Valued Fields, Model-Theoretic Aspects

Lou van den Dries

University of Illinois at Urbana-Champaign

Luminy, January 2018

- Introduction (including some history)
- Hensel's Lemma and henselian local rings
- Some valuation theory
- Algebraically closed valued fields

Introduction

Abraham Robinson proved in the 1950s the model completeness of algebraically closed valued fields, a result that has turned out to be seminal but didn't attract much attention at the time. (To me it was an eye-opener when I read the proof as a graduate student.)

1960s: Ax & Kochen and, independently, Ersov, proved a remarkable theorem on the model theory of henselian valued fields, with applications to p-adic number theory.

AKE (= Ax, Kochen, Ersov) was the starting point for a lot of work by many others, both on the applied side (Macintyre, Denef, Loeser, Hrushovski,...) and material with a more model-theoretic orientation (Haskell-Hrushovski-Macpherson,...).

Notations: $m, n \in \mathbb{N} = \{0, 1, 2, \ldots\}$, R and R' are rings (always commutative with 1), $\boldsymbol{k}$, $\boldsymbol{k}'$, K, and K' are fields.

Given R we have the power series ring $R[[t]]$ whose elements are the formal power series

$$a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \cdots \quad (\text{all } a_n \in R)$$

Exercise: this series is a **unit** of $R[[t]]$ iff a_0 is a unit of R.

Thus, give a field $\boldsymbol{k}$, the series $a_0 + a_1 t + a_2 t^2 + \cdots$ in $\boldsymbol{k}[[t]]$ with constant term $a_0 \neq 0$ are the units of $\boldsymbol{k}[[t]]$. Actually, $\boldsymbol{k}[[t]]$ is an integral domain with fraction field $\boldsymbol{k}((t))$, whose elements are the (formal) Laurent series over $\boldsymbol{k}$: the series

$$\sum_{i=i_0}^{\infty} a_i t^i \qquad (\text{all } a_i \in \boldsymbol{k},\ i_0 \in \mathbb{Z})$$

so we allow finitely many powers t^i with $i < 0$.

Introduction, continued

We can now state some special cases of AKE for $\boldsymbol{k}$ of characteristic 0:

$$\boldsymbol{k} \equiv \boldsymbol{k}' \implies \boldsymbol{k}[[t]] \equiv \boldsymbol{k}'[[t]]$$

(Open problem: can we drop here the characteristic 0 assumption.)

Relevant elementary properties of rings like $\boldsymbol{k}[[t]]$: they are henselian local rings, and they are valuation rings. (Polynomial rings $\boldsymbol{k}[t]$ are not local rings; power series rings like $\boldsymbol{k}[[t_1, t_2]]$ are henselian local rings, but not valuation rings, and the above implication fails for $\boldsymbol{k}[t]$ or $\boldsymbol{k}[[t_1, t_2]]$ in place of $\boldsymbol{k}[[t]]$.)

Other special case of AKE: $\quad \mathbb{C}\{t\} \preccurlyeq \mathbb{C}[[t]]$

Local Rings

A ring R is said to be **local** if it has exactly one maximal ideal $\mathfrak{m}$. In that case the field $\boldsymbol{k} = R/\mathfrak{m}$ is called the **residue field of** R. Think of the residue map $f \mapsto f + \mathfrak{m} : R \to \boldsymbol{k}$ as evaluating the "function" $f \in R$ at a point. Being local is a first-order property of rings: it is equivalent to $a + b$ being a non-unit for all non-units a, b (Exercise.)

Examples: $\boldsymbol{k}[[t]]$, with $\mathfrak{m} = (t)$ and $\boldsymbol{k}[[t]]/\mathfrak{m} \cong \boldsymbol{k}$

$\mathcal{O}_a$:= ring of germs of holomorphic functions at a point $a \in \mathbb{C}$. This is a local domain with $\mathfrak{m} = \{f \in \mathcal{O}_a : f(a) = 0\}$ and Taylor expansion at a yields an embedding of $\mathcal{O}_a$ into $\mathbb{C}[[t]]$ with image $\mathbb{C}\{t\}$

for a prime number p and $n \geqslant 1$ the ring $R := \mathbb{Z}/p^n\mathbb{Z}$ $(n \geqslant 1)$ is local with $\mathfrak{m}$ generated by the image of p in R and $R/\mathfrak{m} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

Local Rings continued

The rings $\mathbb{Z}/p^n\mathbb{Z}$ form a projective system:

$$\cdots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to \cdots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

$$\mathbb{Z}_p := \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z},$$

is called **the ring of** p**-adic integers** and has the advantage over the $\mathbb{Z}/p^n\mathbb{Z}$ of being a local *domain* extending $\mathbb{Z}$. Its elements can be represented uniquely in the form

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots \qquad (\text{all } a_i \in \{0, 1, 2, \ldots, p-1\})$$

For example, $(1 + p + p^2 + p^3 + \cdots)(1 - p) = 1$.

Exercise: what are the p-adic digits of -1?

Local rings, continued

Let R be a local ring. Then we have a descending sequence

$$R = \mathfrak{m}^0 \supseteq \mathfrak{m}^1 \supseteq \mathfrak{m}^2 \supseteq \mathfrak{m}^3 \supseteq \cdots$$

We have $\bigcap_n \mathfrak{m}^n = \{0\}$ in all the examples above. Assume this holds. Then we can define a **norm** on R by

$$|a| := 2^{-n} \quad \text{if } a \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}, \qquad |0| := 0.$$

Thus: $\quad |a| \leqslant 1, \quad |a+b| \leqslant \max(|a|,|b|), \quad |ab| \leqslant |a| \cdot |b|,$

$$|a| = 1 \;\Leftrightarrow\; a \in R \setminus \mathfrak{m} \;\Leftrightarrow\; a \text{ is a unit}, \qquad |a| < 1 \iff a \in \mathfrak{m}.$$

$|a-b|$ is a metric on R, and the local ring R is **complete** if it is complete with respect to this metric. The examples above are complete, except for $\mathcal{O}_a$ and $\mathbb{C}\{t\}$.

Hensel's Lemma

Completeness is not "first-order", but it implies a powerful scheme of first-order properties:

Hensel's Lemma. *Let R be a* complete *local ring, $f(X) \in R[X]$, and $a \in R$, such that $f(a) \in \mathfrak{m}$ and $f'(a) \notin \mathfrak{m}$. Then there is a unique $b \in R$ such that $f(b) = 0$ and $a - b \in \mathfrak{m}$.*

The assumption on $f(X)$ and a can also be expressed as: $|f(a)| < 1$ and $|f'(a)| = 1$. This might suggest its proof by *Newton approximation*; see picture. Formally:

$$f(a+x) \;=\; f(a) + f'(a)x + \text{higher powers of } x.$$

Take x such that $f(a) + f'(a)x = 0$, that is, $x = -f(a)/f'(a)$. Then $|x| = |f(a)| < 1$, and hence $|f(a+x)| \leqslant |f(a)|^2 < |f(a)|$. In this way we construct a sequence (a_n) with $a_0 = a$, $a_1 = a + x$, a_2 obtained from a_1 as a_1 was obtained from $a_0 = a$, and so on. Then (a_n) is a Cauchy sequence, so $a_n \to b$ in R as $n \to \infty$, and then $f(b) = 0$, $|a - b| < 1$.

Henselian local rings

A local ring R is said to be **henselian** if it has the property of Hensel's Lemma: for any $f(X) \in R[X]$ and any $a \in R$ with $f(a) \in \mathfrak{m}$ and $f'(a) \notin \mathfrak{m}$ there exists $b \in R$ such that $f(b) = 0$ and $a - b \in \mathfrak{m}$.

Exercise: show that such b is necessarily unique.

All the examples of local rings we mentioned are henselian, including the non-complete $\mathbb{C}\{t\}$.

Example of a local ring that is not henselian:

$$\boldsymbol{k}[t]_{(t)} \ := \ \{f(t)/g(t) : \ f(t), g(t) \in \boldsymbol{k}[t], \ g(0) \neq 0\} \ \subseteq \ \boldsymbol{k}[[t]]$$

Lifting the residue field

Theorem

Let R be a henselian local ring, $R \supseteq \mathbb{Q}$. Then R has a subfield that is mapped (isomorphically) onto the residue field $\boldsymbol{k}$ by the residue map $a \mapsto \mathrm{res}(a) : R \to \boldsymbol{k}$.

Proof.

Let E be a subfield of R. Note that then the residue map $\mathrm{res} : R \to \boldsymbol{k}$ is injective on E. Suppose $\mathrm{res}(E) \neq \boldsymbol{k}$, and take $a \in R$ such that $\mathrm{res}(a) \notin \mathrm{res}(E)$.

Case 1: $\mathrm{res}(a)$ is transcendental over $\mathrm{res}(E)$. Then a generates a subfield $E(a)$ of R that properly extends E. (Exercise)

Case 2: $\mathrm{res}(a)$ is algebraic over $\mathrm{res}(E)$. Take monic $f(X) \in R[X]$ such that its image in $\boldsymbol{k}[X]$ is the minimum polynomial of $\mathrm{res}(a)$ over $\mathrm{res}(E)$. Then $f(a) \in \mathfrak{m}$ (clear) and $f'(a) \notin \mathfrak{m}$ (why?). Using that R is henselian, we get $b \in R$ such that $f(b) = 0$ and $\mathrm{res}(a) = \mathrm{res}(b)$. Then $E[b]$ is a subfield of R that properly extends E. □

An application

Theorem (Greenleaf, Ax & Kochen)

Let $f_1(X), \dots, f_m(X) \in \mathbb{Z}[X]$, $X = (X_1, \dots, X_n)$. Then for all sufficiently large primes p, every solution of $f_1(X) = \cdots = f_m(X) = 0$ in $\mathbb{F}_p$ can be lifted to a solution in $\mathbb{Z}_p$.

Proof.

The polynomials $f_1, \dots, f_m$ are given by terms in the language L of rings. Construct an L-sentence σ such that for every local ring R we have:

σ is true in $R \iff$ for all $x \in R^n$ with $f_1(x), \dots, f_m(x) \in \mathfrak{m}$ there exists $y \in R^n$ such that

$$f_1(y) = \cdots = f_m(y) = 0 \text{ and } x_1 - y_1, \dots, x_n - y_n \in \mathfrak{m}.$$

Lifting theorem: σ holds in all henselian local rings R with char $\boldsymbol{k} = 0$. Hence σ holds in all henselian local rings R with char $\boldsymbol{k} > N$, for a certain $N = N(f_1, \dots, f_m) \in \mathbb{N}$. So if $p > N$, every solution of $f_1 = \cdots = f_m = 0$ in $\mathbb{F}_p$ can be lifted to a solution in $\mathbb{Z}_p$. □

Valued Fields

A **valuation** on K is a map $v : K^\times \to \Gamma$ onto an ordered abelian group Γ such that for all $a, b \in K^\times$

- $v(a+b) \geqslant \min(va, vb)$ provided $a + b \neq 0$;
- $v(ab) = va + vb$.

We always extend v to all of K by setting $v0 = \infty > \Gamma$, so that the rules above are valid without exception. A **valued field** is a field together with a valuation on it.

Example: $K = \boldsymbol{k}((t^\Gamma))$, consisting of the formal series $f(t) = \sum_\gamma c_\gamma t^\gamma$ given by a function $\gamma \to c_\gamma : \Gamma \to \boldsymbol{k}$ with *well-ordered* support $\{\gamma : c_\gamma \neq 0\}$. Here the valuation $v : K^\times \to \Gamma$ is given by $v(f) = \min \operatorname{supp} f$. For $\Gamma = \mathbb{Z}$ this is the usual field $\boldsymbol{k}((t))$ of Laurent series over $\boldsymbol{k}$.

Other Example: $\mathbb{Q}_p := \operatorname{Frac}(\mathbb{Z}_p)$, the field of p-adic numbers. Every nonzero element of $\mathbb{Z}_p$ is uniquely of the form $p^n \cdot (\text{unit of } \mathbb{Z}_p)$, so every nonzero element of $\mathbb{Q}_p$ is uniquely of the form $p^k \cdot (\text{unit of } \mathbb{Z}_p)$ with $k \in \mathbb{Z}$, and we set $v_p(a) = k$ for $a = p^k \cdot (\text{unit of } \mathbb{Z}_p)$. This is the p-adic valuation $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$.

Valued fields, continued

Both for $\boldsymbol{k}((t))$ and $\mathbb{Q}_p$ the valuation relates to the norm that we imposed on $\boldsymbol{k}[[t]]$ and $\mathbb{Z}_p$ (with these norms extended to their fraction fields by $|a/b| := |a|/|b|$):

$$|x| \leqslant |y| \iff vx \geqslant vy$$

Let $v : K^\times \to \Gamma$ be a valuation. Then $\mathcal{O}_v := \{a : \ va \geqslant 0\}$ is a subring of K with $\mathcal{O}_v^\times = \{a : \ va = 0\}$ and whose nonunits are the a with $va > 0$. Thus $\mathcal{O}_v$ is a local ring with maximal ideal $\mathfrak{m}_v = \{a : \ va > 0\}$. We can reconstruct v basically from $\mathcal{O}_v$, since v induces an isomorphism $K^\times/\mathcal{O}_v^\times \cong \Gamma$ of ordered groups, with the ordering on $K^\times/\mathcal{O}_v^\times$ given by

$$a\mathcal{O}_v^\times \geqslant b\mathcal{O}_v^\times \iff a/b \in \mathcal{O}_v$$

We call $\mathcal{O}_v$ the *valuation ring of* v. In general, a **valuation ring of a field** K is a subring $\mathcal{O}$ of K such that for all $a \in K^\times$, either $a \in \mathcal{O}$ or $a^{-1} \in \mathcal{O}$. In that case, $\mathcal{O} = \mathcal{O}_v$ for some valuation v on K, which by the above is unique up to an ordered group isomorphism.

Valued fields, continued

Alternative definition of a valued field: a field together with a valuation ring of the field.

Examples: the valuation ring of the Laurent series field $\boldsymbol{k}((t))$ is $\boldsymbol{k}[[t]]$. More generally, the valuation ring of $\boldsymbol{k}((t^\Gamma))$ consists of the series $\sum_{\gamma\geqslant 0} c_\gamma t^\gamma$. The valuation ring of $\mathbb{Q}_p$ is $\mathbb{Z}_p$.

Ideology of valuation theory: given a valuation $v : K^\times \to \Gamma$, try to understand K in terms of two structures that are in general simpler: the residue field $\boldsymbol{k}_v = \mathcal{O}/\mathfrak{m}_v$, and the value group Γ.

AKE: this ideology works perfectly if $\mathcal{O}_v$ is henselian and $\text{char}(\boldsymbol{k}_v) = 0$.

Let K be a valued field with residue field $\boldsymbol{k}$. Then $(\text{char}\, K, \text{char}\, \boldsymbol{k})$ can take the values

$$
\begin{aligned}
&(0,0), && \text{for } K = \boldsymbol{k}((t^\Gamma)) \text{ with char } \boldsymbol{k} = 0,\\
&(0,p), && \text{for } K = \mathbb{Q}_p,\\
&(p,p), && \text{for } K = \boldsymbol{k}((t^\Gamma)) \text{ with char } \boldsymbol{k} = p.
\end{aligned}
$$

Valued fields, exercises

Let K be a valued field with valuation ring $\mathcal{O}$, residue field $\boldsymbol{k}$ and value group Γ.

Exercises. Show the following:

1. if E is a subfield of K, then $\mathcal{O} \cap E$ is a valuation ring of E;
2. $\mathcal{O}$ is integrally closed in K, that is, if $x \in K$ and $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ with $a_1, \ldots, a_n \in \mathcal{O}$, then $x \in \mathcal{O}$;
3. if K is algebraically closed, then $\boldsymbol{k}$ is algebraically closed, Γ is divisible, that is, $n\Gamma = \Gamma$ for all $n \geqslant 1$, and $\mathcal{O}$ is henselian. (Converse holds if char $\boldsymbol{k} = 0$.)

Open and closed balls. Let K be a valued field and $v : K^\times \to \Gamma$ its valuation.

$B_a(\gamma) := \{x : \ v(x-a) > \gamma\}$ is the *open* ball centered at a with valuation radius γ;

$\bar{B}_a(\gamma) := \{x : \ v(x-a) \geqslant \gamma\}$ is the *closed* ball centered at a with valuation radius γ.

The open balls form a basis for the **valuation topology** of K, making K a topological field. NB: all balls are open and closed, and $\bar{B}_a(\gamma)$ is *not* the closure of $B_a(\gamma)$.

Key fact: for any two balls B_1 and B_2, if $B_1 \cap B_2 \neq \emptyset$, then $B_1 \subseteq B_2$ or $B_2 \subseteq B_1$.

Valued fields, more exercises

Note that $\mathcal{O}$ is the closed ball centered at 0 with valuation radius 0, and that its maximal ideal is the open ball centered at 0 with valuation radius 0.

Exercises. Show the following (with the valuation topology on $\mathbb{Q}_p$):

1. $\mathbb{Z}_p \cap \mathbb{Q} = \{k/n : \ k \in \mathbb{Z}, \ n \geqslant 1, \ p \text{ does not divide } n\}$;
2. the valuation rings of $\mathbb{Q}$ different from $\mathbb{Q}$ are exactly the above $\mathbb{Z}_p \cap \mathbb{Q}$;
3. $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$;
4. $\mathbb{Z}_p$ is a compact subset of $\mathbb{Q}_p$, and thus $\mathbb{Q}_p$ is locally compact;
5. if the valued field K is a locally compact, then $\mathcal{O}$ is compact, $\boldsymbol{k}$ is finite, and the value group is isomorphic to $\mathbb{Z}$.
6. $\mathbb{Z}_p = \{a \in \mathbb{Q}_p : \ 1 + pa^2 = b^2 \text{ for some } b \in \mathbb{Q}_p\}$ (p odd);
7. the only ring endomorphism of $\mathbb{Q}_p$ is the identity.

Valued field extensions

Let K and K' be valued fields with valuation rings $\mathcal{O}$ and $\mathcal{O}'$. Call K a **valued subfield of K'** (notation: $K \subseteq K'$), if K is a subfield of K' and $\mathcal{O} = \mathcal{O}' \cap K$; in that case we also call K' a **valued field extension of K**.

Assume $K \subseteq K'$. Then we have an induced field embedding $\boldsymbol{k} \to \boldsymbol{k}'$ of the residue fields, as well as an induced ordered group embedding $\Gamma \to \Gamma'$ of the value groups, where $\Gamma = K^\times/\mathcal{O}^\times$ and $\Gamma' = K'^\times/\mathcal{O}'^\times$. Identify $\boldsymbol{k}$ with a subfield of $\boldsymbol{k}'$ via this embedding! Likewise, identify Γ with a subgroup of Γ'.

A valued field extension $K \subseteq K'$ is said to be **immediate** if $\boldsymbol{k} = \boldsymbol{k}'$ and $\Gamma = \Gamma'$.

Examples of immediate and non-immediate extensions:

- the extension $\boldsymbol{k}(t) \subseteq \boldsymbol{k}((t))$ is immediate;
- the extension $\mathbb{C}\{t\}[t^{-1}] \subseteq \mathbb{C}((t))$ is immediate;
- $\mathbb{R}((t)) \subseteq \mathbb{C}((t))$ is not immediate;
- $\boldsymbol{k}((t)) \subseteq \boldsymbol{k}((t^{1/2})) := \boldsymbol{k}((t^{\mathbb{Z}/2}))$ is not immediate.