Introduction to (the model theory of) valued fields

Franziska Jahnke*

12.-16.09.2022

The aim of these lectures is to provide an introduction to valued fields and semi-algebraic sets, with a particular view towards model-theoretic methods. The lectures were given at the *Summer School on Motivic Integration* which took place in September 2022 at the HHU Düsseldorf.[1]

Contents

*Notes taken by Simone Ramello

[1]Many thanks to the organizers!

1 Lecture 1

1.1 Valued fields

Definition 1.1.1. *A valuation on a field* K *is a map* $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$*, where* $(\Gamma, +, \leqslant)$ *is an ordered abelian group (oag)*[2]*, such that*

1. $v(x) = \infty \iff x = 0$,
2. $v(xy) = v(x) + v(y)$,
3. $v(x + y) \geqslant \min\{v(x), v(y)\}$.

Remark 1.1.2. *If* $|\cdot|\colon K \to \mathbb{R}_{\geqslant 0}$ *is an ultrametric absolute value, then fixing any* $b \in \mathbb{R}_{>1}$ *gives rise to a valuation via* $v(x) := -\log_b(|x|)$*. In this case, we have* $v(K^\times) \subseteq \mathbb{R}$*.*

Example 1.1.3 (Examples or ordered abelian groups).

- *Any subgroup* $(\Gamma, +) \leqslant (\mathbb{R}, +)$ *is an oag, with the order being induced by the (unique) order on* $\mathbb{R}$*. We call these rank 1 (they have no non-trivial convex subgroup).*
- *Given two oags* Γ *and* Δ*, the lexicographic product* $\Gamma \oplus_{\text{lex}} \Delta$ *is given by component-wise addition on* $\Gamma \times \Delta$ *with the lexicographic ordering* $<_{\text{lex}}$*: for any* $\gamma, \gamma' \in \Gamma$ *and* $\delta, \delta' \in \Delta$*, define*
$$(\gamma, \delta) \leqslant_{\text{lex}} (\gamma', \delta') \iff \gamma < \gamma' \text{ or } (\gamma = \gamma' \text{ and } \delta \leqslant \delta')$$
One (explicit) example is $\mathbb{Z} \oplus_{\text{lex}} \mathbb{Z}$*. If* Γ *and* Δ *are nontrivial, the lexicographic sum does not have rank 1:* $\{0\} \oplus_{\text{lex}} \Delta$ *is a non-trivial convex subgroup.*

Example 1.1.4 (Examples of valued fields).

- *Any field with* $\Gamma = \{0\}$ *with* $v(K^\times) = \{0\}$ *and* $v(0) = \infty$*. This is called the trivial valuation.*
- *The p-adic valuation* v_p *on* $\mathbb{Q}$*: for* $x \in \mathbb{Q}^\times$*, write* $x = p^n \frac{c}{d}$ *with* $c, d \in \mathbb{Z}$*,* $p \nmid c, d$*. Then* $v_p(x) = n \in \mathbb{Z}$*.*
- *The p-adic valuation on the field of* p*-adics* $\mathbb{Q}_p$*: consider* $\mathbb{Q}_p := \{\sum_{i \geqslant m} a_i p^i \mid m \in \mathbb{Z}, a_i \in \{0, 1, \ldots p-1\}\}$ *with carry-over on sum and multiplication. Define*
$$v_p(\sum_{i \geqslant m} a_i p^i) = \min\{i \mid a_i \neq 0\}.$$
We will see that this coincides on $\mathbb{Q}$ *with* v_p *as defined in the bullet point above.*
- *The power series valuation* v_t *on a power series field: Consider* $K = k((t))$*. Write* $v_t(\sum_{i \geqslant m} a_i t^i) := \min\{i \mid a_i \neq 0\}$*.*
- *Note that so far, all of our examples had rank 1 (indeed,* $\mathbb{Z}$*) value groups. More generally, let* $K = k((\Gamma)) := \{\sum_{\gamma \in \Gamma} a_\gamma t^\gamma \mid \{\gamma \mid a_\gamma \neq 0\}$ *is well-ordered*$\}$*. Write* $v_\Gamma(\sum_\gamma a_\gamma t^\gamma) := \min\{\gamma \mid a_\gamma \neq 0\}$*.*

[2] that is, an abelian group with a total order such that $+$ and $\leqslant$ are compatible

1.2 Basic properties and associated quantities

We will often write νK for the value group Γ of (K, ν). Here is a list of basic properties:

1. $\nu(1) = 0$: indeed, $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$,

2. $\nu(x) = \nu(-x) = -\nu(x^{-1})$ for all $x \in K$: note first that $0 = \nu(1) = \nu(-1) + \nu(-1)$, so (as ordered abelian groups are torsion-free), we have $\nu(-1) = 0$. The rest now follows immediately from the axioms for valuations.

3. $\nu(x) < \nu(y)$ implies that $\nu(x+y) = \min\{\nu(x), \nu(y)\} = \nu(x)$: indeed, if $\nu(x+y) > \nu(x)$ then $\nu(x) = \nu(x+y-y) \geqslant \min\{\nu(x+y), \nu(-y)\} = \min\{\nu(x+y), \nu(y)\} > \nu(x)$, a contradiction.

Using these properties, it is easy to verify that the p-adic valuation we defined on $\mathbb{Q}$ and the restriction of the p-adic valuation we defined on $\mathbb{Q}_p$ coincide on $\mathbb{Q}$: by property 2 above, it suffices to show that they coincide on any $n \in \mathbb{N} \setminus \{0\}$. Writing n base p, we get a finite p-adic expansion

$$n = a_0 p^0 + \ldots a_m p^m$$

(for some $m \leqslant n$) and we get $\min\{i \mid a_i \neq 0\} = \max\{j \mid p^j \mid n\}$.

Remark 1.2.1. *Any valued fields comes naturally with the following structure:*

- $\mathcal{O}_\nu := \{x \in K \mid \nu(x) \geqslant 0\}$ *is a valuation ring of* K*, i.e. for every* $x \in K$ *we have* $x \in \mathcal{O}_\nu$ *or* $x^{-1} \in \mathcal{O}_\nu$*,*

- $\mathcal{O}_\nu$ *has a unique maximal ideal,* $\mathfrak{m}_\nu := \{x \in K \mid \nu(x) > 0\}$*, as* $\mathfrak{m}_\nu = \mathcal{O}_\nu \setminus \mathcal{O}_\nu^\times$

- *the quotient* $K\nu := \mathcal{O}_\nu / \mathfrak{m}_\nu$ *is called the residue field of* (K, ν)*.*

Example 1.2.2. *We work out the valuation ring, maximal ideal and residue field for each of the valued fields discussed in example 1.1.4:*

1. *trivial valuation on* K*:* $\mathcal{O}_\nu = K$, $\mathfrak{m}_\nu = \{0\}$, $K\nu = K$,

2. p*-adic valuation on* $\mathbb{Q}$*:* $\mathcal{O}_{\nu_p} := \{c/d \in \mathbb{Q} \mid (c, d) = 1, d \neq 0, p \nmid d\} = \mathbb{Z}_{(p)}$, $\mathfrak{m}_{\nu_p} = p\mathbb{Z}_{(p)}$, $K\nu = \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$,

3. p*-adic valuation on* $\mathbb{Q}_p$*:* $\mathcal{O}_{\nu_p} := \{\sum_{i \geqslant 0} a_i p^i \mid a_i \in \{0, \ldots p-1\}\} = \mathbb{Z}_p$ *(i.e., the ring of* p*-adic integers), with maximal ideal* $\mathfrak{m}_{\nu_p} = p\mathcal{O}_{\nu_p}$*; similarly,* $K\nu \simeq \mathbb{F}_p$,

4. *power series: for* $K = k((\Gamma))$*, we get* $\mathcal{O}_\nu = k[\![\Gamma]\!]$ *and* $K\nu = k$*.*

1.3 Topology and Haar measure

We now take a step aside to introduce the Haar measure on the p-adic numbers.

Definition 1.3.1. *For* $\gamma \in \Gamma$, $y \in K$*, we define*

1. $B_{>\gamma}(y) := \{x \in K \mid \nu(x-y) > \gamma\}$*, the* open ball of radius γ around y,

2. $B_{\geqslant\gamma}(y) := \{x \in K \mid \nu(x-y) \geqslant \gamma\}$*, the* closed ball of radius γ around y.

Note that we have $B_{>0}(0) = \mathfrak{m}_\nu \subset B_{\geqslant 0}(0) = \mathcal{O}_\nu$.

Lemma 1.3.2. *By the ultrametric inequality, for any two balls* B_1 *and* B_2 *we either have* $B_1 \subseteq B_2$, $B_2 \subseteq B_1$ *or* $B_1 \cap B_2 = \varnothing$.

Proof. Indeed, given any ball $B_{\geqslant\gamma}(y)$ and any c in this ball, $B_{\geqslant\gamma}(c) = B_{\geqslant\gamma}(y)$: for any $x \in B_{\geqslant\gamma}(y)$, we have $\nu(x-c) = \nu(x-y+y-c) \geqslant \min\{\nu(x-y), \nu(y-c)\} \geqslant \gamma$. This gives one inclusion. The other is symmetric. The same argument works for open balls. $\square$

As a consequence, open (respectively, closed) balls form a neighbourhood base of an Hausdorff field topology τ_ν on K. Indeed, the naming 'open' and 'closed' is just suggestive: $K \setminus B_{>\gamma}(y) = \bigcup_{\nu(b-y)<\gamma} B_{>\nu(b-y)}(b)$ hence $B_{>\gamma}(y)$ is also closed, so it is a clopen; similarly for 'closed' balls. In particular, the topology generated by the open balls coincides with that generated by the closed balls.

Exercise 1.3.3. *Show that* τ_ν *is discrete if and only if* ν *is the trivial valuation.*

Remark 1.3.4. *With respect to* τ_{ν_p}, $\mathbb{Q}_p$ *is locally compact: indeed,* $\mathbb{Z}_p$ *is compact (the rest follows from translations), which can be seen as either because of the isomorphism* $\mathbb{Z}_p \simeq \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} \subseteq_{\text{closed}} \prod_n \mathbb{Z}/p^n\mathbb{Z}$ *(and the latter is compact by Tychonov's theorem as its a product of compact spaces since each* $\mathbb{Z}/p^N\mathbb{Z}$ *is finite) or because* $\mathbb{Z}_p$ *is complete and totally bounded. In both of these arguments, the fact that* $K\nu$ *is finite plays an important role. If* $K\nu$ *is infinite,* τ_ν *is not locally compact, as* $\mathcal{O}_\nu := \bigsqcup_{r\in R}(r + \mathfrak{m}_\nu)$ *with* $R \subseteq \mathcal{O}_\nu^\times$ *a system of representatives for* $K\nu$ *will not admit a finite open subcover.*

For a topological space τ, we use $\mathcal{B}$ to denote the collection of *Borel sets*, that is the σ-algebra[3] generated by the open sets.

For τ a group topology on $(G, \cdot)$, $S \subseteq G$ and $g \in G$, we use

$$g \cdot S = \{g \cdot s \mid s \in S\}$$

to denote the left translate of S. Note that if S is Borel, then $g \cdot S$ is also Borel.

Definition 1.3.5. *Let* $(G, \cdot, \tau)$ *be a topological group. A* Borel measure μ *on* G *is a measure on* G *that is defined on* $\mathcal{B}$. *A Borel measure is called* regular *if all of the following conditions hold:*

- $\mu(C) < \infty$ *for all compact sets* C
- $\mu(U) = \sup\{\mu(C) \mid C \subseteq U,\ C$ *compact*$\}$ *for any* $U \subseteq G$ *open*
- $\mu(A) = \inf\{\mu(U) \mid A \subseteq U,\ U$ *open*$\}$ *for any* $A \in \mathcal{B}$

Theorem 1.3.6 (Haar). *Any locally compact, Hausdorff topological group admits a* Haar measure, *i.e., a left-invariant regular non-zero Borel measure* μ. *If* μ' *is another such measure, then there is* $\alpha \in \mathbb{R}$ *such that* $\mu = \alpha \cdot \mu'$.

Note that if μ is a Haar measure on G, then so is $\alpha \cdot \mu$ for any $\alpha \in \mathbb{R}_{>0}$. As $\mathbb{Z}_p$ is compact (and hence has finite measure with respect to any Haar measure on $\mathbb{Q}_p$), we may fix the unique Haar measure μ such that $\mu(\mathbb{Z}_p) = 1$. Then, we get $\mu(p\mathbb{Z}_p) = \frac{1}{p}$, and for any $y \in K$ and $\gamma \in \mathbb{Z}$ we have $\mu(B_{\geqslant\gamma}(y)) = \frac{1}{p^\gamma}$ and $\mu(B_{>\gamma}(y)) = \frac{1}{p^{\gamma+1}}$.

[3] Recall that a σ-algebra is closed under countable unions, countable intersections and complements

Exercise 1.3.7. *Verify that*

$$\mu(\{b \in \mathbb{Z}_p : 3 \mid \nu_p(b)\} = \frac{1 - 1/p}{1 - (1/p)^3}$$

holds.

2 Lecture 2

2.1 Semi-algebraic sets

Throughout the section, let (K, ν) be a valued field.

Definition 2.1.1.
- *A subset* $A \subseteq K^n$ *is called* semi-algebraic *if* A *is a finite Boolean combination of sets given by polynomial equalities (i.e. equalities of the form* $f(x) = 0$, $f \in K[x_1, \dots x_n]$*) and valuation inequalities (i.e. inequalities of the form* $\nu(g_1(x)) \geqslant \nu(g_2(x))$, $g_1, g_2 \in K[x_1, \dots x_n]$*).*
- *A subset* $A \subseteq K^n$ *is called* constructible *if* A *is a finite Boolean combination of sets given by polynomial equalities.*

In particular, constructible sets are semi-algebraic.

Example 2.1.2. *A subset* $A \subseteq K^1$ *constructible iff* A *cofinite or finite. On the other hand,* $A \subseteq K^1$ *semi-algebraic iff* A *is a Boolean combination of singletons and balls (exercise!).*

The following theorem was proved independently by Tarski and Chevalley (albeit in very different formulations and with rather different proofs).

Theorem 2.1.3 (Tarski/Chevalley)**.** *If* K *is algebraically closed, then any projection* pr: $K^n \to K^i$ *(for* $n \geqslant i$*) of a constructible subset of* K^n *is a constructible subset of* K^i*.*

Remark 2.1.4. *The theorem above holds precisely in finite and in algebraically closed fields; e.g. in* $K = \mathbb{R}$ *you can project* $x^2 - y = 0$ *to the positive reals, which are not constructible.*

Our next big aim will be to approach the following theorem model-theoretically:

Theorem 2.1.5 (A. Robinson)**.** *Let* (K, ν) *a valued field such that* K *is algebraically closed. Then, the projection of any semi-algebraic set is semi-algebraic.*

2.2 First attempt at first-order logic

Definition by example: the language of rings, $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$. The language of ordered abelian groups $\mathcal{L}_{\text{oag}} = \{0, +, -, \leqslant\}$. The language of ordered monoids $\mathcal{L}_{\text{oag}}^+ = \{0, +, -, \leqslant, \infty\}$.

Definition 2.2.1. *A first-order language* $\mathcal{L}$ *is given by*

1. *a set of constant symbols* $\{c_i \mid i \in I\}$*, e.g.* 0, 1, ∞,
2. *a set of function symbols* $\{f_j \mid j \in J\}$*, each with a fixed arity, e.g.* $+$ *and* $\cdot$ *of arity* 2 *and* $-$ *of arity* 1,

3. *a set of relation symbols* $\{R_k \mid k \in K\}$*, each with a fixed arity, e.g.* $\leqslant$ *of arity* 2*,*

4. *a binary relation* $=$*, a fixed set of variables* $\{v_i \mid i \in \mathbb{N}\}$*,*

5. *connectives* $\wedge, \vee, \neg, \to, \longleftrightarrow$*,*

6. *quantifiers* $\forall$ *and* $\exists$*.*

An $\mathcal{L}$-structure consists of nonempty set together with interpretation for each of the symbols. In particular, any unitary ring is naturally an $\mathcal{L}_{\text{ring}}$-structure, with the symbols interpreted in the obvious way.

$\mathcal{L}$-formulas are built "in the obvious way", such that if you plug something into the variables that are not under the influence of a quantifier, you should get a statement that is either true or false. Again, definition by example: in the language of rings,

1. $\exists y(y \cdot y = x)$ makes sense,

2. $y^2 := y \cdot y$ does not make sense (in fact, it is a term, not a formula).

Definition 2.2.2. *A formula is quantifier-free if no quantifiers occur.*

Example 2.2.3. *Quantifier-free* $\mathcal{L}_{\text{ring}}$*-formulas are precisely finite Boolean combinations of formulae of the form* $f(\bar{x}) = 0$*, for* $f \in \mathbb{Z}[x_1, \dots x_n]$*.*

Remark 2.2.4. *If* K *is a field, then quantifier-free* $\mathcal{L}_(K)$*-formulae (that is,* $\mathcal{L}_{\text{ring}}$*-fomulas where one additionally allows constants for the elements of* K*) define constructible sets, and viceversa.*

Theorem 2.2.5. *(Tarski) If* K *is algebraically closed, let* T *be the* $\mathcal{L}$*-theory saying "*K *is a field" and "every polynomial of degree* n *has a root in* K*", for* $n \geqslant 2$*; then* T *eliminates quantifiers.*

Definition 2.2.6. *A theory*[4] T *eliminates quantifiers if for every* $\mathcal{L}$*-formula* $\phi(\bar{x})$ *there is a quantifier-free* $\mathcal{L}$*-formula* $\psi(\bar{x})$ *such that* $T \vdash \forall x(\phi(x) \longleftrightarrow \psi(x))$*, i.e. in all models of* T *the two formulae define the same set.*

Proof. (Sketch: why Chevalley and Tarski morally say the same thing) Enough to check $\phi(\bar{x}) \equiv \exists z \tilde{\phi}(\bar{x}, z)$ is equivalent to a quantifier-free formula. Then $\tilde{\phi}(\bar{x}, z)$ defines a constructible subset of K. Then $\mathrm{pr}_{\bar{x}}(\tilde{\phi}(\bar{x}, z))$ is constructible, which gives the desired qf-formulae equivalent to $\phi(\bar{x})$. □

2.3 Ordered abelian groups of higher rank occur naturally in model theory

Theorem 2.3.1. *(Compactness) If* T *is an* $\mathcal{L}$*-theory, and every finite subset of* T *has a model, then* T *has a model.*

As a consequence, if $\Gamma \neq \{0\}$ is an ordered abelian group in $\mathcal{L}_{\text{oag}}$, then there is $\Gamma^* \equiv \Gamma$ (i.e. the same $\mathcal{L}_{\text{oag}}$-sentences hold in Γ and Γ^*) such that Γ^* has a non-trivial convex subgroup. Indeed, consider $\mathcal{L}' = \mathcal{L}_{\text{oag}} \cup \{c, c'\}$ and the $\mathcal{L}'$-theory given by

$$T = \mathrm{Th}_{\mathcal{L}_{\text{oag}}}(\Gamma) \cup \{n \cdot c' < c) \mid n \in \mathbb{N}\}.$$

[4]A theory T is a set of $\mathcal{L}$-sentences (formulae without free variables). Intuitively, a theory is a set of axioms, and models are structures where these axioms hold. For example, the field axioms form an $\mathcal{L}_{\text{ring}}$-theory, with models being precisely all fields.

Every finite subsets of T has a model (it is finitely satisfiable in Γ!) and this gives you an element c' whose convex hull is a proper subgroup.

Even if we are only interested in valued fields with rank-1 value group, for a model-theoretic study, we will have to consider value groups of higher rank!

3 Lecture 3

3.1 Second attempt at first-order logic

Goal: capture $v\colon K \twoheadrightarrow \Gamma \cup \{\infty\}$ model theoretically.

We will work with $\mathcal{L}_\Gamma$, a two-sorted language with one sort for K and one for $\Gamma \cup \{\infty\}$. On K, we have the language of rings $\{0, 1, +, \cdot, -\}$; on $\Gamma \cup \{\infty\}$, we have the language $\{0, +, \leqslant, \infty\}$; we have a function symbol $v\colon K \to \Gamma \cup \{\infty\}$ between the sorts. Variables come attached with a sort, and quantifiers only run over a sort.

Definition 3.1.1. *We will call* ACVF *the $\mathcal{L}_\Gamma$-theory given by,*

1. $K \vDash$ ACF, *i.e.*, K *is algebraically closed,*
2. $v\colon K \to \Gamma \cup \{\infty\}$ *is a non-trivial valuation (in particular,* $\Gamma \vDash$ OAG*).*

Remark 3.1.2. *If* $(K, v) \vDash$ ACVF, *then*

1. Γ *is divisible: indeed, if* $n > 0$ *and* $\gamma \in \Gamma$, *say* $\gamma = v(a)$ *for some* $a \in K$, *then* $x^n - a$ *has a root* b *in* K, *and then* $v(a) = v(b^n) = nv(b)$,
2. Kv *is algebraically closed: indeed, if we take* $P(X) = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathcal{O}_v[X]$, *then all roots of* P *lie in* $\mathcal{O}_v$. *Otherwise, if* $v(b) < 0$ *then for all* $i < n$, $v(b^i) < 0$, *so*
$$nv(b) < iv(b) \leqslant \underbrace{v(a_i)}_{\geqslant 0} + iv(b)$$
and thus $v(P(b)) = nv(b) < 0$. *Thus,* $\mathrm{res}(P) = X^n + \sum_{i=0}^{n-1} \mathrm{res}(a_i) X^i$ *splits in* Kv.

The converse does not hold, the problem arises through immediate extensions. For the converse to hold, one needs to assume further that (K, v) *satisfies Hensel's Lemma and is defectless.*

Theorem 3.1.3. *(A. Robinson, Weispfenning)* ACVF *eliminates quantifiers in* $\mathcal{L}_\Gamma$.

3.2 Quantifier elimination

The key step for Robinson's theorem is the following embedding lemma:

Lemma 3.2.1. *Let* M *and* N *be models of* ACVF *and let* $A \subseteq M$ *be an* $\mathcal{L}_\Gamma$*-substructure. Assume* N *is* $|M|^+$*-saturated. Then any* $\mathcal{L}_\Gamma$*-embedding* $f\colon A \to N$ *extends to an* $\mathcal{L}_\Gamma$*-embedding* $g\colon M \to N$.

If you don't like saturation: you can prove the lemma under the assumption that N is $|M|^+$-spherically complete (that is: in N, every nested sequence of $|M|$-many balls is non-empty). One then proves quantifier elimination by a back-and-forth argument.

Theorem 3.2.2. *(Macintyre, McKenna, van den Dries)*

1. *If* K *is infinite, and* $\mathrm{Th}(K)$ *eliminates quantifiers in the language of rings, then* K *is algebraically closed.*

2. *If* (K, ν) *eliminates quantifiers, and* ν *is non-trivial, then* $(K, \nu) \models \mathrm{ACVF}$.

3.3 What about the p-adics or $\mathbb{C}((t))$?

Consider $P_n(X) \equiv \exists Y(Y^n = X)$.

Lemma 3.3.1. *For every* $n \geqslant 2$, $P_n(\mathbb{Q}_p)$ *is not semi-algebraic.*

Proof. Assume $P_n(\mathbb{Q}_p)$ is semi-algebraic. Then $\mathbb{Q}_p \setminus P_n(\mathbb{Q}_p)$ is also semi-algebraic. Note that if $P_n(\mathbb{Q}_p)$ does not contain a ball around 0, then there would be a "punctured" ball around 0 in the complement.

In particular, there is B around 0 such that either $B \subseteq P_n(\mathbb{Q}_p)$ or $B \setminus \{0\} \subseteq P_n(\mathbb{Q}_p)^c$. This means that, for example, there is γ such that $\nu(x) \geqslant \gamma \implies x \in P_n(\mathbb{Q}_p)$. However, $p^{n\gamma+1}$ has valuation $\geqslant \gamma$ but it is not an n-th power. Similarly for the second case (since $n \div \nu_p(p^n)$). In other words, any ball B around 0 must intersect both $P_n(\mathbb{Q}_p)$ and $P_n(\mathbb{Q}_p)^c$. $\square$

Note that by substituting p with t, we obtain the same result in $\mathbb{C}((t))$.

Nonetheless, using these P_n's, we still obtain control over the definable sets:

Theorem 3.3.2 (Macintyre). *For each* $n \geqslant 1$, *let* $P_n(X)$ *denote a unary relation interpreted as* $P_n(X) \equiv \exists Y(Y^n = X)$. *Then the theory* $\mathrm{Th}(\mathbb{Q}_p)$ *eliminates quantifiers in the Macintyre language* $\mathcal{L}_{\mathrm{Mac}} = \mathcal{L}_{\mathrm{ring}} \cup \{P_n \mid n \geqslant 1\}$.

In other words, every definable set in the language of rings is equivalent — modulo $\mathrm{Th}(\mathbb{Q}_p)$ — to a Boolean combination of sets of the form $f(\bar{x}) = 0$ and $P_n(g(\bar{x}))$, for $f(\bar{x})$ and $g(\bar{x})$ polynomials over $\mathbb{Z}$. In particular, all definable sets in $\mathbb{Q}_p$ are Boolean combinations of sets of the form $f(\bar{x}) = 0$ and $P_n(g(\bar{x}))$, for $f, g \in \mathbb{Q}_p[X_1, \dots, X_m]$.

Theorem 3.3.3 (Folklore). *The same holds over* $\mathbb{C}((t))$.

BUT wait a moment, what happened to my semi-algebraic sets? Are they still definable?

3.4 Definability of valuations

Theorem 3.4.1 (Hensel's Lemma). *The valued fields* $(\mathbb{Q}_p, \nu_p)$ *and* $(\mathbb{C}((t)), \nu_t)$ *are* henselian, *i.e. given* $b \in \mathcal{O}_\nu$ *and* $f \in \mathcal{O}_\nu[X]$ *with* $f(b) \in \mathfrak{m}_\nu$, $f'(b) \notin \mathfrak{m}_\nu$, *then there is* $\beta \in \mathcal{O}_\nu$ *with* $f(\beta) = 0$ *and* $\beta - b \in \mathfrak{m}_\nu$.

Proof. By Newton approximation. Choose $a_0 = b$ and define a sequence $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. It is a Cauchy sequence with respect to the p-adic (respectively, t-adic) metric. By completeness, a_n converges to some $\beta \in \mathcal{O}_\nu$ which is a root of f. $\square$

Theorem 3.4.2 (J. Robinson). *We can define* $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ *in the language of rings via* $\varphi_p(X) \equiv \exists Y(Y^2 = 1 + pX^2)$, *for* $p \neq 2$, *and via* $\varphi_2(X) \equiv \exists Y(Y^3 = 1 + pX^3)$ *in* $\mathbb{Q}_2$. *Similarly, we can define* $\mathbb{C}[\![t]\!] \subseteq \mathbb{C}((t))$ *via* $\varphi_t(X) \equiv \exists Y(Y^2 = 1 + tX^2)$.

In $\mathbb{Q}_p$, this implies that all closed balls are definable without parameters in the language of rings (note that $p = 1 + \ldots 1$). Since $\mathfrak{m}_v$ is then also definable without parameters (as $\mathfrak{m}_v = p\mathcal{O}_v$), all open balls are also definable. Note that we have $\varphi_p \equiv P_2(1 + pX^2)$ (resp. $\varphi_2 \equiv P_3(1 + pX^3)$), so $\mathbb{Z}_p$ and $\mathfrak{m}_v$ (and hence all balls) are indeed definable without quantifiers (and without parameters) in $\mathcal{L}_{\mathrm{Mac}}$.

Proof. (for $p \neq 2$ in $\mathbb{Q}_p$) Take any $b \in \mathbb{Q}_p$. We want to show that $b \in \mathbb{Z}_p \iff \exists Y(Y^2 = 1 + pb^2)$. First suppose that $v(b) < 0$: since $2 \nmid v(p)$, then $2 \nmid v(b^2 p) < 0$, so $v(b^2 p) = v(1 + b^2 p)$ is not divisible by 2, and thus $1 + b^2 p \notin P_2(\mathbb{Q}_p)$. Vice versa, suppose $b \in \mathcal{O}_v$ and consider $f(Y) = Y^2 - 1 - b^2 p$. This is a polynomial over $\mathbb{Z}_p$ and we have $f(1) \in p\mathbb{Z}_p$, $f'(1) = 2 \notin p\mathbb{Z}_p$. By henselianity, we get $\beta \in \mathbb{Z}_p$ such that $f(\beta) = 0$, i.e. $\beta^2 = 1 + b^2 p$. □

In $(\mathbb{C}((t)), v_t)$, the formula $\varphi_t(X)$ used a parameter for t. This is however not necessary:

Theorem 3.4.3 (Ax)**.** *Let K be a field with $\mathrm{char}(K) \neq 2$. In $(K((t)), v_t)$, the valuation ring $\mathcal{O}_v$ is defined by the (parameter-free) $\mathcal{L}_{\mathrm{ring}}$-formula*

$$\Phi(X) \equiv \exists W, Y \forall U, X_1, X_2 \exists Z \forall Y_1, Y_2\, [(Z^2 = 1 + WX_1^2 X_2^2 \vee Y_1^2 \neq 1 + WX_1^2 \vee Y_2^2 \neq 1 + WX_2^2) \wedge U^2 \neq W \wedge Y^2 = 1 + WX^2].$$

The formula $\Phi(X)$ takes the union over all $\varphi(X, a) \equiv \exists Y\ (Y^2 = 1 + aX^2)$ for $a \in K((t))$, provided that a is not a pth power and that $\varphi(X, a)$ is closed under multiplication.

Thus, one can deduce that all balls in $\mathbb{C}((t))$ are again definable without quantifiers (and without parameters) in $\mathcal{L}_{\mathrm{Mac}}$.

4 Some literature for further reading

4.1 Model theory

1. Tent, Ziegler — *A course in model theory*
2. Hils, Loeser — *A first journey through logic*
3. Marker — *Model theory: an introduction*

4.2 Model theory of valued fields

1. van den Dries — *Lectures on the model theory of valued fields* (chapter in *Model theory in algebra, analysis and arithmetic*)
2. Hils — *Model theory of valued fields* (chapter in *Lectures in model theory*, see also the previous chapter Jahnke — *An introduction to valued fields* in the same volume)

4.3 Model theory of the p-adics

1. Prestel, Roquette — *Formally p-adic fields*
2. Macintyre's original paper