$.

Definition 1.2.

(*i*) $R_w := \{a \in K : w(a) \geqslant 0\}$ is a subring of K, called the **valuation ring** of w.

(*ii*) $I_w := \{a \in K : w(a) > 0\} \subseteq R_w$ is called the **valuation ideal** of w.

(*iii*) $U_w := \{a \in R_w : a^{-1} \in R_w\} = \{a \in R_w : w(a) = 0\}$ is a multiplicative subgroup of R_w and is called the **group of units** of R_w.

Remark 1.3.

- Note that $R_w = U_w \mathbin{\dot\cup} I_w$. By this observation one can immediately show that R_w is a local ring with unique maximal ideal I_w.

- Note that for any $x \in K^\times$ either $x \in R_w$ or $x^{-1} \in R_w$ (or both in case $x \in U_w$).

Definition 1.4.

(*i*) The **residue field** is denoted by $K_w := R_w/I_w$.

(*ii*) The **residue map** $R_w \to K_w$, $a \mapsto \overline{a} := aw$ is the canonical projection.

(*iii*) The **group of** 1**-units** of R_w is denoted by

$$1 + I_w := \{a \in R_w : w(a-1) > 0\}$$

and is a multiplicative subgroup of U_w.

2. The natural valuation of an ordered field

Let $(K, +, \cdot, 0, 1, <)$ be an ordered field.

Remark 2.1. $(K, +, 0, <)$ is an ordered divisible abelian group.

So on $(K, +, 0, 1)$ we have already defined the natural valuation, namely via the "Archimedean equivalence relation":

$$\begin{array}{rcc} 0 \neq a & \mapsto & v(a) := [a] \\ 0 & \mapsto & \infty \end{array}$$

We have set $G := (K, +, 0, 1)/\sim^+$ and totally ordered G by

$$[a] < [b] :\Leftrightarrow b <<^+ a.$$

We shall show now that we can endow the totally ordered value set $(G, <)$ with a group operation $+$ such that $(G, +, <)$ is a totally ordered abelian group. For every $a, b \in K \setminus \{0\}$ define

$$[a] + [b] := [ab],$$

or in valuation notation

$$v(a) + v(b) := v(ab).$$

Lemma 2.2.

(*i*) $(G, +, <)$ *is an ordered abelian group.*

(*ii*) *The map* $v : (K, +, \cdot, 0, 1, <) \to G \cup \{\infty\}$ *is a (field) valuation.*

From now on let K be an ordered field and $v : K \to G \cup \{\infty\}$ its natural valuation, with value group $v(K^*) = G$.

Consider

$R_v := \{a \in K : v(a) \geqslant 0\}$,

$I_v := \{a \in K : v(a) > 0\}$.

What are R_v and I_v (from the point of view of chapter 1)?

$$\begin{aligned} R_v :&= \{a : [a] \geqslant [1]\} \\ &= \{a : a \sim^+ 1 \text{ or } a <<^+ 1\} \\ &= \{a : v(a) \geqslant v(1)\}. \\ I_v :&= \{a : [a] > [1]\} \\ &= \{a : a <<^+ 1\} \\ &= \{a : v(a) > v(1)\}. \end{aligned}$$

Proposition 2.3. *(Properties of the natural valuation)*

(1) *The valuation ring R_v is a convex subring of K. It consists of all the elements of K that are bounded in absolute value by some natural number $n \in \mathbb{N}$. Therefore R_v is often called the ring of bounded elements, or the ring of finite elements.*
This valuation ring of the natural valuation is indeed the convex hull of $\mathbb{Q}$ in K. It is the smallest convex subring of $(K, <)$.

(2) *The valuation ideal I_v is a convex ideal. It consists of all elements of K that are strictly bounded in absolute value by $\frac{1}{n}$ for every $n \in \mathbb{N}$. Therefore I_v is called the ideal of infinitely small elements, or ideal of infinitesimal elements.*

(3) *The residue field K_v is Archimedean, i.e. a subfield of $\mathbb{R}$.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (11: 18/05/15 - CORRECTED ON 22/05/19)

SALMA KUHLMANN

Contents

1. The field of generalized power series

Let $k \subseteq \mathbb{R}$ be an Archimedean field and G an ordered abelian group. Recall that we have defined a (totally) ordered abelian group, namely the Hahn product

$$\mathbb{K} := \mathrm{H}_G(k, +, 0, <),$$

i.e. take the Hahn product over the family $S := [G, \{k : g \in G\}]$ with the lexicographic ordering, i.e.

$$\mathbb{K} := \{s : G \to k : \text{support}\, s \text{ is well-ordered in } G\},$$

where support $s := \{g \in G : s(g) \neq 0\}$.
Endow this set with pointwise addition of functions, i.e. $\forall s, r \in \mathbb{K}$

$$(s + r)(g) := s(g) + r(g) \in k,$$

and the lexicographic order:

$$s > 0 :\Leftrightarrow s(\min \text{support}(s)) > 0 \text{ in } k \quad \forall s \in \mathbb{K} \backslash \{0\}.$$

We have verified that $(\mathbb{K}, +, <_{\text{lex}})$ is an ordered abelian group. Our first goal of today is to make $\mathbb{K}$ into a (totally) ordered field. We need to define multiplication.

Notation 1.1. For $s \in \mathbb{K}$ write

$$s = \sum_{g \in G} s(g) t^g = \sum_{g \,\in\, \text{support}\, s} s(g) t^g.$$

Definition 1.2. For $r, s \in \mathbb{K}$ define

$$(rs)(g) := \sum_{h \in G} r(g - h) s(h),$$

i.e.

$$sr = \sum_{g \in G} \left(\sum_{h \in G} r(g - h) s(h) \right) t^g.$$

We now adress the following problem: Let $\mathfrak{F} := \{s_i : i \in I\} \subseteq \mathbb{K}$. Can we "make sense" of $\sum_{i \in I} s_i$ as an element of $\mathbb{K}$?

Definition 1.3.

(i) The family $\mathfrak{F}$ is said to be **summable**, if
  (1) $\operatorname{support} \mathfrak{F} := \bigcup_{i \in I} \operatorname{support} s_i$ is well-ordered in G,
  (2) $\forall g \in \operatorname{support} \mathfrak{F}$, the set $S_g := \{i \in I : g \in \operatorname{support} s_i\}$ is finite.

(ii) Assume that $\mathfrak{F}$ is summable. Write

$$\sum_{i \in I} s_i := \sum_{g \,\in\, \operatorname{support} \mathfrak{F}} \left(\sum_{i \in S_g} s_i(g) \right) t^g.$$

We now prove that this multiplication is well-defined. For $h \in G$ define

$$\begin{aligned} \rho_h := t^h r : &= \sum_{g \in G} r(g) t^{g+h} \\ &= \sum_{g \,\in\, \operatorname{support} r} r(g) t^{g+h}, \end{aligned}$$

i.e. $\rho_h(g) = r(g-h)\ \forall g \in G$. Note that $\rho_h \in \mathbb{K}$ because

$$\operatorname{support} \rho_h = \operatorname{support} r \oplus \{h\} = \{g + h : g \in \operatorname{support} r\},$$

which is again well-ordered (ÜA).

We now consider

$$\mathfrak{F} := \{s(h)\rho_h : h \in \operatorname{support} s\}.$$

Lemma 1.4. *$\mathfrak{F}$ is summable.*

Note that once the lemma is established we define

$$sr = \sum_{h \,\in\, \operatorname{support} s} s(h)\rho_h = \sum_{g \,\in\, \operatorname{support} \mathfrak{F}} \left(\sum_{h \in S_g} s(h)\rho_h(g) \right) t^g,$$

and comparing, we see that this is the product.

Proof. (1) Show that $\operatorname{support} \mathfrak{F} = \bigcup_{h \in \operatorname{support} s} \operatorname{support}(\rho_h s(h))$ is well-ordered. Indeed

$$\begin{aligned} \bigcup_{h \,\in\, \operatorname{support} s} \operatorname{support}(\rho_h s(h)) &= \bigcup_{h \,\in\, \operatorname{support} s} (\operatorname{support} r \oplus \{h\}) \\ &= \operatorname{support} s \oplus \operatorname{support} r. \end{aligned}$$

ÜA: If A, B are well-ordered, then $A \oplus B$ is well-ordered.

(2) Show that $S_g = \{h \in \operatorname{support} s : g \in \operatorname{support}(\rho_h s(h))\}$ is finite for $g \in \operatorname{support} \mathfrak{F}$. We have

$$\begin{aligned} S_g : &= \{h \in \operatorname{support} s : g \in \operatorname{support} r \oplus \{h\}\} \\ &= \{h \in \operatorname{support} s : g = g' + h, g' \in \operatorname{support} r\} \\ &= \{h \in \operatorname{support} s : g - h \in \operatorname{support} r\}. \end{aligned}$$

Assume S_g is infinite. Since S_g is well-ordered, take an infinite strictly increasing sequence in it, say a sequence of $h's$ in it. But then $g - h's$ is an infinite strictly decreasing sequence in support r, contradicting that support r is well-ordered. □

Note we have shown that $\operatorname{support}(rs) \subseteq \operatorname{support} r \oplus \operatorname{support} s$.

Notation 1.5. $\mathbb{K} = k((G))$.

Our next goal is to show that $k((G))$ with the convolution multiplication is a field. We give two proofs:

(1) Follows from "Neumann's lemma" (now)
(2) From S. Prieß-Crampe: $k((G))$ is pseudo-complete (later)

Lemma 1.6. *(Neumann's lemma)*
Let $\varepsilon \in k((G))$ *such that* $\operatorname{support} \varepsilon \subseteq G^{>0}$ (written $\varepsilon \in k((G^{>0}))$) *and* $\{c_n\}_{n\in\mathbb{N}} \subset k^*$. *Then the family* $\mathfrak{F} = \{c_n \varepsilon^n : n \in \mathbb{N}\}$ *is summable, i.e.* $\sum\limits_{n\in\mathbb{N}} c_n \varepsilon^n \in k((G))$.

Corollary 1.7. $k((G))$ *is a field.*

Proof. Let $s \in k((G)), s \neq 0$. Set $g_0 := \min \operatorname{support} s$ and $c_0 = s(g_0) \neq 0$. Write

$$s = c_0 t^{g_0}(1 - \varepsilon),$$

where

$$\varepsilon = - \sum_{\substack{g>g_0 \\ g \in \operatorname{support} s}} \frac{s(g)}{c_0} t^{g-g_0} \in k((G^{>0})),$$

so

$$s^{-1} := c_0^{-1} t^{-g_0} \left(\sum_{i=0}^{\infty} \varepsilon^i \right).$$

Verify that

$$\left(\sum_{i=0}^{\infty} \varepsilon^i \right)(1 - \varepsilon) = 1,$$

i.e.

$$(1 - \varepsilon)^{-1} = \sum_{i=0}^{\infty} \varepsilon^i.$$

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (12: 21/05/15 - CORRECTED ON 27/05/2019)

SALMA KUHLMANN

Contents

1. Proof of Neumann's lemma

The aim of today's lecture is to prove Neumann's lemma. By what was shown last time, we then obtain that $k((G))$ is indeed a field.

Proposition 1.1. *Set* $S_n := \operatorname{support} \varepsilon^n$ *and* $S := \bigcup_{n \in \mathbb{N}} S_n$. *Then* S *is a well-ordered set.*

Remark 1.2. *Note that* $\operatorname{support} \varepsilon^n \subseteq \operatorname{support} \varepsilon \oplus \ldots \oplus \operatorname{support} \varepsilon$ *(n-times). Thus,* S_n *is well-ordered for any* $n \in \mathbb{N}$.

Proof. (of the proposition)
We argue by contradiction. Let $(u_i : i \in \mathbb{N}) \subseteq S$ be an infinite strictly decreasing sequence. We write

$$u_i = a_{i_1} + \ldots + a_{i_{n_i}},$$

where $a_{i_j} \in S_1 \subset G^{>0}$ $\forall j = 1, \ldots, u_i$. Let v_G denote the natural valuation on G.

ÜB: $\operatorname{sign}(g_1) = \operatorname{sign}(g_2) \Rightarrow v_G(g_1 + g_2) = \min\{v_G(g_1), v_G(g_2)\}$.

Note that $v_G(u_i) = \min\{v_G(a_{i_j})\} \underbrace{=}_{\text{wlog}} v_G(a_{i_1})$. Thus, $v_G(S_u) = v_G(S_1)$. Now recall that

$$0 < g_1 < g_2 \Rightarrow v_G(g_1) \geqslant v_G(g_2).$$

Since $v_G(S_1)$ is anti well-ordered and since $(v_G(u_i) : i \in \mathbb{N}) \subset v_G(S_1)$ is an increasing sequence, it must stabilize after finitely many terms. We assume without loss of generality that it is constant and denote this constant by $U \in v_G(G \backslash \{0\})$, without loss of generality U is as large as possible. So for every $i \in \mathbb{N}$ consider $v_G(u_i) = U = v_G(a_{i_1})$. Let a^* be the smallest element in S_1 for which $v_G(a^*) = U$.

We have that $v_G(u_1) = U = v_G(a^*)$, so $0 < u_1 \leqslant ra^*$ for some $r \in \mathbb{N}$. Fix r. Then $u_i \leqslant ra^*$ $\forall i \in \mathbb{N}$. Since S_1 is well-ordered, it does not contain any infinite decreasing sequence, so we may without loss of generality assume that $n_i > 1\ \forall i \in \mathbb{N}$. We write $u_i = a_{i_1} + v_i$, where $v_i \in S_{n_i - 1}$ and $v_i \neq 0\ \forall i$.

Claim: There is a subsequence $(v_{i_k})_k$ of $(v_i)_i$, which is strictly decreasing.

Let us construct this subsequence. Note that the set $\{u_i - v_i : i \in \mathbb{N}\}$ is well-ordered. Proceed as follows:
Let $u_{i_1} - v_{i_1} = \min\{u_i - v_i\}$, let $u_{i_2} - v_{i_2}$ be the smallest element of the set $\{u_i - v_i : i > i_1\}$ etc., so $(u_{i_k} - v_{i_k})_k$ is an increasing sequence, i.e. $u_{i_{k+1}} - v_{i_{k+1}} \geqslant u_{i_k} - v_{i_k}$, so

$$v_{i_{k+1}} - v_{i_k} \leqslant u_{i_{k+1}} - u_{i_k}.$$

Therefore, $(v_{i_k})_k$ is strictly decreasing in S, and this proves the claim.

Now note that $0 < v_i < u_i\ \forall i$. Therefore, $v_G(v_i) \geqslant v_G(u_i) = U$, i.e. $v_G(v_{i_k}) = U\ \forall k$ (recall that U was as large as possible).
But now $a^* \leqslant a_{i_1}$ and $u_i \leqslant ra^*$. Hence,

$$v_i = (u_i - a_{i_1}) \leqslant (r-1)a^*\ \forall i,$$

in particular for all i_k, so $v_{i_k} \leqslant (r-1)a^*\ \forall k$ and $(v_{i_k})_k$ is strictly decreasing with $v_G(v_{i_k}) = U\ \forall k$.

Repeat the argument with the sequence $\{v_{i_k}\} \subset S \subset G^{>0}$ to eventually get a sequence $\leqslant (r-l)a^* < 0$, the desired contradiction.

□

Proposition 1.3. $\forall g \in S : |\{n \in \mathbb{N} : g \in S_n\}| < \infty$.

Proof. Assume $\exists a \in S$ such that $|\{n \in \mathbb{N} : a \in S_n\}| = \infty$. Since S is well-ordered, we may choose a to be the smallest such element of S. Write

$$a = a^j_{i_1} + \ldots + a^j_{i_{n_j}} \in S_{n_j} \quad (*)$$

where n_j is strictly increasing in $\mathbb{N}$ and $a^j_{i_k} \in S_1$. So $\{a^j_{i_1} : j \in \mathbb{N}\} \subseteq S_1$ is well-ordered. Thus, this set has an infinite increasing sequence, assume without loss of generality that $(a^j_{i_1} | j \in \mathbb{N})$ is increasing.

Denote by $a'_j := a^j_{i_2} + \ldots + a^j_{i_{n_i}} \in S_{n_j - 1}$, so $a'_j < a\ \forall i \in \mathbb{N}$. Since $(*)$ is constant and $(a_{i_1} | i \in \mathbb{N})$ is increasing, we obtain that $\{a'_j : j \in \mathbb{N}\}$ is decreasing and contained in S. Therefore it stabilizes, i.e. becomes ultimately constant. Denote this constant by $a'_j := a'\ \forall j >> N$. So $a' \in S_{n_j - 1}$, and therefore

$$\left|\{n \in \mathbb{N} : a' \in S_n\}\right| = \infty\ \forall j >> N,$$

and $a' < a$ because $a' = a'_j < a\ \forall j >> N$, contradicting the minimality of a.
□

The two propositions finish the proof of Neumann's lemma.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (13: 28/05/15 - CORRECTED ON 03/06/19)

SALMA KUHLMANN

Contents

1. The field of generalized power series

In order to prove that $k((G))$ is a field, we have seen that it suffices to find a multiplicative inverse for $f \in k((G))$ of the form $f = 1 + s$, where $v(s) > 0$, i.e. support $s \subset G^{>0}$. We already constructed $(1+s)^{-1}$ via the expansion which gives a summable series by Neumann's lemma.

Today we give an alternative proof by S. Prieß-Crampe, which capitalizes on the fact that $k((G))$ is pseudo-complete.

Proof. Let $v := v_{\min}$ be the canonical valuation on the Hahn product $k((G))$; that is $v(f) = \min \operatorname{support} f$ for $f \neq 0,\ f \in k((G))$. It is enough, as noted, to find an inverse for $f = 1 + s,\ s \neq 0$ with $v(s) > 0$. Note that $v(f) = 0$ and $f(0) = 1$. Denote $\mathbb{K} := k((G))$ and consider the set

$$\Sigma := \{v(1 - fy) : y \in \mathbb{K} \text{ and } 1 - fy \neq 0\}.$$

Note that $\Sigma \neq \emptyset$.

Case 1: Σ has a largest element α. Let $\tilde{y} \in \mathbb{K}$ be such that $v(1 - f\tilde{y}) = \alpha$. Set $z := 1 - f\tilde{y}$ and $\hat{y} := \tilde{y} + z(\alpha)t^\alpha$. Compute

$$\begin{aligned} v(1 - f\hat{y}) &= v(1 - f\tilde{y} - fz(\alpha)t^\alpha) \\ &\geqslant \min\{v(1 - f\tilde{y}), v(fz(\alpha)t^\alpha)\} = \alpha. \end{aligned}$$

On the other hand

$$\begin{aligned} (1 - f\hat{y})(\alpha) &= (1 - f\tilde{y})(\alpha) - (fz(\alpha)t^\alpha)(\alpha) \\ &= z(\alpha) - z(\alpha) \\ &= 0. \end{aligned}$$

Thus $v(1 - f\hat{y}) > \alpha$, a contradiction to the maximal choice of α, unless $1 - f\hat{y} = 0$, so $1 = f\hat{y}$ and therefore $\hat{y} = f^{-1}$.

(**Recall:** In chapter 1 we have shown that $\mathbb{K}$ is pseudo-complete, or equivalently, maximally valued).

Case 2: Σ has no largest element. Thus, there is a strictly increasing sequence $\{\pi_\rho\}_{\rho<\sigma}$ of Σ where σ is a limit ordinal and $\{\pi_\rho\}_{\rho<\sigma}$ is cofinal in Σ.
For every $\rho < \sigma$ choose $y_\rho \in \mathbb{K}$ such that $v(1-fy_\rho) = \pi_\rho$. Now for $\mu < \nu < \sigma$ we have $\pi_\mu < \pi_\nu$. We claim that $\{y_\rho\}_{\rho<\sigma}$ is pseudo-Cauchy. Indeed

$$\begin{aligned} v(y_\mu - y_\nu) &= v(1 - fy_\mu + fy_\nu - 1) \\ &= \min\{\pi_\mu, \pi_\nu\} = \pi_\mu. \end{aligned}$$

So the sequence is indeed pseudo-Cauchy. Now since $\mathbb{K}$ is pseudo-complete let y^* be a pseudo-limit of $\{y_\rho\}_{\rho<\sigma}$, i.e. $v(y^* - y_\rho) = \pi_\rho$ for all $\rho < \sigma$. Assume that $1 - fy^* \neq 0$. Then $\tau := v(1 - fy^*) \in \Sigma$. By cofinality of $\{\pi_\rho\}_{\rho<\sigma}$ there is a ρ large enough such that $\tau < \pi_\rho$. On the other hand

$$\begin{aligned} \tau = v(1 - fy^*) &= v(1 - fy_\rho + fy_\rho - fy^*) \\ &\geqslant \min\{v(1 - fy_\rho), v(fy_\rho - fy^*)\} \\ &\geqslant \pi_\rho, \end{aligned}$$

a contradiction.

□

Remark 1.1.

(*i*) We have used the fact that for $0 \neq s, r \in \mathbb{K}$, we have

$$v_{\min}(sr) = v_{\min}(s) + v_{\min}(r).$$

This follows immediately from the definition of multiplication of series in the convolution product.

(*ii*) Note that here the pseudo-limit y^* turns out to be unique. We can conclude that the breadth of $\{\pi_\rho\}_{\rho<\sigma}$ is $\{0\}$.

In conclusion, for $k \subseteq \mathbb{R}$ an Archimedean field and G any non-trivial ordered abelian group, the field $\mathbb{K} = k((G))$ endowed with $<_{\text{lex}}$ is a totally ordered non-Archimedean field. Its natural valuation is $v_{\min}$, its value group is G and its residue field k. Note that in general $k((G))$ needs not to be a real closed field.

In the next lectures we will give necessary and sufficient conditions on k and G such that $\mathbb{K} = k((G))$ is a real closed field.

2. Hardy fields

Definition 2.1. Consider the set of all real valued functions defined on positive real half lines:

$$\mathcal{F} := \{f \mid f\colon [a, \infty) \to \mathbb{R} \text{ or } f\colon (a, \infty) \to \mathbb{R},\ a \in \mathbb{R} \cup \{-\infty\}\}.$$

Define an equivalence relation on $\mathcal{F}$ by

$$f \sim g \;\Leftrightarrow\; \exists\, N \in \mathbb{N} \text{ s.t. } f(x) = g(x)\ \forall\, x \geqslant N.$$

Let $[f]$ denote the equivalence class of f, also called the "germ of f at ∞". We identify $f \in \mathcal{F}$ with its germ $[f]$.

We denote by $\mathcal{G} := \mathcal{F}/\sim$ the set of all germs. Note that $\mathcal{G}$ is a commutative ring with 1 by defining

$$[f] + [g] := [f + g]$$
$$[f] \cdot [g] := [f \cdot g]$$

Note that $\mathcal{G}$ is not a field. For example $[\sin x]$ is not invertible.

Definition 2.2. A subring H of $\mathcal{G}$ is a **Hardy field** if it is a field with respect to the operations above and if it is closed under differentiation of germs, i.e. $\forall f \in H : f' \in H$ exists and is well-defined ultimately (i.e. for all $x > N \in \mathbb{N}$).

Remark 2.3. (defining a total order on a Hardy field).
Let H be a Hardy field and $f \in H$, $f \neq 0$. Since $1/f \in H$, $f(x) \neq 0$ ultimately. Moreover since $f' \in H$, f is ultimately differentiable and thus ultimately continuous. Therefore, by the Intermediate Value Theorem, the sign of f is ultimately constant and non-zero (i.e. f is strictly positive on some interval (N, ∞) or f is strictly negative on some interval (N, ∞)).
Thus we can define

$$f > 0 \text{ if ult sign } f = 1,$$

respectively

$$f < 0 \text{ if ult sign } f = -1.$$

Verify that $(H, <)$ is a totally ordered field.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (14: 01/06/15 - CORRECTED ON 03/06/19)

SALMA KUHLMANN

Contents

1. Hardy fields

Today we want to define the canonical valuation on a Hardy field H. For this purpose we observe:

Remark 1.1. (Monotonicity of germs)
Let H be a Hardy field and $f \in H$, $f' \neq 0$. Since $f' \in H$ is ultimately strictly positive or negative, it follows that f is ultimately strictly increasing or decreasing. Therefore

$$\lim_{x \to +\infty} f(x) \in \mathbb{R} \cup \{-\infty, \infty\}$$

exists.

Example 1.2.

(*i*) $\mathbb{R}$ and $\mathbb{Q}$ are Archimedean Hardy fields (constant germs)

(*ii*) Consider the set of germs of real rational functions with coefficients in $\mathbb{R}$ (multivariate). By abuse of denation denote it by $\mathbb{R}(X)$. Verify that this is a Hardy field.
Note that with respect to the order defined on a Hardy field, this is a non-Archimedean field, because the function X is ultimately $> N$ for all $N \in \mathbb{N}$.

2. The natural valuation of a Hardy field

Definition 2.1. (The canonical valuation on a Hardy field H).
Let H be a Hardy field. Define for $0 \neq f, g \in H$

$$f \sim g \;\Leftrightarrow\; \lim_{x \to \infty} \frac{f(x)}{g(x)} = r \in \mathbb{R} \setminus \{0\}.$$

This is an equivalence relation, called **asymptotic equivalence relation**. Denote the equivalence class of $0 \neq f$ by $v(f)$. Define

$$v(0) := \infty \text{ and } v(f) + v(g) := v(fg),$$

Moreover, define an order on the set $\{v(f) : f \in H\}$ by setting

$$\infty = v(0) > v(f) \text{ for } f \neq 0.$$

and

$$v(f) > v(g) \Leftrightarrow \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Verify that $(v(H), +, <)$ is a totally ordered abelian group.

Lemma 2.2. *The map*

$$\begin{array}{rcl} v : H & \longrightarrow & v(H) \cup \{\infty\} \\ 0 \neq f & \mapsto & v(f) \\ 0 & \mapsto & \infty \end{array}$$

is a valuation and it is equivalent to the natural valuation.

Remark 2.3.

$$R_v = \{f : \lim_{x\to\infty} f(x) \in \mathbb{R}\}.$$

$$I_v = \{f : \lim_{x\to\infty} f(x) = 0\}.$$

$$\mathcal{U}_v = \{f : \lim_{x\to\infty} f(x) \in \mathbb{R}^{\times}\}.$$

3. Construction of non-Archimedean real closed fields

Our next goal is to prove the following:

Theorem 3.1. *(Main Theorem of chapter 2)*
Let $k \subseteq \mathbb{R}$ be a subfield, G a totally ordered abelian group and $\mathbb{K} := k((G))$. Then $\mathbb{K}$ is a real closed field if and only if

(i) G is divisible,

(ii) k is a real closed field.

Remark 3.2. Once the Main Theorem is proved we can proceed as follows (starting from $\mathbb{R}$) to construct non-Archimedean real closed fields:

(1) Let $\emptyset \neq \Gamma$ be a totally ordered set.

(2) Choose divisible subgroups of $(\mathbb{R}, +, 0, <)$, say $\{B_\gamma : \gamma \in \Gamma\}$ (note that $\mathbb{R}$ is a $\mathbb{Q}$-vector space).

(3) Take $\coprod_{\gamma\in\Gamma} B_\gamma \subset G \subset \mathrm{H}_{\gamma\in\Gamma} B_\gamma$. Note that G is a divisible ordered abelian group.

(4) Take $k \subset \mathbb{R}$ a subfield and consider $k^{\mathrm{rc}} = \{\alpha \in \mathbb{R} : \alpha \text{ alg. over } k\}$. Then $k^{\mathrm{rc}} \subset \mathbb{R}$ is a real closed field (because $\mathbb{R}$ is real closed).

(5) Set $\mathbb{K} = k^{\mathrm{rc}}((G))$.

In the next chapters, we will show "Kaplansky's embedding theorem": any real closed field is a subfield of such a $\mathbb{K}$.

4. Towards the proof of the Main Theorem

Let $k \subset \mathbb{R}$ and G be an ordered abelian group.

Proposition 4.1. *Set $\mathbb{K} = k((G))$ and $v = v_{\min}$. If $\mathbb{K}$ is real closed, then G is divisible and k is a real closed field.*

Proof. We first prove that G is divisible. So let $g \in G$ and $n \in \mathbb{N}$. We have to show that $\frac{g}{n} \in G$. Assume without loss of generality $g > 0$. Consider $\mathbb{K} \ni s = t^g > 0$ in the lex order on $\mathbb{K}$.

(Note that a real closed field R is "root closed for positive elements": For some $s > 0$ consider $x^n - s$. Then $0^n - s < 0$ and $(s+1)^n - s > 0$. The Intermediate Value Theorem gives a root in the interval $]0, s+1[$).

Since $\mathbb{K}$ is real closed take $y = \sqrt[n]{s} \in \mathbb{K}$. Then $v(s) = g$ and thus $v(y) = \frac{g}{n} \in G$.

To show that k is a real closed field let $n \in \mathbb{N}$ be odd and consider some polynomial
$$x^n + c_{n-1}x^{n-1} + \ldots + c_0 \in k[X] \subseteq \mathbb{K}[X].$$
Since $\mathbb{K}$ is real closed, we find some $x \in \mathbb{K}$ such that x is a root of this polynomial, i.e.
$$x^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0.$$
Note that the residue field of $\mathbb{K}$ is k and the residue map is a homomorphism. We want to compute $\bar{c}$ for $c \in k$. Note that $s = c = ct^0 \in k$ so $v_{\min}(c) = 0$ and $\bar{c} = c$. So the residue map is just the identity on k. It remains to show that $v(x) \geqslant 0$. Assume $v(x) < 0$. Then
$$v(x^n + \ldots + c_0) = v(0) = \infty,$$
a contradiction.

$\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (15: 08/06/15 - CORRECTED ON 06/06/19)

SALMA KUHLMANN

Contents

1. The Main Theorem

In the previous lecture we introduced the "Main Theorem" of this chapter.

Theorem 1.1. *Let $k \subseteq \mathbb{R}$ be a subfield, G a totally ordered abelian group and $\mathbb{K} := k((G))$. Then $\mathbb{K}$ is a real closed field if and only if*

(*i*) *G is divisible,*

(*ii*) *k is a real closed field.*

Last time we already proved the implication "$\Rightarrow$". For the converse we need some notions and preliminary results.

2. The divisible hull

Proposition 2.1.

(*i*) *Let $(G, +)$ be a torsion free abelian group. Then there exists a unique (up to isomorphism of groups) minimal divisible group $(\tilde{G}, +)$ that contains $(G, +)$.*
$(\tilde{G}, +)$ is called the ***divisible hull*** *of G.*

(*ii*) *If $H \leqslant G$, then $\tilde{H} \leqslant \tilde{G}$.*

(*iii*) *If G is a totally ordered abelian group (particularly torsion free), then the order on G extends uniquely to an order on $\tilde{G}$. Therefore the ordered divisible hull $(\tilde{G}, <)$ of $(G, <)$ is unique up to an order preserving isomorphism.*

Proof. (*i*) Consider the set $\{(x, n) : x \in G, n \in \mathbb{N}\}$ under the equivalence relation

$$(x, n) \sim (y, m) :\Leftrightarrow mx = ny,$$

i.e. set

$$\tilde{G} := \{(x,n) : x \in G, n \in \mathbb{N}\} \,/\, \sim .$$

Define an addition on $\tilde{G}$ by $(x,n)\tilde{+}(y,m) := (mx+ny, mn)$.

Verify that (ÜA)
- $\tilde{+}$ is well-defined and $(\tilde{G}, \tilde{+})$ is a torsion free abelian group.
- the map $g \mapsto (g,1)$ defines an embedding of G in $\tilde{G}$.
- $(\tilde{G}, \tilde{+})$ is divisible.
- if $G^* \supseteq G$ is a group extension and G^* is divisible and torsion free, then

  $$\mathbb{Q}G := \{qx : q \in \mathbb{Q}, x \in G\}$$

  is a minimal divisible subgroup of G^* containing G. Moreover, the map $(a,n) \mapsto \frac{1}{n}a$ is an isomorphism of groups $\tilde{G} \to \mathbb{Q}G$.

(*ii*) Straight forward by construction as in (*i*) (ÜA).

(*iii*) Declare $(x,n) \in \tilde{G}$ to be positive if and only if $x \in G$ is positive. Verify that the map $G \to \tilde{G}$, $a \mapsto (a,1)$ is order preserving.

□

Remark 2.2. *G is divisible if and only if $G = \tilde{G}$.*

Proposition 2.3. *(Generalized ultrametric inequality)*

(*i*) $v(a) \neq v(b) \Rightarrow v(a+b) = \min\{v(a), v(b)\}$.

(*ii*) $v(\sum a_i) \geqslant \min\{v(a_i)\}$.

(*iii*) *If there exists a unique index $i_0 \in \{1, \ldots, n\}$ such that $v(a_{i_0}) = \min\{v(a_i) : i = 1, \ldots, n\}$, then $v(\sum a_i) = \min\{v(a_i)\}$.*

Proposition 2.4. *Let (L,v) be a valued field and $K \subseteq L$ be a subfield such that $L|K$ is algebraic. Then $v(L)$ is contained in the divisible hull of $v(K)$.*

Proof. Let $\alpha \in v(L) \backslash v(K)$ and let $l \in L$ be such that $\alpha = v(l)$. Since L is algebraic over K, l satisfies

$$\sum_{i=0}^{n} a_i l^i = 0$$

for some $a_i \in K$ with $0 \neq a_n$. Applying v on both sides yields

$$v\left(\sum_{i=0}^{n} a_i l^i\right) = \infty = v(0).$$

Thus, there must be two indices $i, j \in \{0, \ldots, n\}$ with $i < j$ such that $\infty \neq v(a_j l^j) = v(a_i l^i)$. In other words

$$v(a_j) + jv(l) = v(a_i) + iv(l)$$

i.e.

$$(j-i)v(l) = v(a_i) - v(a_j) \in v(K)$$

and therefore

$$\alpha = \frac{v(a_i) - v(a_j)}{j-i} \in v(\tilde{K}).$$

□

3. Algebraically closed fields

In this section we prove the Main Theorem for algebraically closed fields. We conclude by showing that this transfers to real closed fields by applying the Theorem of Artin-Schreier (see RAG I).

Proposition 3.1. *Let (L, v) be a valued field and $K \subset L$ a subfield such that $L|K$ is algebraic. Then the residue field $\overline{L}$ is contained in an algebraic closure of the residue field $\overline{K}$.*

Proof. Let $0 \neq \overline{z} \in \overline{L}$ and $0 \neq z \in L$ be a preimage of $\overline{z}$ in L. Now L is algebraic over K, so z satisfies a polynomial equation

$$a_n z^n + \ldots + a_0 = 0 \quad (a_i \in K, a_n \neq 0).$$

Set $v(a_j) = \min\{v(a_i) : i = 0, \ldots, n\}$ and $b_i := \frac{a_i}{a_j}$ for $i = 0, \ldots, n$. Then $b_j = 1$ and $v(b_i) \geqslant 0$ for $i = 0, \ldots, n$. Therefore

$$0 \neq b_n X^n + \ldots + b_0 \in K_v[X]$$

and

$$b_n z^n + \ldots + b_0 = 0,$$

where K_v denotes the valuation ring of K. Thus $\overline{z}$ is a root of the non-zero polynomial $0 \neq \sum_{i=0}^n \overline{b_i} X^i \in \overline{K}[X]$, i.e. $\overline{z}$ is algebraic over $\overline{K}$. □

Theorem 3.2. *(algebraically closed fields of generalized power series, Mac Lane, 1939)*
Set $\mathbb{K} := k((G))$ for some field k and some ordered abelian group G. Then $\mathbb{K}$ is algebraically closed if and only if

(i) *G is divisible,*

(ii) *k is an algebraically closed field.*

Proof. "⇒" is analogue to the proof for the real closed field case seen last lecture (ÜA). Let us prove "⇐". So we want to show that $\mathbb{K}$ is algebraically closed.

Claim: Every algebraic extension L of $\mathbb{K}$ is immediate.

(Since $\mathbb{K}$ is maximally valued, as was shown in lectures $6-8$, $\mathbb{K}$ will then admit no proper algebraic extensions at all, i.e. is algebraically closed)

Proof of the claim: Since $L|\mathbb{K}$ is algebraic we know by Proposition 2.4 that

$$v(L) \subseteq v(\mathbb{K}) = \tilde{G} = G.$$

On the other hand, since (L, v) is a valued extension of $(\mathbb{K}, v)$, we have $v(L) \supseteq v(\mathbb{K}) = G$, so we get $v(L) = v(\mathbb{K})$.
Similarly we show that $\overline{L} = \overline{\mathbb{K}} = k$. By Proposition 3.1 $\overline{L}$ is contained in the algebraic closure of k, but $\overline{k} = k$. So $\overline{L} \subseteq \overline{k} = k$. On the other hand, since (L, v) is a valued field extension of $(\mathbb{K}, v)$, we have $\overline{L} \supseteq \overline{\mathbb{K}} = k$, so again $\overline{L} = k$. Hence the valued field extension $(L, v)|(\mathbb{K}, v)$ is immediate. □

Remark 3.3. *What is meant in the claim is the following: $(\mathbb{K}, v)$ is a valued field and $L|\mathbb{K}$ a field extension, extending the valuation v on $\mathbb{K}$ to a valuation v on L. After that we mean (L, v) is an immediate extension of $(\mathbb{K}, v)$.*

4. Finishing the proof of the Main Theorem

Proposition 4.1. *Let k be a field, G an ordered abelian group and $i = \sqrt{-1}$. Then $k((G))(i) \cong k(i)((G))$.*

Proof. ÜA. □

Theorem 4.2. *(real closed fields of power series)*
$k((G))$ is a real closed field if and only if k is a real closed field and G is divisible.

Proof. It remains to prove "$\Leftarrow$". Since k is real closed, $k(i)$ is algebraically closed (Artin-Schreier). So $k(i)((G))$ is algebraically closed by Mac Lane. But then $k((G))(i)$ is also algebraically closed. By Artin-Schreier $k((G))$ is a real closed field. □

Example 4.3. Define $\tilde{\mathbb{Q}}^{\mathrm{rc}}$:= the field of all real algebraic numbers. Then $\mathbb{K} = \tilde{\mathbb{Q}}^{\mathrm{rc}}((\mathbb{Q}))$ is a real closed field. Note that $\mathbb{K}$ is not countable.

Question: Are there countable non-Archimedean real closed fields?

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (16: 11/06/15 - CORRECTED ON 14/06/2019)

SALMA KUHLMANN

Contents

1. Real closed fields of power series

Notation 1.1. For $\mathbb{K} = k((G))$ let $k(G)$ denote the subfield of $\mathbb{K}$ generated by $k \cup \{t^g : g \in G\}$.

Theorem 1.2. *Let K be a real closed field, v its natural valuation, $G = v(K^\times)$ its value group, $\overline{K}$ its residue field. Then K is order isomorphic to a subfield $i(K)$ such that*

$$\overline{K}(G)^{\mathrm{rc}} \subseteq i(K) \subseteq \overline{K}((G)).$$

Remark 1.3. We denote by $k(G)^{\mathrm{rc}}$ the relative algebraic closure of $k(G)$ in $\mathbb{K}$. Note that if $\mathbb{K}$ is real closed, then $k(G)^{\mathrm{rc}}$ is (isomorphic to) the real closure of $k(G)$ (i.e. K is "sandwiched" between two real closed fields of power series).

Remark 1.4. Note about $k(G)$:

(*i*) Consider all series in $\mathbb{K}$ which have finite support and denote it by $k[G] := \{s \in \mathbb{K} : \text{support}(s) \text{ is finite}\}$.

ÜB: $k[G]$ is a subring of $\mathbb{K}$, so it is a domain, called the **group ring** over k and the group G.

Excurs about $k[G]$: Let $s \in k[G]$, $\text{support}(s) = \{g_1, \ldots, g_r\}, r \in \mathbb{N}$, i.e. there are coefficients $c_1, \ldots, c_r \in k$ such that $s = c_1 t^{g_1} + \ldots + c_r t^{g_r}$, so the group ring $k[G]$ can be viewed as the ring of "polynomials" with coefficients in k and variables in $\{t^g : g \in G\}$.
Example: If $G = \mathbb{Z}$, say $k = \mathbb{R}$ or $k = \mathbb{C}$, then $k[G]$ is called the **ring of Laurent polynomials**.

(*ii*) $k(G) = \text{ff}(k[G]) = k(t^g : g \in G)$.

2. Embedding of the value group

The aim of this section is to prove that the value group of a real closed field K under its natural valuation can be embedded into the multiplicative subgroup $(K^{>0}, \cdot, 1, <)$.

Proposition 2.1. *Let K be an ordered field and $G = v(K^\times)$, where v denotes the natural valuation.*

- (i) *the map*

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

is a surjective homomorphism of ordered groups with kernel

$$U_v^{>0} = \{a \in K_v : a > 0, v(a) = 0\}.$$

So $U_v^{>0}$ is a convex subgroup of $(K^{>0}, \cdot, 1, <)$ and $K^{>0}/U_v^{>0} \cong G$.

- (ii) *if moreover $K^{>0}$ is divisible (in particular this is the case if K is real closed), then $(K^{>0}, \cdot, 1, <) = B \cdot U_v^{>0}$, where B is a multiplicative subgroup of $(K^{>0}, \cdot, 1)$ and is order-isomorphic to G.*

Remark 2.2. Here we are considering $(K^{>0}, \cdot, 1, <)$ as a $\mathbb{Q}$-vector space as follows:

- (i) $(K^{>0}, \cdot, 1, <)$ is an ordered abelian group.
- (ii) Define the scalar map $\mathbb{Q} \times K^{>0} \to K^{>0}$, $(q, a) \mapsto a^q$.
  Note that $U_v^{>0}$ is also divisible. Use the Theorem from LA1 about existence and uniqueness up to isomorphism of a complement to a subspace in a vector space.

Proof. (of the proposition)

- (i) Note that

$$\nu(ab) = -v(ab) = -v(a) - v(b) = \nu(a) + \nu(b).$$

To show surjectivity let $g \in G$ and choose $a > 0$, $a \in K$, such that $-v(a) = g$ (then $\nu(a) = g$).
Order-preserving: Let $a \geqslant 1$. Show $\nu(a) \geqslant 0$, i.e. $-v(a) \geqslant 0$ or $v(a) \leqslant v(1)$ (via Archimedean equivalence classes).
Compute kernel:

$$a \in \ker \nu \Leftrightarrow \nu(a) = 0 \Leftrightarrow -v(a) = 0 \Leftrightarrow v(a) = 0 \Leftrightarrow a \in U_v^{>0},$$

since $a \in K^{>0}$.

□

Corollary 2.3. *If K is a totally ordered field such that $(K^{>0}, \cdot, 1)$ is divisible (in particular if K is real closed), then there exists an order preserving embedding of $v(K^\times)$ into $(K^{>0}, \cdot, 1, <)$.*

3. Embedding of the residue field

In this section we prove that the residue field of a real closed field K, with respect to the natural valuation, embedds in K.

Proposition 3.1. *Let K be a real closed field. Then there exists a subfield of K which is order-isomorphic to the residue field $\overline{K}$ of K with respect to the natural valuation (i.e. the residue field embedds in K).*

Proof. We want to apply Zorn's lemma to the collection Θ of all Archimedean subfields of K, which is partially ordered under inclusion. Note that $\mathbb{Q}$ is Archimedean, i.e. Θ is non-empty. Now let $\mathcal{C} \subseteq \Theta$ be a totally ordered subset. We need to find an upper bound in Θ. Set $\mathcal{S} = \bigcup \mathcal{C}$ and verify that this is indeed an upper bound.
Let $k \subseteq K$ be a maximal Archimedean subfield. We will show $k \cong \overline{K}$. Note that $k^{\times} \subset U_v$. Consider the residue map $k \to \overline{K}$, $x \mapsto \overline{x}$. This is an injective homomorphism. We claim that it is also surjective.
First of all note that k is real closed. This is because the real closure of an Archimedean field is Archimedean. Moreover the real closure of a subfield of K_v is a subfield of K_v. Indeed $v(z) = 0$ for any z in the relative algebraic closure of k, because $v(z)$ is in the divisible hull $\widetilde{v(k)} = \{0\}$ of $v(k)$. So the relative algebraic closure of k, if a proper extension, would contradict the maximal choice of k. Note that by Proposition 4.1 lecture 14, also $\overline{k}$ is real closed.
Now assume the residue map is not surjective, i.e. $\exists \overline{y} \in \overline{K} \backslash \overline{k}$. Let $y \in U_v$ denote a preimage of $\overline{y}$. We claim that $k(y) \subseteq U_v$ and that $(k(y)$ is Archimedean. Note that y is transcendental, so $k(y) = ff(k[y])$. Consider $a_n y^n + \ldots + a_0 \in k[y]$. If

$$\overline{a_n y^n + \ldots + a_0} = \overline{a_n}\,\overline{y}^n + \ldots + \overline{a_0} = 0,$$

then $\overline{y}$ would be algebraic over $\overline{k}$.
So any $z \in k(y)$ has $\overline{z} \neq 0$, so $k(y) \subset U_v$ and is Archimedean (because $\forall z \in k(y) : v(z) = 0$, so $z \sim^{+} 1$), contradicting the maximality of k.

$\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (17: 15/06/15 - CORRECTED ON 17/06/2019)

SALMA KUHLMANN

Contents

1. Kaplansky's Embedding Theorem

In the last lecture we showed that

(i) the value group of a real closed field K is isomorphic (as an ordered group) to a subgroup of $(K^{>0}, \cdot, 1, <)$.

(ii) if K is a real closed field, then every maximal Archimedean subfield of K is isomorphic to $\overline{K}$ (with respect to the natural valuation), and there exist such Archimedean subfields (lemma of Zorn). Therefore the residue field $\overline{K}$ is isomorphic to some subfield of K.

(iii) If $k[G]$ is a group ring, then $\mathrm{ff}(k[G]) = k(G) = k(t^g : g \in G)$ is the smallest subfield of $k((G))$ generated by $k \cup \{t^g : g \in G\}$.

Theorem 1.1. *(Kaplansky's "sandwiching" or embedding theorem for rcf) Let K be a real closed field, G its value group and k its residue field. Then there exists a subfield of K isomorphic to $k(G)^{rc}$.*
Moreover, every such isomorphism extends to an embedding of K into $k((G))$,

$$\begin{tikzcd} K \arrow[r, hook, "\mu"] \arrow[d, no head] & k((G)) \arrow[d, no head] \\ l(\mathbb{B})^{\mathrm{rc}} \arrow[r, "\mu_0", "\sim"'] & k(G)^{\mathrm{rc}} \end{tikzcd}$$

i.e. K is isomorphic to a subfield $\mu(K)$ such that $k(G)^{rc} \subseteq \mu(K) \subseteq k((G))$.

Proof. Let $l \subseteq K$ be a subfield isomorphic to k and let $\mathbb{B}$ be a subgroup isomorphic to G. More precisely, $\mathbb{B}$ is a multiplicative subgroup of $(K^{>0}, \cdot, 1, <)$ isomorphic to the multiplicative subgroup $\{t^g : g \in G\}$ of monomials in $k((G))$. Consider the subfield of K generated by $l \cup \mathbb{B}$, i.e. the subfield $l(\mathbb{B})$ and we take its relative algebraic closure in K.
It is clear that $\exists$ isomorphism $\mu_0 : l(\mathbb{B})^{\mathrm{rc}} \to k(G)^{\mathrm{rc}}$.

Claim 1: the extension $l(\mathbb{B})^{\mathrm{rc}} \subseteq K$ is immediate.
This is because the residue field of a real closure equals the real closure of the residue field equals the residue field of K. Also the value group of the real closure is the divisible hull of the value group $= G$. So the extension is value group preserving and residue field preserving. Therefore the extension is immediate.
Now consider the collection of all pairs (M, μ) where M is a real closed subfield of K containing $l(\mathbb{B})^{\mathrm{rc}}$ and $\mu : M \hookrightarrow k((G))$ is an embedding of M extending μ_0. We partially order this collection the obvious way, i.e.

$$(M_1, \mu_1) \leqslant (M_2, \mu_2) :\Leftrightarrow M_1 \subseteq M_2, \mu_{2|M_1} = \mu_1.$$

It is clear that every chain $\mathcal{C}$ in this collection has an upper bound in it, namely $\bigcup \mathcal{C}$. So the hypothesis of Zorn's lemma is verified. Therefore, we find some maximal element (M, μ).

$$\begin{tikzcd} K \arrow[r, "\mu"] \arrow[d, dash, "\text{immediate}"'] & k((G)) \arrow[d, dash] \\ l(\mathbb{B})^{\mathrm{rc}} \arrow[r, "\mu_0", "\sim"'] & k(G)^{\mathrm{rc}} \end{tikzcd}$$

Claim 2: $M = K$.
We argue by contradiction. If this is not the case, let $y \in K \backslash M$. Note that y is transcendental over M. Also since $K \supseteq M$ is immediate, y is a pseudo-limit of a pseudo-Cauchy sequence $\{y_\alpha\}_{\alpha \in S} \subset M$ without a limit in M. Set $z_\alpha := \mu(y_\alpha)$, so $\{z_\alpha\}_{\alpha \in S} \subset k((G))$ is a pseudo-Cauchy sequence and $k((G))$ is pseudo-complete, so choose $z \in k((G))$ a pseudo-limit of $\{z_\alpha\}_{\alpha \in S}$.

Claim 3: z is transcendental over $\mu(M)$.
This is because $z \notin \mu(M)$. Otherwise $\mu^{-1}(z) \in M$ would be a pseudo-limit of $\{y_\alpha\}_{\alpha \in S} = \{\mu^{-1}(z_\alpha)\}_{\alpha \in S}$ in M, a contradiction.
Therefore $M(y) \cong \mu(M)(z)$ as fields and $M(y)^{\mathrm{rc}} \cong \mu(M)(z)^{\mathrm{rc}}$, contradicting the maximality of (M, μ).

□

Chapter III: Convex valuations on ordered fields:

2. Convex valuations

Let K be a non-Archimedean ordered field. Let v be its non-trivial natural valuation with valuation ring K_v and valuation ideal I_v.

Definition 2.1. Let w be a valuation on K. We say that w **is compatible with the order** (or **convex**) if $\forall\, a, b \in K$

$$0 < a \leqslant b \;\Rightarrow\; w(a) \geqslant w(b).$$

Example 2.2. We have seen that the natural valuation is compatible with the order. Moreover, K_v is convex.

Proposition 2.3. *(Characterization of compatible valuations).*
The following are equivalent:

(1) *w is compatible with the order of K.*

(2) *K_w is convex.*

(3) *I_w is convex.*

(4) *$I_w < 1$.*

(5) $1 + I_w \subseteq K^{>0}$.

(6) *The residue map*
$$K_w \to Kw,\; a \mapsto a + I_w$$
induces an ordering on Kw given by
$$a + I_w \geqslant 0 \;:\Leftrightarrow\; a \geqslant 0.$$

(7) *The group*
$$\mathcal{U}_w^{>0} := \{a \in K : w(a) = 0 \;\wedge\; a > 0\}$$
of positive units is a convex subgroup of $(K^{>0}, \cdot, 1, <)$.

Proof. (1) $\Rightarrow$ (2). $0 < a \leqslant b \in K_w \Rightarrow w(a) \geqslant w(b) \geqslant 0 \Rightarrow a \in K_w$.

(2) $\Rightarrow$ (3). Let $a, b \in K$ with $0 < a < b \in I_w$. Since $w(b) > 0$, it follows that $w(b^{-1}) = -w(b) < 0$ and then $b^{-1} \notin K_w$.
Therefore also $a^{-1} \notin K_w$, because $0 < b^{-1} < a^{-1}$ and K_w is convex by assumption. Hence $w(a) > 0$ and $a \in I_w$.

(3) $\Rightarrow$ (4). Otherwise $1 \in I_w$ but $w(1) = 0$, contradiction.

(4) $\Rightarrow$ (5). Clear.

□

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (18: 18/06/15 - CORRECTED ON 28/06/19)

SALMA KUHLMANN

Contents

1. The rank of ordered fields

(Applications later on: the rank of a Hardy-field).

Definition 1.1. Let K be a field and w and w' be valuations on K. We say that w' is **finer** than w or that w is **coarser** than w', if $K_{w'} \subseteq K_w$ (or equivalently $I_w \subseteq I_{w'}$).

Remark 1.2.

(i) An overring of a valuation ring is a valuation ring.

(ii) If w' is a convex valuation and w is coarser than w', then w is a convex valuation.

(iii) We have proved that the natural valuation on an ordered field K induces the smallest (for inclusion) convex valuation ring of K.

(iv) The collection of all convex valuations (respectively valuation rings) of K is totally ordered by inclusion.

Definition 1.3. The **rank** of the totally ordered field K is the (order type of the totally ordered) set

$$\mathcal{R} := \{K_w : K_w \text{ is a convex valuation and } K_v \subsetneq K_w\},$$

where v denotes the natural valuation. Note that

$$\mathcal{R} := \{K_w : w \text{ is strictly coarser than } v\}.$$

Example 1.4.

- The rank of an Archimedean ordered field is empty (since its natural valuation is trivial), its order type 0.

- The rank of the rational function field $K = \mathbb{R}(t)$ with any order is a singleton. Indeed the field $\mathbb{R}(t)$ is non-Archimedean under any order (see RAG I). Moreover, any ordering of $\mathbb{R}(t)$ has rank 1.

2. The Descent

From the ordered field K down to the ordered group $v(K^\times) =: G$.

Let K_w be a convex valuation ring of K. We associate to w the following subset of G :

$$\begin{aligned} G_w : &= \{v(a) : a \in K,\, w(a) = 0\} \\ &= \{v(a) : a \in K^{>0},\, w(a) = 0\} \\ &= v(U_w) = v(U_w^{>0}). \end{aligned}$$

Remark 2.1. Note that w is a coarsening of v if the following holds:

$$v(a) \leqslant v(b) \Rightarrow w(a) \leqslant w(b).$$

Lemma 2.2. *G_w is a convex subgroup of G.*

Proof.

- $0 = v(1)$ and $1 \in U_w$.
- Let $g \in G_w$. Show $-g \in G_w$. Let $a \in U_w$ such that $g = v(a)$. Then $a^{-1} \in U_w$ and
$$G_w \ni v(a^{-1}) = -v(a) = -g.$$
- Similarly assume $g_1, g_2 \in G_w$. There exist $a_1, a_2 \in U_w$ such that $v(a_i) = g_i$. Then $a_1a_2 \in U_w$ and
$$v(a_1a_2) = v(a_1) + v(a_2) = g_1 + g_2 \in G_w.$$
- Let $g \in G_w$ and $0 < h < g$ for some $h \in G$. Show $h \in G_w^{>0}$. Let $g = v(b), b \in U_w$, and $h = v(a)$ for some $a \in K^{>0}$. Then
$$v(a) \leqslant v(b) \Rightarrow w(a) \leqslant w(b) = 0 \Rightarrow w(a) = 0.$$

□

Lemma 2.3. *The value group $w(K^\times)$ is isomorphic (as an ordered group) to $v(K^\times)/G_w$, so*

$$w(K^\times) \cong v(K^\times)/v(U_w).$$

Proof. Consider the map

$$\phi : v(K^\times) \to w(K^\times),\, v(a) \mapsto w(a).$$

Compute

$$\begin{aligned} \ker\phi &= \{v(a) : \phi(v(a)) = 0\} \\ &= \{v(a) : w(a) = 0\} \\ &= G_w, \end{aligned}$$

i.e. ϕ is a surjective homomorphism with kernel G_w, so $w(K^\times) \cong v(K^\times)/G_w$. Moreover this isomorphism is order preserving: note that since G_w is a convex subgroup of $v(K^\times)$, the group $v(K^\times)/G_w$ is totally ordered.

□

Definition 2.4. Given w a coarsening of v, we call $G_w = v(U_w)$ the **convex subgroup of G associated to w.**

Conversely, we get the following result:

Lemma 2.5. *Given any convex subgroup C of G we define a valuation w on K as follows:*

$$w : K^\times \to v(K^\times)/C,\ w(a) = v(a) + C \quad \textit{(the canonical map)}$$

Then w is a convex valuation on K and $G_w = C$.

Proof.

- $v(a) \in G_w \Leftrightarrow w(a) = 0 \Leftrightarrow v(a) \in C$.
- $$\begin{aligned} w(a+b) = v(a+b) + C &\geqslant \min\{v(a) + C, v(b) + C\} \\ &\Leftrightarrow v(a+b) \geqslant \min\{v(a), v(b)\} \\ &\Leftrightarrow w(a+b) \geqslant \min\{w(a), w(b)\}. \end{aligned}$$
- $0 < a \leqslant b \Rightarrow v(a) \geqslant v(b) \Rightarrow v(a) + C \geqslant v(b) + C \Rightarrow w(a) \geqslant w(b)$.
- $$\begin{aligned} w(ab) = v(ab) + C &= (v(a) + v(b)) + C \\ &= (v(a) + C) + (v(b) + C) \\ &= w(a) + w(b). \end{aligned}$$

□

Definition 2.6. w is called the **convex valuation associated to C.**

Let us summarize:

Proposition 2.7. *Suppose that w is coarser than v. Then for all $a, b \in K$:*

$$v(a) \leqslant v(b) \Rightarrow w(a) \leqslant w(b).$$

Let $G_w = v(U_w)$ be the convex subgroup of $v(K^\times)$ associated to w. Then

$$w(K^\times) \cong v(K^\times)/G_w.$$

Conversely every convex subgroup C of $v(K^\times)$ is of the form G_w, where w is the convex valuation associated to C.

Corollary 2.8. *(Descent into the value group)*
The correspondence $K_w \mapsto G_w$ is a one to one (inclusion) order preserving correspondence between the rank of K and the rank of $G = v(K^\times)$.

Example 2.9.

(i) $K = \mathbb{R}((\mathbb{Z}))$ the field of Laurent series ordered lex. Then $\mathcal{R}_K = 1$.

(ii) $K = \mathbb{R}((\mathbb{Q})) \Rightarrow$ rank is 1,

(iii) $K = \mathbb{R}((\mathbb{R})) \Rightarrow$ rank is 1.

(iv) $K = \mathbb{R}((\mathbb{Z} \times \mathbb{Z})) \Rightarrow$ rank is 2.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (19: 22/06/15 - CORRECTED ON 01/07/19)

SALMA KUHLMANN

Contents

1. Final segments

As always, let K be an ordered field and let v denote the natural valuation on K with value group $G := v(K^*)$.

Lemma 1.1. *Let G be a totally ordered abelian group and denote by v_G its natural valuation.*

- (i) *If $G_w \neq \{0\}$ is some convex subgroup of G, then $\Gamma_w := v_G(G_w \backslash \{0\})$ is a non-empty final segment of $\Gamma := v_G(G\backslash\{0\})$*
  (Γ denotes the value set of G)
- (ii) *Conversely, if Γ_w is a non-empty final segment of Γ, then*
  $$G_w := \{g \in G : v_G(g) \in \Gamma_w\} \cup \{0\}$$
  is a convex subgroup of G with $\Gamma_w = v_G(G_w)$.

Proof.

- (i) Clearly Γ_w is non-empty since $G_w \neq \{0\}$. Show Γ_w is a final segment. Let $\gamma \in \Gamma_w$ and $\gamma' \in \Gamma$ such that $\gamma < \gamma'$. We want to show that $\gamma' \in \Gamma_w$.
  Now $\gamma \in \Gamma_w$, so let $g \in G_w$ such that $\gamma = v_G(g)$ and let $g' \in G$ such that $v_G(g') = \gamma'$. Now $\gamma < \gamma'$ means $g' << g$, i.e. $n|g'| \leqslant |g|$. Therefore $g' \in G_w$ since G_w is convex. Thus, $\gamma' \in \Gamma_w$ as required.
- (ii) ÜA.

$\square$

Definition 1.2. Let $\Gamma \neq \emptyset$ be a totally ordered set. Define

$$\Gamma^{\text{fs}} := \{F : F \neq \emptyset \text{ a final segment of } \Gamma\}.$$

Remark 1.3. The set Γ^{fs} is totally ordered by inclusion. Indeed, given $F_1 \neq \emptyset, F_2 \neq \emptyset$ final segments, either $F_1 \subseteq F_2$ or $F_2 \subseteq F_1$ (verify!). So Γ^{fs} is a totally ordered set.

Example 1.4.

- For $\Gamma = \mathbb{R}$, what is the order type of Γ^{fs}?
  A proper non-empty final segment of $\mathbb{R}$ is either of the form $r^+ := [r, \infty)$ or $r^- := (r, \infty)$ for $r \in \mathbb{R}$ (Recall the Dedekind completeness of the reals, see RAG I). Hence,
  $$\Gamma^{\text{fs}} = \{r^{\pm} : r \in \mathbb{R}\} \cup \{\mathbb{R}\}.$$
  Clearly $r^- < r^+$. Let $r_1 \neq r_2$, say $r_1 < r_2$. Then $r_2^- < r_2^+ < r_1^- < r_1^+$, i.e. Γ^{fs} is a double covering of $\mathbb{R}$,
  $$\left(\sum_{\mathbb{R}} 2\right) + 1 = \mathbb{R} \times_{\text{lex}} 2 + 1.$$
- Suppose $\Gamma = \mathbb{Q}$ and $F := \{q \in \mathbb{Q} : q > \sqrt{2}\}$. Let $\emptyset \neq F$ be a proper final segment of $\mathbb{Q}$.
  - $q \in \mathbb{Q}$, then $F = [q, \infty) =: q^+$ and $F = (q, \infty) =: q^-$ in $\mathbb{Q}$.
  - $r \in \mathbb{R} \backslash \mathbb{Q}$, $F = r^{-1} \cap \mathbb{Q} = r^+ \cap \mathbb{Q}$.

  We claim that these are all the proper non-empty final segments.
- $\mathbb{Z}^{\text{fs}} = \mathbb{Z} + \{1\}$.

Corollary 1.5. *There is a 1 to 1 correspondence*
$$G_w \mapsto v_G(G_w \backslash \{0\}) = \Gamma_w$$
between the rank of G and Γ^{fs}, where $\Gamma = v_G(G \backslash \{0\})$.

Corollary 1.6. *There is a bijective correspondence*
$$K_w \mapsto G_w = v(U_w) \mapsto \Gamma_w$$
between the rank of K and Γ^{fs}.

Lemma 1.7. *The map*
$$\iota : \Gamma \to \Gamma^{fs}, \, \gamma \mapsto \gamma^+$$
is an order reversing embedding. Its image consists of those final segments which have a smallest element

Notation 1.8. Let us denote by Γ^* the set Γ endowed with the reverse order.

Corollary 1.9. *The map $\iota : \Gamma^* \hookrightarrow \Gamma^{fs}, \, \gamma \mapsto \gamma^+$ is an order preserving embedding.*

Definition 1.10. A final segment which has a smallest element is called a **principal final segment**.

Corollary 1.11. *Γ^* is isomorphic to the chain of principal final segments of Γ.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (20: 25/06/15 - CORRECTED ON 01/07/19)

SALMA KUHLMANN

Contents

1. Principal final segments

Last lecture we studied the order type of the chain Γ^{fs} of non-empty final segments of the set $\Gamma =: v_G(G\backslash\{0\})$.

Lemma 1.1. *The order type of the chain Γ^{fs} is uniquely determined by the order type of Γ, i.e. if Γ_1 and Γ_2 are chains such that $\phi : \Gamma_1 \cong \Gamma_2$ as ordered sets, then $\Gamma_1^{fs} \cong \Gamma_2^{fs}$ as ordered sets.*

Proof. Define $\phi^{\text{fs}} : \Gamma_1^{\text{fs}} \to \Gamma_2^{\text{fs}}$, $F \mapsto \phi(F)$. Verify (ÜA) that ϕ is injective, i.e.

$$F_1 \subsetneq F_2 \Rightarrow \phi(F_1) \subsetneq \phi(F_2) \quad (*)$$

so the map ϕ^{fs} is injective. Also if $F' \in \Gamma_2^{\text{fs}}$, then $\phi^{-1}(F') \in \Gamma_1^{\text{fs}}$, so $\phi^{\text{fs}}(\phi^{-1}(F')) = F'$, showing ϕ^{fs} is surjective.
Finally ϕ^{fs} is order preserving because of $(*)$. □

Recall we noted last lecture that Γ^* is order isomorphic to the totally ordered (inclusion) set of principal final segments, given by

$$\Gamma^* \to \Gamma^{\text{pfs}},\ \gamma \mapsto [\gamma, \infty) = \gamma^+.$$

2. Principal convex subgroups

Definition 2.1. Let G be a totally ordered abelian group and $G_w \neq \{0\}$ a convex subgroup. G_w is said to be a **principal convex subgroup**, if $\exists g \in G$ such that G_w is the smallest convex subgroup containing g.

Remark 2.2. In the notation introduced and used in chapter I, $G_w = C_g$, i.e. G_w is the convex subgroup generated by g.

Lemma 2.3. *Let $G_w \neq \{0\}$ be a convex subgroup of G. The following are equivalent:*

(i) *G_w is principle convex generated by g,*

(ii) *Γ_w is a principal final segment, namely $v_G(g)^+$.*

Proof. First show $(i) \Rightarrow (ii)$. Note that $[g] \cap G_w^{<0}$ is an initial segment in G_w and that $[g] \cap G_w^{>0}$ is a final segment in G_w. So $v_G(g)$ is the smallest element of the final segment Γ_w, i.e. $\Gamma_w = v_G(g)^+$.
Show now $(ii) \Rightarrow (i)$. Assume that $\exists g \in G^{>0}$ such that $\Gamma_w = v_G(g)^+$ and argue reversing implications that we must have $[g] \cap G_w^{>0}$ is a final segment, i.e. G_w is the smallest convex subgroup containing g and multiples. □

3. Principal convex rank

Definition 3.1. Let G be a totally ordered abelian group. The **principal rank of** G is the order type of the chain of principle convex subgroups $\neq \{0\}$ of G.

Corollary 3.2. *(Characterization of the principal rank)*
The map $G_w \mapsto \min v_G(G_w)$ is an order reversing bijection between the principal rank of G and Γ. Therefore the principle rank of G is order isomorphic to Γ^{pfs}, i.e. to Γ^*.

Remark 3.3.

- Going down for the rank:

  rank of $K \to$ rank of $G = v(K) \to \Gamma^{\mathrm{fs}}$, $\Gamma = v_G(G) = v_G(v(K))$.
- Going up for the principal rank:

  $\Gamma^{\mathrm{pfs}} \cong \Gamma^* \to$ principal rank of $G \to$ principal rank of K?

Definition 3.4.

(i) A convex subring $K_w \supsetneq K_v$ is said to be a **principal convex subring** if $\exists a \in K^{>0} \backslash K_v$ such that K_w is the smallest convex subring containing a. We say K_w is the convex subring generated by a.

(ii) The **principal rank of** K is the (order type of the) set of all principal convex valuation rings ordered by inclusion. Denote it by $\mathcal{R}^{\mathrm{pr}} \subset \mathcal{R}$.

Definition 3.5. Let $a, b \in K^{>0} \backslash K$. We define a relation

$$a \sim b :\Leftrightarrow \exists n \in \mathbb{N} \text{ such that } a^n \geqslant b \text{ and } b^n \geqslant a.$$

ÜA: Show that $\sim$ is an (Archimedean) equivalence relation. Moreover,

$$a \sim b \Leftrightarrow v(a) \sim^+ v(b) \Leftrightarrow v_G(v(a)) = v_G(v(b)).$$

Therefore

$$K \to v(K) \to v_G(v(K^*)).$$

Theorem 3.6. *(Characterization of the principal rank of an ordered field) For $K_w \in \mathcal{R}$, the following are equivalent:*

(i) *$K_w \in \mathcal{R}^{pr}$ (generated by a)*

(ii) *G_w is a principal convex subgroup of $G = v(K^*)$ generated by $v(a)$.*

(iii) *Γ_w is a principal final segment generated by $v_G(v(a))^+$.*

Corollary 3.7. $\mathcal{R}^{pr} \cong \Gamma^*$.

Corollary 3.8. *Given a chain $\Delta \neq \emptyset$, there exists a non-Archimedean real closed field K such that $\mathcal{R}_K^{\mathrm{pr}}$ is isomorphic to Δ.*

Proof. Take $k = \mathbb{R}$ (for example). Set $\Gamma = \Delta^*$, set $G := \bigoplus_\Gamma \mathbb{R}$ the Hahn sum. Then G has principal rank $\Gamma^* = \Delta^{**} = \Delta$. Set

$$\mathbb{K} = k((G)) = \mathbb{R}((G)).$$

Then $\mathbb{K}$ has principal rank Δ. □

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 $T_{\exp} = \text{Th}(\mathbb{R}, +, \cdot, 0, 1, <, \exp)$ 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 η is a convex subspace of M and $M \cong N \sqcup$ ker η.

(*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 $\mathbb{B}' \cong (\overline{K}^{>0},\cdot,1,<)$.

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (22: 02/07/15 - CORRECTED ON 15/07/19)

SALMA KUHLMANN

Contents

1. Decomposition

Recall 1.1. We had the additive and multiplicative decomposition. Let K be a totally ordered field, root closed for positive elements (in particular, if K is real closed). Then

$$(K, +, 0, <) = \mathbb{A} \sqcup \mathbb{A}' \sqcup I_v,$$

$$(K^{>0}, \cdot, 1, <) = \mathbb{B} \sqcup \mathbb{B}' \sqcup 1 + I_v,$$

where $\mathbb{A}$ is a complement to the valuation ring and $\mathbb{A}'$ a complement to the valuation ideal in the valuation ring $S(\mathbb{A}) = [G^{<0}, \{(\overline{K}, +, 0, <)\}]$, $\mathbb{A}' \cong (\overline{K}, +, 0, <)$.

$\mathbb{B}$ is a (multiplicative) complement to $U_v^{>0}$ in $K^{>0}$ and $\mathbb{B}'$ is a complement to $1 + I_v$ in U_v. We have $\mathbb{B} \cong G$ and $\mathbb{B}' \cong (\overline{K}^{>0}, \cdot, 1, <)$.

2. Compatible exponentials

Definition 2.1. Let K be a totally ordered field root closed for positive elements.

(i) $f : (K, +, 0, <) \xrightarrow{\sim} (K^{>0}, \cdot, 1, <)$ is called an **exponential**.

(ii) An exponential f on K is called v-**compatible** (i.e. compatible with the natural valuation) if
- $f(K_v) = U_v^{>0}$ (the image of the valuation ring is the group of positive units)
- $f(I_v) = 1 + I_v$ (the image of the valuation ideal is the group of 1-units)

Remark 2.2. We only study v-compatible exponentials. In fact: a root closed (positive elements) totally ordered field K admits an exponential if and only if it admits a v-compatible exponential.

Indeed, if K admits an exponential e, then it admits a v-compatible exponential f, namely: Let $a \in K^{>0}$ such that $e(a) = 2$ and set $f(x) = e(ax)$. One verifies that $f(K_v) = U_v^{>0}$ and $f(I_v) = 1 + I_v$ (ÜA).

The question we want to answer: Given a totally ordered field (root closed for positive elements), when does K admit a v-compatible exponential. We will give necessary conditions on $v(K^*)$ and $\overline{K}$ as follows:

Remark 2.3. If f is a v-compatible exponential, then

(*i*) $f(K_v) = f(\mathbb{A}' \sqcup I_v) = U_v^{>0} = \mathbb{B}' \sqcup 1 + I_v$,

(*ii*) $f(I_v) = 1 + I_v$,

(*iii*) $f(\mathbb{A} \sqcup \mathbb{A}' \sqcup I_v) = \mathbb{B} \sqcup \mathbb{B}' \sqcup (1 + I_v)$.

Therefore f "decomposes" into 3 isomorphisms of ordered groups, namely

- the left exponential $f_L := f \upharpoonright \mathbb{A}$,
- the middle exponential $f_M := f \upharpoonright \mathbb{A}'$,
- the right exponential $f_R := f \upharpoonright I_v$.

Note that

$$\mathbb{A} \sqcup \mathbb{A}' \sqcup I_v \cong (K, +0, <) \cong (K^{>0}, \cdot, 1, <) \cong \mathbb{B} \sqcup \mathbb{B}' \sqcup 1 + I_v$$

and conversely, given $f_L : \mathbb{A} \cong \mathbb{B}$, $f_M : \mathbb{A}' \cong \mathbb{B}'$, and $f_R : I_v \cong 1 + I_v$, the exponential

$$f : (K, +, 0, <) \to (K^{>0}, \cdot, 1, <), a + a' + \varepsilon \mapsto f_L(a) f_M(a') f_R(\varepsilon)$$

on K is v-compatible.

So the question is: when does a totally ordered field K (root closed for positive elements) admit a left exponential, a middle exponential and a right exponential?

Proposition 2.4. *Let K be a non-Archimedean real closed field, $G = v(K^*)$. Assume that K admits a left exponential. Then*

$$S(G) = [G^{<0}, \{(\overline{K}, +, 0, <)\}],$$

i.e. the value set of G is isomorphic to $G^{<0}$ and all Archimedean components of G are isomorphic to $(\overline{K}, +, 0, <)$.

Proof. Note that $\mathbb{A} \cong \mathbb{B}$ and $\mathbb{B} \cong G$, so $\mathbb{A} \cong G$. In particular

$$[G^{<0}, \{(\overline{K}, +, 0, <)\}] = S(\mathbb{A}) = S(G).$$

□

Example 2.5. Consider the divisible ordered abelian group $G = \coprod_{\mathbb{N}} \mathbb{Q}$ and $\mathbb{K} = \mathbb{R}((G))$. Then $\mathbb{K}$ does not admit an exponential because

- G is divisible, so $G^{<0} \not\cong \mathbb{N}$,
- the Archimedean components of G are $\mathbb{Q}$, whereas the residue field is $\mathbb{R}$.

Example 2.6. Consider $G = \coprod_{\mathbb{Q}} \mathbb{Q}^{\mathrm{rc}}$. Note that the value set of G is $\mathbb{Q}$ and that $G^{<0}$ is a dense linear order without end points. So by Cantor $\mathbb{Q} \cong G^{<0}$.

Consider $\mathbb{K} = \mathbb{Q}^{\mathrm{rc}}((\coprod_{\mathbb{Q}} \mathbb{Q}^{\mathrm{rc}}))$. Then $\mathbb{K}$ is real closed and also the Archimedean components of G are all isomorphic to $\mathbb{Q}^{\mathrm{rc}}$ (the additive group of the residue field).

Unfortunately $\mathbb{K}$ still does not admit a left exponential because of the following theorem (without proof)

Theorem 2.7. *Let $\mathbb{K} = k((G))$, $G \neq \{0\}$, a real closed field of power series. Then $\mathbb{K}$ does not admit a left exponential function.*

Thus, the necessary condition on the value group is not sufficient.
Question: Does $\mathbb{K} = \mathbb{Q}^{\mathrm{rc}}((\coprod_{\mathbb{Q}} \mathbb{Q}^{\mathrm{rc}}))$ admit a right exponentiation?

Theorem 2.8. *Every real closed field of formal power series admits a right exponential function, namely*

$$\exp : \mathbb{R}((G^{>0})) \xrightarrow{\sim} 1 + \mathbb{R}((G^{>0})),\ \varepsilon \mapsto \sum_i \frac{\varepsilon^i}{i!}$$

(recall Neumann's lemma, see chapter II)

Proposition 2.9. *Let K be a real closed field and assume that K admits a middle exponential. Then $\overline{K}$ is an exponential Archimedean field.*

Proof. Note that

$$(\overline{K}, +, 0, <) \cong \mathbb{A}' \cong \mathbb{B}' \cong (\overline{K}^{>0}, 1, \cdot, <),$$

therefore f_M is an exponential on $\overline{K}$. $\square$

$\mathbb{K}$ does not admit a middle exponential (e is transcendental, $\mathbb{Q}^{\mathrm{rc}}$ is not an Archimedean exponential field).

Example 2.10. Let E be a countable real closed exponentially closed subfield of $\mathbb{R}$. Note that such an E exists, it can be constructed by induction from $\mathbb{Q}$ by countable iteration of taking real closure, exponential closure and closure under logarithm for positive elements.

Consider $G = \bigcup_{\mathbb{Q}} E$, $\mathbb{K} = E((G))$. Then $\mathbb{K}$ admits a middle and right exponential, but still no left exponential.

Open Question: Does every non-Archimedean real closed field admit a right exponential function?

Theorem 2.11. *(Ron Brown)*
Let (V, v) be a countable dimensional valued vector space. Then V admits a valuation basis.
In particular, if (V_1, v_1) and (V_2, v_2) are countable dimensional valued vector spaces with same skeleton $S(V_1) = S(V_2)$, then they are isomorphic as valued vector spaces, i.e. $(V_1, v_1) \cong (V_2, v_2)$.

Proof. Follows by induction from the following lemma □

Lemma 2.12. *Let V be a valued vector space, W a finite dimensional subspace with valuation basis $\mathcal{B}$ and let $a \in V$. Then $\mathcal{B}$ can be extended to a valuation basis of $< W, a >$.*

Proof. Consider $\{v(b) : b \in \mathcal{B}\}$ finite. So there exists some $a_0 \in W$ such that $v(a - a_0) \notin v(W)$ or, if this is not possible, such that $v(a - a_0) \in v(W)$ is maximal. Without loss of generality, $a \notin W$. If $v(a - a_0) \notin v(W)$, then $\mathcal{B} \cup \{a - a_0\}$ is the required valuation basis of $< W, a >$.
Otherwise set $\gamma := v(a - a_0) \in v(W)$. By the characterization of valuation basis (see chapter I) B_γ forms a basis of $\mathcal{B}(W, \gamma)$. If $\pi(\gamma, a - a_0)$ would live in $\mathcal{B}(W, \gamma)$, there would be a linear combination a_1 of elements of $\mathcal{B}$ with value γ such that $\pi(\gamma, a - a_0 - a_1) = 0$. But this means that $v(a - a_0 - a_1) > \gamma$, a contradiction. So $\pi(\gamma, a - a_0) \notin \mathcal{B}(W, \gamma)$, so $\mathcal{B} \cup \{a - a_0\}$ is valuation independent.

□

Corollary 2.13. *(Answer to the open question in the countable case)*
Let K be a countable non-Archimedean real closed field. Then K admits right exponentiation.

Proof. It can be shown that for any ordered field $S(I_v) \cong S(1 + I_v)$. In particular, by Brown's theorem, if K is countable, I_v and $I_v + 1$ are both countable and have the same skeleton, so they are isomorphic. □

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (23: 06/07/15)

SALMA KUHLMANN

Contents

Appendix

The goal of this lecture is to describe the real closure of a Hardy field. In particular, we want to prove the following theorem:

Theorem 0.1. *(Main Theorem)*
The real closure of a Hardy field is again a Hardy field.

1. Preliminaries

Notation 1.1.

- If f is a differentiable function from some half-line (a, ∞) to $\mathbb{C}$, we will denote by $\delta(f)$ the derivative of f.
- If k is a field and $P \in k[X]$, let P' denote the derivative of P and $Z(P)$ the set of roots of P.
- $F := \{f : (a, \infty) \to \mathbb{C} \mid a \in \mathbb{R}\}$.
- $G := \{f : (a, \infty) \to \mathbb{R} \mid a \in \mathbb{R}\} \subseteq F$.
- For $f, g \in F$ define
$$f \sim g :\Leftrightarrow \exists a \in \mathbb{R}\, \forall x > a : f(x) = g(x).$$
Then $\sim$ is an equivalence relation on F. Denote by $\overline{f}$ the equivalence class of f.
- Denote $\mathcal{F} := F/\sim$ and $\mathcal{G} := G/\sim$. Then $\mathcal{F}$ and $\mathcal{G}$ are rings with operations defined by:
$$\overline{f} + \overline{g} = \overline{f+g} \text{ and } \overline{f}\,\overline{g} = \overline{fg}.$$
- We say that $\overline{f}$ is differentiable if there exists $a \in \mathbb{R}$ such that f is differentiable on (a, ∞), and in that case we define the derivative of $\overline{f}$ as $\delta(\overline{f}) := \overline{\delta(f)}$

Definition 1.2.

(*i*) A **Hardy field** is a subring K of $\mathcal{G}$ which is a field and such that for every $\overline{f} \in K$, $\overline{f}$ is differentiable and $\delta(\overline{f}) \in K$.

(*ii*) A **complex Hardy field** is a subring K of $\mathcal{F}$ which is a field and such that for every $\overline{f} \in K$, $\overline{f}$ is differentiable and $\delta(\overline{f}) \in K$.

Definition 1.3. Let K be a Hardy field and $P \in K[X]$ of degree n, say $P = \sum_{m=0}^{n} \overline{f}_m X^m$. If $a \in \mathbb{R}$ is such that $f_1, \ldots, f_n$ are all defined and C^1 on (a, ∞) and $f_n(x) \neq 0$ for all $x > a$, we say that P is **defined** on (a, ∞). Note that such an a always exists.

Notation 1.4. If P is defined on (a, ∞), then for any $x > a$ we define $P_x := \sum_{m=0}^{n} f_m(x) X^m \in \mathbb{R}[X]$.

Remark 1.5. Note that P_x also has degree n and that $(P_x)' = (P')_x$, which we will just denote by P'_x. Of course, the definition of P_x depends on the choice of representatives for $\overline{f}_1, \ldots, \overline{f}_n$. However, whenever a polynomial is introduced, we will always assume we have fixed the representatives of its coefficients, so that P_x is well-defined.

Remark 1.6. Note that if $g \in F$, then $P(\overline{g})$ is the germ of the function $\sum f_i g^i$, so $P(\overline{g}) = 0$ if and only if there exists some a such that $P_x(g(x)) = 0$ for all $x > a$.

Recall 1.7. Let K be a field and $P \in K[X]$.

(*i*) P has only simple roots in its splitting field iff $gcd(P, P') = 1$ iff there exist $A, B \in K[X]$ such that $AP + BP' = 1$.

(*ii*) If $char(K) = 0$ and P is irreducible, then $gcd(P, P') = 1$.

The keystone of the proof of the main theorem is a well-known theorem from analysis, namely the **implicit function theorem**, which we recall here.

Theorem 1.8. *(IFT)*
Let $U \subseteq \mathbb{R}^n$, $V \subseteq \mathbb{R}^m$ be open, $u : U \times V \to \mathbb{R}^m$ a C^k function for some $k \in \mathbb{N}$ and $(x_0, y_0) \in U \times V$ such that $u(x_0, y_0) = 0$ and $det(\frac{\partial u}{\partial y}(x_0, y_0)) \neq 0$. Then there exists an open ball U_0 containing x_0, an open ball V_0 containing y_0 and a C^k function $\phi : U_0 \to V_0$ such that for any $(x, y) \in U_0 \times V_0$:

$$u(x, y) = 0 \Leftrightarrow y = \phi(x).$$

We will actually need a particular form of the implicit function theorem, namely:

Theorem 1.9. *(IFT')*
Let K be a Hardy field, $P \in K[X]$ defined on (a, ∞), $x_0 > a$ and y_0 a complex root of P_{x_0} which is not a root of P'_{x_0}. Then there exists an open interval I containing x_0, an open ball U containing y_0 and a C^1 function $\phi : I \to U$ such that:

$$(*) \quad \forall (x, y) \in I \times U : P_x(y) = 0 \Leftrightarrow y = \phi(x)$$

Proof. Set

$$u : (a, \infty) \times \mathbb{C} \to \mathbb{C},\ (x, y) \mapsto P_x(y).$$

Then u is C^1 on $(a, \infty) \times \mathbb{C}$. By assumption, we have $u(x_0, y_0) = 0$ and $\frac{\partial u}{\partial y}(x_0, y_0) = P'_{x_0}(y_0) \neq 0$, so we can apply the IFT to the function u at the point (x_0, y_0). □

2. Proof of the Main Theorem

Lemma 2.1. *Let K be a Hardy field and $P \in K[X]$ defined on (a, ∞). If $gcd(P, P') = 1$, then there exists some $b > a$ such that $gcd(P_x, P'_x) = 1$ for all $x > b$.*

Proof. Since $gcd(P, P') = 1$, there are $A, B \in K[X]$ such that $AP + BP' = 1$. Now let $b > a$ such that A, B are defined on (b, ∞); for $x > b$ we have $A_x P_x + B_x P'_x = 1$, hence $gcd(P_x, P'_x) = 1$. □

Lemma 2.2. *Let K be a Hardy field, $P \in K[X]$ non-zero defined on (a, ∞) and f a continuous function from (a, ∞) to $\mathbb{C}$ such that $P_x(f(x)) = 0$ and $P'_x(f(x)) \neq 0$ for all $x > a$. Then f is differentiable on (a, ∞).*

Proof. Let $x_0 > a$, $y_0 := f(x_0)$. By hypothesis, y_0 is a root of P_{x_0} but not of P'_{x_0}. Thus, we may apply IFT', and obtain I, U and ϕ as in IFT' such that $(*)$ holds.
Set $J := I \cap f^{-1}(U)$. U is a neighborhood of y_0 and f is continuous, so $f^{-1}(U)$ is a neighborhood of x_0, so J is also a neighborhood of x_0. Let $x \in J$; by assumption we have $P_x(f(x)) = 0$ and $(x, f(x)) \in I \times U$, which by $(*)$ implies that $f(x) = \phi(x)$.
Therefore $f_{|J} = \phi_{|J}$, which, since ϕ is C^1, implies that f is differentiable at x_0. Since x_0 was chosen arbitrarily, we obtain that f is differentiable on (a, ∞). □

Proposition 2.3. *Let K be a Hardy field and $f \in F$ a continuous function such that there exists $P \in K[X]$ non-zero such that $P(\overline{f}) = 0$. Then the ring $K[\overline{f}]$ is a complex Hardy field. If f happens to be in G, then $K[\overline{f}]$ is a Hardy field.*

Proof. Without loss of generality we can assume that P is irreducible. This implies that $K[\overline{f}]$ is isomorphic to $K[X]/(PK[X])$, so it is a field. We now have to show that every element of $K[\overline{f}]$ is differentiable and that $K[\overline{f}]$ is stable under derivation. It is sufficient to show that $\overline{f}$ is differentiable and that $\delta(\overline{f}) \in K[\overline{f}]$.

Since $P(\overline{f}) = 0$, there exists some $a \in \mathbb{R}$ such that $P_x(f(x)) = 0$ for all $x > a$. As P is irreducible and $\mathrm{char}(K) = 0$, $gcd(P, P') = 1$, so by Lemma 2.1 there exists some $b > a$ such that $gcd(P_x, P_x') = 1$ for all $x > b$. Hence, P_x and P_x' have no root in common. Thus, $P_x(f(x)) = 0 \neq P_x'(f(x))$ for any $x > b$. Now apply Lemma 2.2 and obtain that f is differentiable on (b, ∞). Set $P = \sum_{m=0}^{n} \overline{g}_m X^m$. Then

$$\begin{aligned}
0 = \delta(P(\overline{f})) &= \sum_{m=0}^{n} \delta(\overline{g}_m \overline{f}^m) \\
&= \delta(\overline{g_0}) + \sum_{m=1}^{n} (\delta(\overline{g}_m)\overline{f}^m + m\overline{g}_m \overline{f}^{m-1}\delta(\overline{f})) \\
&= \sum_{m=0}^{n} \overline{\delta(g_m)}\,\overline{f}^m + \delta(\overline{f}) \sum_{m=1}^{n} m\overline{g}_m \overline{f}^{m-1} \\
&= Q(\overline{f}) + \delta(\overline{f})P'(\overline{f})
\end{aligned}$$

with $Q \in K[X]$, hence $\delta(\overline{f}) = \frac{-Q(\overline{f})}{P'(\overline{f})} \in K(\overline{f}) = K[\overline{f}]$. $\square$

Lemma 2.4. *Let K be a Hardy field, $n \in \mathbb{N}$ and $P \in K[X]$ of degree n defined on (a, ∞), such that P_x has n distinct roots in $\mathbb{C}$ for all $x > a$.*
For any pair $(x_0, y_0) \in (a, \infty) \times \mathbb{C}$ such that y_0 is a root of P_{x_0}, there exists a C^1 function $\phi : (a, \infty) \to \mathbb{C}$ such that $y_0 = \phi(x_0)$ and

$$\forall x > a : P_x(\phi(x)) = 0 \quad (\dagger)$$

Proof. Let $x_0 > a$ and y_0 a complex root of P_{x_0}. Since P_{x_0} has simple roots, y_0 is not a root of P_{x_0}', so we can apply IFT' and we get an open interval I containing x_0, an open ball U containing y_0 and a C^1 function $\phi : I \to U$ such that $(*)$ is satisfied, which in particular implies that $\phi(x_0) = y_0$ and $P_x(\phi(x)) = 0$ for all $x \in I$. Define $\mathcal{E}$ to be the set

$\{(J, \psi) \mid I \subseteq J$ open interval, ψ C^1-extension of ϕ to J satisfying $(\dagger)$ on $J\}$.

Note that $\mathcal{E}$ is non-empty since $(I, \phi) \in \mathcal{E}$. We can partially order $\mathcal{E}$ by saying that $(J, \psi) \leqslant (J', \chi)$ if $J \subseteq J'$ and χ extends ψ.
Let $(J_h, \psi_h)_{h \in H}$ be a chain in $\mathcal{E}$. Set $J := \bigcup_{h \in H} J_h$ and define ψ on J by $\psi(x) = \psi_h(x)$ if $x \in J_h$; this is well-defined because ψ_h is an extension of $\psi_{h'}$ for any $h, h' \in H$ such that $J_{h'} \subseteq J_h$. If $x \in J$, then $x \in J_h$ for some $h \in H$, and since $(J_h, \psi_h) \in \mathcal{E}$ we have $P_x(\psi_h(x)) = 0$, hence $P_x(\psi(x)) = 0$. Thus, ψ satisfies $(\dagger)$ on J, so $(J, \psi) \in \mathcal{E}$. Moreover, we have $(J_h, \psi_h) \leqslant (J, \psi)$ for any $h \in H$, so (J, ψ) is an upper bound of $(J_h, \psi_h)_{h \in H}$.
We just proved that any chain of $\mathcal{E}$ has an upper bound. By Zorn's lemma, it follows that $\mathcal{E}$ has a maximal element (J, ψ)

To conclude the proof, we have to show that $J = (a, \infty)$. Set $b := \sup J$. Towards a contradiciton, assume that $b \neq \infty$. By hypothesis, P_b has n distinct roots $y_1, \ldots, y_n$, none of which is a root of P_b'. We apply IFT' at each of the points $(b, y_1), \ldots, (b, y_n)$, and we obtain open intervals $I_1, \ldots, I_n$ containing b, open balls $U_1, \ldots, U_n$ containing $y_1, \ldots, y_n$ and C^1 functions $\phi_1 : I_1 \to U_1, \ldots, \phi_n : I_n \to U_n$, such that for each $m \in \{1, \ldots, n\}$, for any

$(x,y) \in I_m \times U_m$, $P_x(y) = 0 \Leftrightarrow y = \phi_m(x)$. Since $y_1, \ldots, y_n$ are pairwise distinct,we can choose the sets $U_1, \ldots, U_n$ so small that they are pairwise disjoint.

Let $I' := \bigcap_{m=1}^n I_m$. For any $x \in I'$, we have $\phi_1(x) \in U_1, \ldots, \phi_n(x) \in U_n$; since $U_1, \ldots, U_n$ are pairwise disjoint, $\phi_1(x), \ldots, \phi_n(x)$ are pairwise distinct. By $(*)$, each $\phi_m(x)$ is a root of P_x; since P_x has n roots, it follows that $Z(P_x) = \{\phi_1(x), \ldots, \phi_n(x)\} \subseteq \bigcup_{m=1}^n U_m$.

Let $J' := I' \cap J$; note that J' is an interval. For any $x \in J'$, $(\dagger)$ implies that $\psi(x)$ is a root of P_x, hence $\psi(x) \in \bigcup_{m=1}^n U_m$. Thus, $\psi(J') \subseteq \bigcup_{m=1}^n U_m$. Since ψ is continuous, $\psi(J')$ is connected. Since $U_1, \ldots, U_n$ are pairwise disjoint, this implies that there exists $m \in \{1, \ldots, n\}$ such that $\psi(J') \subset U_m$.

Let $x \in J'$; we have $(x, \psi(x)) \in I_m \times U_m$ and $P_x(\psi(x)) = 0$. Since ϕ_m satisfies $(*)$ on $I_m \times U_m$, it follows that $\psi(x) = \phi_m(x)$. This proves that $\psi_{|J'} = \phi_{m|J'}$.

Define the function $\tilde{\psi}$ on $J \cup I'$ by $\tilde{\psi}(x) := \begin{cases} \psi(x) & \text{if } x \in J \\ \phi_m(x) & \text{if } x \in I' \end{cases}$.

This definition makes sense because ψ and ϕ_m agree on I'. $\tilde{\psi}$ is a strict extension of ψ. Since ψ and ϕ_m are C^1, $\tilde{\psi}$ is also C^1. Since ψ satisfies $(\dagger)$ on J and ϕ_m satisfies $(*)$ on I', it follows that $\tilde{\psi}$ satisfies $(\dagger)$ on $J \cup I'$, which contradicts the maximality of (J, ψ). Thus, $b = \infty$ (note that we could prove the same way that $\inf J = a$). □

Lemma 2.5. *Let K be a Hardy field and $P \in K[X]$ of degree n such that $gcd(P, P') = 1$. Then there exists some $a \in \mathbb{R}$ and n C^1 functions $\phi_1, \ldots \phi_n : (a, \infty) \to \mathbb{C}$ such that $Z(P_x) = \{\phi_1(x), \ldots, \phi_n(x)\}$ for each $x > a$.*

Proof. By Lemma 2.1, there exists some $a_0 \in \mathbb{R}$ such that $gcd(P_x, P'_x) = 1$ for all $x > a_0$, which means that P_x has n distinct roots in $\mathbb{C}$. Let $a > a_0$, and let $y_1, \ldots, y_n$ be the n distinct roots of P_a. By the previous lemma, we obtain n C^1 functions $\phi_1, \ldots, \phi_n : (a_0, \infty) \to \mathbb{C}$ such that $\phi_m(a) = y_m$ for any $m \in \{1, \ldots, n\}$, and $\{\phi_1(x) \ldots, \phi_n(x)\} \subseteq Z(P_x)$ for any $x > a$. To show equality, we just have to show that $\phi_l(x) \neq \phi_m(x)$ for any $x > a$ and any $m, l \in \{1, \ldots, n\}$.

Now let $m, l \in \{1 \ldots n\}$ and $E := [a, \infty] \cap (\phi_m - \phi_l)^{-1}(\{0\})$. Assume $E \neq \varnothing$. By continuity of ϕ_m and ϕ_l, E is a closed subset of $\mathbb{R}$ and has a lower bound a, so it has a minimum b. Since $\phi_m(a) \neq \phi_l(a)$, $b > a$. Set $c := \phi_m(b)$. c is a root of P_b, so we can apply IFT' at the point (b, c) and we get an open neighborhood $I \times U$ of (b, c) and a map $\phi : I \to U$ satisfying $(*)$. Since U is a neighborhood of c, and since $c = \phi_m(b) = \phi_l(b)$, $\phi_l^{-1}(U)$ and $\phi_m^{-1}(U)$ are neighborhoods of b, so

$$J := I \cap (a, \infty) \cap \phi_l^{-1}(U) \cap \phi_m^{-1}(U)$$

is a neighborhood of b. Let $x \in J$ such that $x < b$; $(x, \phi_l(x))$ and $(x, \phi_m(x))$ both belong to $I \times U$ and we have $P_x(\phi_m(x)) = P_x(\phi_l(x)) = 0$; since ϕ satisfies $(*)$ on $I \times U$, this implies $\phi_l(x) = \phi(x) = \phi_m(x)$, so $x \in E$, which contradicts the minimality of b. Thus, $E = \varnothing$. □

Proposition 2.6. *Let k be a Hardy field,*

$$K := \{\overline{f} \in \mathcal{G} \mid \ f \text{ continuous and } \exists P \in k[X] \text{ with } P \neq 0 \wedge P(\overline{f}) = 0\}$$

and

$$L := \{\overline{f} \in \mathcal{F} \mid \ f \text{ continuous and } \exists P \in k[X] \text{ with } P \neq 0 \wedge P(\overline{f}) = 0\}.$$

Then K is a Hardy field, L is a complex Hardy field, L is the algebraic closure of k and K is the real closure of k.

Proof. Obviously, $k \subseteq K \subseteq L$. Now let $\overline{f}, \overline{g} \in K$. By Proposition 2.3, $k[\overline{f}]$ is a Hardy field. Since g is continuous and $\overline{g}$ is canceled by a polynomial in $k[\overline{f}][X]$, we can once again use Proposition 2.3 and we obtain that $k[\overline{f}, \overline{g}]$ is a Hardy field, and since it is algebraic over k, it is contained in K. Since $k[\overline{f}, \overline{g}]$ is a Hardy field, we have

$$0, 1, \overline{f} - \overline{g}, \frac{\overline{f}}{\overline{g}}, \delta(\overline{f}), \delta(\overline{g}) \in k[\overline{f}, \overline{g}],$$

hence

$$0, 1, \overline{f} - \overline{g}, \frac{\overline{f}}{\overline{g}}, \delta(\overline{f}), \delta(\overline{g}) \in K.$$

This proves that K is Hardy field. The same proof shows that L is a complex Hardy field.

Now let us show that L is algebraically closed. Let $P \in k[x]$ irreducible of degree $n > 1$. Since $char(k) = 0$, $gcd(P, P') = 1$. By Lemma 2.5 there exists some $a \in \mathbb{R}$ and C^1 functions $\phi_1, \ldots, \phi_n : (a, \infty) \to \mathbb{C}$, such that for any $x > a$, $Z(P_x) = \{\phi_1(x), \ldots, \phi_n(x)\}$. This means that $\overline{\phi}_1, \ldots, \overline{\phi}_n$ are n distinct roots of P. Since $\phi_1, \ldots, \phi_n$ are continuous functions from (a, ∞) to $\mathbb{C}$ and $\overline{\phi}_1, \ldots, \overline{\phi}_n$ are canceled by $P \in k[X]$, we have $\overline{\phi}_1, \ldots \overline{\phi}_n \in L$.

Thus, any polynomial with coefficients in k splits in L. Since L/k is an algebraic extension, this proves that L is algebraically closed, and thus L is the algebraic closure of k. Finally note that $L = K(i)$. Since $K(i)$ is algebraically closed, K is real closed, and it is the real closure of k. □

Corollary 2.7. *The real closure of a Hardy field is again a Hardy field.*

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (24: 09/07/15 - CORRECTED ON 09/07/19)

SALMA KUHLMANN

Contents

1. Baer-Krull Representation Theorem

Recall that an ordering $\leqslant$ and a valuation v on a field K are called compatible if

$$0 \leqslant x \leqslant y \Rightarrow v(y) \leqslant v(x).$$

In Proposition 2.3 of lecture 17 we fixed an ordered field $(K, \leqslant)$ and characterized the $\leqslant$-compatible valuations on K. Today, we fix a valued field (K, v) and describe the v-compatible orderings on K.

Notation 1.1. Let (K, v) be a valued field. Let Γ be the value group of v. The quotient group $\overline{\Gamma} = \Gamma/2\Gamma$ becomes in a canonical way an $\mathbb{F}_2$-vector space. We denote by $\overline{\gamma} = \gamma + 2\Gamma$ the residue class of $\gamma \in \Gamma$.
Let $\{\pi_i : i \in I\} \subseteq K^*$ such that $\{\overline{v(\pi_i)} : i \in I\}$ is an $\mathbb{F}_2$-basis of $\overline{\Gamma}$. Then $\{\pi_i : i \in I\}$ is called a **quadratic system of representatives** of K with respect to v.

Theorem 1.2. *(Baer-Krull Representation Theorem)*
Let (K, v) be a valued field. Let $\mathcal{X}(K)$ and $\mathcal{X}(Kv)$ denote the set of all orderings of K and Kv, respectively. Fix some quadratic system $\{\pi_i : i \in I\}$ of representatives of K with respect to v.
Then there is a bijective correspondence

$$\{P \in \mathcal{X}(K) : K_v \text{ is } P\text{-convex}\} \longleftrightarrow \{-1, 1\}^I \times \mathcal{X}(Kv)$$

described as follows: given an ordering P on K such that K_v is P-convex, let $\eta_P : I \to \{-1, 1\}$, where $\eta_P(i) = 1 \Leftrightarrow \pi_i \in P$. Then the map

$$P \mapsto (\eta_P, \overline{P})$$

is the above bijective correspondence.

Proof. Given a mapping $\eta : I \to \{-1, 1\}$ and an ordering Q on Kv, we will define an ordering $P(\eta, Q)$ on K, such that K_v is $P(\eta, Q)$-convex and $P(\eta, Q)$ is mapped to (η, Q) by the map described in the claim.
Let $a \in K^*$. As $\{\overline{v(\pi_i)} : i \in I\}$ is a basis of $\overline{\Gamma}$, there exist uniquely determined indices $i_1, \ldots, i_r$ such that

$$\overline{v(a)} = \overline{v(\pi_{i_1})} + \ldots + \overline{v(\pi_{i_r})}.$$

Thus, for some $b \in K$, one has

$$\begin{aligned} v(a) &= v(\pi_{i_1}) + \ldots + v(\pi_{i_r}) + 2v(b) \\ &= v(\pi_{i_1} \ldots \pi_{i_r} b^2). \end{aligned}$$

Hence, we find some $u \in U_v$ such that

$$a = u\pi_{i_1} \cdots \pi_{i_r} b^2.$$

Note that since b is only determined up to a unit, u is only determined up to a unit square. Let $\eta : I \to \{-1, 1\}$ be a mapping and $Q \in \mathcal{X}(Kv)$ a positive cone on Kv. We define $P(\eta, Q) \subset K$ by $0 \in P(\eta, Q)$ and for each $a \in K^*$ with $a = u\pi_{i_1} \cdot \ldots \cdot \pi_{i_r} b^2$ as above,

$$a \in P(\eta, Q) :\Leftrightarrow \eta(i_1) \cdots \eta(i_r)\overline{u} \in Q.$$

Note that $P(\eta, Q)$ is well-defined, as u and hence $\overline{u}$ is determined up to a unit square and $i_1, \ldots, i_r$ are completely determined. We have to show that $P(\eta, Q)$ is an ordering such that K_v is $P(\eta, Q)$-convex, and that $\overline{P(\eta, Q)} = Q$. We first show that $P(\eta, Q)$ is additively closed. Let $a, a' \in P(\eta, Q)$ with $a, a' \neq 0$. Moreover, let $u, u' \in U_v$, $b, b' \in K$ and $i_1, \ldots, i_r, j_1, \ldots, j_s \in I$ such that

$$\begin{aligned} a &= u\pi_{i_1} \cdots \pi_{i_r} b^2, \\ a' &= u'\pi_{j_1} \cdots \pi_{j_s} (b')^2. \end{aligned}$$

If $v(a) \neq v(a')$, say $v(a) < v(a')$, then $v(a + a') = v(a)$. Hence, $a + a' = ca$ for some $c \in U_v$. Note that $\frac{a'}{a} \in I_v$. Thus, from $1 + \frac{a'}{a} = c$ follows $\overline{c} = \overline{1}$. We obtain $a + a' = cu\pi_{i_1} \cdots \pi_{i_r} b^2$.
As $a \in P(\eta, Q)$ we have

$$\begin{aligned} Q \ni \eta(i_1) \cdots \eta(i_r)\overline{u} &= \eta(i_1) \cdots \eta(i_r)\overline{1}\overline{u} \\ &= \eta(i_1) \cdots \eta(i_r)\overline{cu}. \end{aligned}$$

Hence, $a + a' \in P(\eta, Q)$.
If $v(a) = v(a')$, then $\{i_1, \ldots, i_r\} = \{j_1, \ldots, j_s\}$. Furthermore, $b' = bu''$ for some $u'' \in U_v$. Hence,

$$a + a' = (u + u'(u'')^2)b^2\pi_{i_1} \cdots \pi_{i_r}.$$

If $\eta(\pi_{i_1}) \cdots \eta(\pi_{i_r}) = 1$, then $\overline{u}, \overline{u'} \in Q$ and hence

$$\overline{u + u' + (u'')^2} = \eta(\pi_{i_1}) \cdots \eta(\pi_{i_r})\overline{u + u' + (u'')^2} \in Q,$$

i.e. $a + a' \in P(\eta, Q)$.
If $\eta(\pi_{i_1}) \cdots \eta(\pi_{i_r}) = -1$, then $-\overline{u}, -\overline{u'} \in Q$. Hence

$$-\overline{u + u'(u'')^2} = \eta(\pi_{i_1}) \cdots \eta(\pi_{i_r})\overline{u + u'(u'')^2} \in Q,$$

and therefore $a + a' \in P(\eta, Q)$.
In order to prove that $P(\eta, Q)$ is closed under multiplication, we extend η to an $\mathbb{F}_2$-linear map from $\overline{\Gamma}$ to $\{-1, 1\}$. We define $\eta(\overline{v(\pi_i)}) = \eta(i)$, which determines the map completely, since the elements $\overline{v(\pi_i)}$ form a basis for $\overline{\Gamma}$. By composing

$$K^* \xrightarrow{v} \Gamma \to \overline{\Gamma} \xrightarrow{\eta} \{-1, 1\}$$

we obtain a group homomorphism $K^* \to \{-1, 1\}$, which we also denote by η. We have $a \in P(\eta, Q)$ if and only if $\eta(a)\overline{u} \in Q$ for all $a \in K^*$. From this it

follows at once that $aa' \in P(\eta, Q)$ for $a, a' \in P(\eta, Q)$.
As $Q \cup -Q = Kv$, it is clear from the definition that

$$P(\eta, Q) \cup -P(\eta, Q) = K$$

and as $-1 \notin Q$, it is clear that $-1 \notin P(\eta, Q)$.
Further note that $1 + I_v \subseteq P(\eta, Q)$. Indeed, if $x \in I_v$, then $v(1 + x) = 0$, i.e. $1 + x = ub^2$. Thus,

$$\overline{ub^2} = \overline{1 + x} = \overline{1} \in Q,$$

which implies that $1 + x \in P(\eta, Q)$. Hence, by Proposition 2.3 of lecture 17, K_v is $P(\eta, Q)$-convex. This shows that $P(\eta, Q)$ is a positive cone of K and that K_v is $P(\eta, Q)$-convex.
We still have to prove that the mapping from the claim is bijective. Let $u \in U_v \cap P(\eta, Q)$. Then it follows from the definition that $\overline{u} \in Q$. Hence, $\overline{P(\eta, Q)} \subseteq Q$. As $\overline{P(\eta, Q)}$ and Q are both positive cones, $\overline{P(\eta, Q)} = Q$. Moreover, $\pi_i \in P(\eta, Q) \Leftrightarrow \eta(\pi_i) = 1$ is clear from the definition. This proves surjectivity of the map described in the claim.
Injectivity: Assume P is mapped to (η, Q). It is clear from the definition that $P(\eta, Q) \subseteq P$, and threfore $P(\eta, Q) = P$.

$\square$

Remark 1.3. Under additional assumptions, either factor of the cartesian product in the Baer-Krull Theorem may vanish.

(1) If Γ is 2-divisible, then $\overline{\Gamma} = \{0\}$, and therefore $I = \emptyset$. Thus, there is a bijective correspondence
$$\{P \in \mathcal{X}(K) : K_v \text{ is } P\text{-convex}\} \longleftrightarrow \mathcal{X}(Kv)$$
(2) If $\sum(Kv)^2$ is an ordering, then Kv is uniquely ordered (see RAG I). Thus, there is a bijective correspondence
$$\{P \in \mathcal{X}(K) : K_v \text{ is } P\text{-convex}\} \longleftrightarrow \{-1, 1\}^I.$$

Remark 1.4. If $(K, \leqslant)$ is an ordered field, then

$$\mathbb{Z}(\leqslant) := \{x \in K : x, -x \leqslant a \text{ for some } a \in \mathbb{Z}\}$$

is called the **$\leqslant$-convex hull of $\mathbb{Z}$** in K. It is a valuation ring on K which is non-trivial (i.e. $\neq K$) if and only if $\leqslant$ is non-Archimedean.

Corollary 1.5. *A field K admits a non-Archimedean ordering if and only if K carries a non-trivial valuation with real residue class field.*

Proof. Let P be a non-Archimedean ordering on K. Then $\mathbb{Z}(P)$ corresponds to a non-trivial valuation v on K, and $K_v = \mathbb{Z}(P)$ is P-convex. Applying the Baer-Krull Theorem to (K, v) yields that P corresponds to $(\eta_P, \overline{P})$. In particular, $\overline{P}$ is an ordering on Kv, i.e. Kv is real.
Conversely, let v be a non-trivial valuation on K (i.e. $K_v \subsetneq K$) with real residue class field Kv. Let Q be an ordering on Kv and choose $\eta = 1$ (i.e. $\eta(i) = 1$ for all i). By the Baer-Krull Theorem, there exists an ordering P of K for which K_v is P-convex. Note that $\mathbb{Z}(P) \subseteq K_v \subsetneq K$, since $\mathbb{Z}(P)$ is the smallest P-convex subring of K. Thus, P is non-Archimedean. $\square$

REAL ALGEBRAIC GEOMETRY LECTURE NOTES (25: 13/07/15)

SALMA KUHLMANN

Contents

Review

1. Chapter I: Valued vector spaces

Let us summarize:

Theorem 1.1. *(Hahnsandwiching Theorem)*
Let V be a valued $\mathbb{Q}$-vector space with skeleton $S(V) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}]$. Then

$$\bigcup_{\Gamma} B(\gamma) \hookrightarrow V \hookrightarrow \mathrm{H}_{\Gamma}\, B(\gamma).$$

Two big steps:

(1) $\bigcup_{\Gamma} B(\gamma) \hookrightarrow V$.

- we developed the notion of $\mathcal{B} \subset (V, v)$ to be a valuation basis.
- we showed the existence of a maximal valuation independent subset $\mathcal{B}_0$ of (V, v) and proved that $(< \mathcal{B}_0 >_{\mathbb{Q}}, v >) \subseteq (V, v)$ is an immediate extension.
- we noted that $\bigcup_{\Gamma} B(\gamma)$ admits a valuation basis and that the converse is true, i.e. whenever (V, v) admits a valuation basis, then $(V, v) \cong (\bigcup_{\Gamma} B(\gamma), v_{\min})$.
$(S(V) = [\Gamma, \{B(\gamma) : \gamma \in \Gamma\}])$
- so in general we proceeded as follows:
  - Given (V, v), choose some maximal valuation independent subset $\mathcal{B}_0$.

- Set $V_0 =< \mathcal{B}_0 >_{\mathbb{Q}}$. Then V_0 admits a valuation basis, namely $\mathcal{B}_0$.
- $\bigcup_\Gamma B(\gamma) \cong V_0$, so $\bigcup_\Gamma B(\gamma) \hookrightarrow V$.

(2) $V \hookrightarrow \mathrm{H}_\Gamma B(\gamma)$.

- we first showed that maximally valued $\Leftrightarrow$ pseudo complete.
- we showed that $\mathrm{H}_\Gamma B(\gamma)$ is pseudo complete.
- we proved that if $V_1'|V_1$ is immediate and $y \in V_1' \backslash V_1$, then y is a pseudo-limit of a pseudo-Cauchy sequence in V_1 with no pseudo-limit in V_1.

2. Chapter II: Valuations on ordered fields

Theorem 2.1. *(Kaplansky's Sandwich Theorem)*
Let K be a real closed field with $v(K^*) = G$ and $\overline{K} = k$. Then

$$k(G)^{rc} \hookrightarrow K \hookrightarrow k((G)).$$

This was again proved in 2 steps:

(1) We showed $G \hookrightarrow (K^{>0}, \cdot, 1, <)$ and $k \hookrightarrow K$.

(2) We proved the theorem that if k is real closed and G is divisible, then $k((G))$ is real closed. For this we first proved the same theorem with "real closed" replaced with "algebraically closed". Then (Mac Lane) if k is algebraically closed and G is divisible, then $k((G))$ is algebraically closed.

- $k((G))$ is pseudo-complete.
- the value group of an algebraic extension is contained in the divisible hull of the value group.
- the residue field of an algebraic extension is contained in the algebraic closure of the residue field of the original field.

With these results, one can prove that every algebraic extension must be immediate.

3. Chapter III: Convex valuations on ordered fields

We studied the (under inclusion) linearly ordered set of convex valuations in an ordered field, i.e. the rank $\mathcal{R}$ of K. We characterized it via the rank of $v(K^*)$ and the rank of the value set of $v(K^*)$, respectively,

$$K \xrightarrow{v} v(K^*) \xrightarrow{v_G} \Gamma.$$

Theorem 3.1. *(Characterization of valuations compatible with the order $\leqslant$ of K)*
For a valuation w on an ordered field $(K, \leqslant)$, the following are equivalent:

- *w is compatible with $\leqslant$,*
- *K_w is convex,*
- *I_w is convex*
- *$I_w < 1$,*
- *the residue map $K \to Kw$ induces canonically a total order on Kw ($P \mapsto \overline{P}$).*

Moreover, in the addendum, we proved the Baer-Krull Representation Theorem:

$$\{P \in \mathcal{X}(K) : K_v \text{ is } P\text{-convex}\} \xrightarrow{\sim} \mathcal{X}(K_v) \times \{-1, 1\}^I,$$

where $\mathcal{X}(K)$ and $\mathcal{X}(Kv)$ denote the set of all orderings of K and Kv, respectively, and $I := \dim_{\mathbb{F}_2} G/2G$.

4. Chapter IV: Ordered exponentials fields

Consider $(K, +, 0, <) \xrightarrow{\sim} (K^{>0}, \cdot, 1, <)$.

Theorem 4.1. *(Main Theorem)*

(i) $(K, +, 0, <) = \mathbb{A} \sqcup (\overline{K}, +, 0, <) \bigcup I_v$,

(ii) $(K^{>0}, \cdot, 1, <) = \mathbb{B} \sqcup (\overline{K}^{>0}, \cdot, 1, <) \sqcup 1 + I_v$.

Recall that $\exp_L : \mathbb{A} \xrightarrow{\sim} \mathbb{B}$, $\exp_M : (K, +, 0, <) \xrightarrow{\sim} (\overline{K^{>0}}, \cdot, 1, <)$ and $\exp_R : I_v \xrightarrow{\sim} 1 + I_v$, the left, middle and right exponential functions.

Discussion of necessary valuation-theoretic conditions:

Theorem 4.2. *If $(K, +, 0, 1, <)$ admits a v-compatible exponential, then*

(i) $\overline{exp} : (\overline{K}, +, 0, 1, <) \to (\overline{K}^{>0}, \cdot, 1, <)$, *so $\overline{K}$ is an exponential field.*

(ii) $S(v(K^*)) = [G^{<0} : \{(\overline{K}, +, 0, <)\}]$.

Example 4.3.

- Constructing real closed fields which do not admit an exponential function.
  Countable case: a countable divisible ordered abelian group (non-Archimedean) is an exponential group $\Leftrightarrow \cong \bigcup_{\mathbb{Q}} A$, where A is a countable Archimedean divisible ordered abelian group.
- exp is defined on I_v by Neumann's lemma, $\exp(\varepsilon) = \sum \frac{\varepsilon^i}{i!}$. So $\mathbb{K} = k((G))$ always admit $\exp_R$.

Theorem 4.4. $\mathbb{K}$ *never admits an* $\exp_L$.

Question: Does every real closed field admit $\exp_R$?

- True for countable fields.
- True for fields of power series.
- Otherwise?