p-adically closed fields: *a p-anoramic tour*

Simone Ramello

Galois seminar – 21/12/2022

Contents

Warning 0.1. This is gonna be a *panoramic* tour, like the kind you get from a bus that goes around in a city, briefly stopping every now and then, but never letting you off the vehicle. This means that there will be little to no proofs, and you are gonna have to believe some definitions by example.

Our goal today is understanding the p-adic numbers from a model theoretic point of view. The final goal of the seminar is, after all, completely characterizing the model theory of $\mathbb{Q}_p$ via its absolute Galois group. To do so, we will start off by looking for an algebraic characterization. However, we will soon realize that it is too strict of a characterization. We will have to relax it, and speak of *ramification* and $\mathbb{Z}$*-groups*.

As most of the participants don't really have a model theoretic background, a necessary stop will be model theory, or rather a *glimpse* into model theoretic questions and methods. After that, we will discover the hidden gem of this tour: a precise description of the complete theory of the p-adics numbers, or rather of the theory of p-adically closed fields. We will finish off with some consequences of this characterization, which will be important later in the seminar.

A sneaky peek: algebra-coloured glasses

We have already seen that the p-adic numbers arise as the *completion* of $\mathbb{Q}$ along a certain absolute value $|\cdot|_p$, defined as

$$|x|_p = p^{-v_p(x)},$$

where $v_p(x)$ is equal to the maximum N such that $p^N \mid x$, if $x \in \mathbb{Z}$, and is completely determined by the equation $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ if a and b are coprime integers. We are thus working with a *valued field* $(\mathbb{Q}_p, v_p)$ with *valuation ring*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\},$$

residue field of cardinality p (i.e., isomorphic to $\mathbb{F}_p$), and *value group* isomorphic to $\mathbb{Z}$. Moreover, the valuation of p is precisely $v_p(p) = 1$, the smallest positive element of $\mathbb{Z}$; no element divides p, and yet it vanishes in the residue field.

Any p-adic number can be presented in the form

$$a_{-N}p^{-N} + a_{-N+1}p^{-N+1} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots = \sum_{n \geq -N} a_n p^n,$$

where $\{a_n \mid n \geq -N\} \subseteq \mathbb{F}_p$, $a_{-N} \neq 0$ and $N \in \mathbb{N}$. This allows us to compute its valuation easily, as it is equal to $-N \in \mathbb{Z}$. Elements of $\mathbb{Z}_p$ are thus exactly those of the form

$$a_0 + a_1 p + a_2 p^2 + \ldots,$$

with a_0 possibly zero. Addition and multiplication on these series are performed by *carry-over*.

This allows us to give a first, tentative definition of what it means to be *like* $\mathbb{Q}_p$.

Definition 0.2 (*Tentative*). A valued field (K, v) is *algebraically like* $\mathbb{Q}_p$ if,

1. Kv has p elements,
2. $vK \simeq \mathbb{Z}$,
3. K is complete with respect to the corresponding absolute value $|x|_v := e^{-v(x)}$,
4. $v(p)$ is the smallest positive element of vK (i.e., $v(p) = 1$ under the isomorphism above).

This is both a very successful and a very boring characterization.

Theorem 0.3 (*See Serre, Local fields*). (K, v) is algebraically like $\mathbb{Q}_p$ if and only if $(K, v) \simeq (\mathbb{Q}_p, v_p)$.

1 First stop: a glimpse into model theory

We seek a characterization of $\mathbb{Q}_p$ that is both less strict and feasible from the point of view of model theory. What is model theory, again?

Model theorists deal in the *formal information* contained in mathematical objects. They (we?) are interested in what kind of properties of a certain mathematical structure we can encode in formulae built from a certain formal language. To see what I mean more precisely, let's go through some definitions by examples. **Warning:** necessarily, these will not be very precise, or cover every possible detail or case. If this makes you feel icky, you can find a more precise treatment of this on any model theory group, e.g. Tent-Ziegler.

Language. A language is a set of symbols, abstractly something of the form

$$\mathcal{L} = \underbrace{\{f_i \mid i \in I\}}_{\text{function symbols}} \cup \underbrace{\{R_j \mid j \in J\}}_{\text{relation symbols}} \cup \underbrace{\{c_k \mid k \in K\}}_{\text{constant symbols}}.$$

Each function symbol comes attached with an *arity* $n_i \in \mathbb{N}$, $i \in I$, and similarly for relation symbols with arity $m_j \in \mathbb{N}$, $j \in J$.

We will mainly think of $\mathcal{L}_{\text{vf}}$, the *language of valued fields*, which takes the form

$$\mathcal{L}_{\text{vf}} = \underbrace{\{+, \cdot, -, 0, 1\}}_{\text{language of rings}} \cup \underbrace{\{\mathcal{O}\}}_{\text{unary relation}}$$

where we think of the first symbols as representing the operations and elements of a ring (or a field), and the symbol $\mathcal{O}$ as representing a valuation ring. The symbols $+$ and $\cdot$ come attached with arity 2, the symbol $-$ with arity 1 and the symbol $\mathcal{O}$ with arity 1 (*unary* relation, or predicate). As the name suggest, this is the language that we will use to express properties of valued fields through ($\mathcal{L}_{\text{vf}}$-)formulae.

Formulae. Formulae in $\mathcal{L}_{\mathrm{vf}}$[1] are built recursively, starting from these two types of basic building blocks:

$$p(X_1, \dots X_n) = q(Y_1, \dots Y_m), \quad r(Z_1, \dots Z_\ell) \in \mathcal{O},$$

where p, q, r are some polynomials over $\mathbb{Z}$ in some sets of variables $X_1, \dots X_n, Y_1, \dots Y_m, Z_1, \dots Z_\ell$. For example,

$$X_1^2 + 3X_2 = 0, \;\; X_1X_2 - Y_1 + Z_1^5 \in \mathcal{O}.$$

These formulae express whether certain polynomials vanish, or whether they have non-negative valuation. Next, we compose these building blocks using *connectives* $\wedge$ (and), $\vee$ (or), $\rightarrow$ (implies), $\neg$ (not). For example,

$$(X_1^2 + 3X_2 = 0) \vee \neg(X_1X_2 - Y_1 + Z_1^5 \in \mathcal{O}),$$

or

$$(X_1X_2 - Y_1 + Z_1^5 \in \mathcal{O}) \rightarrow (X_1X_2 - Y_1 + Z_1^5 = 0).$$

We often turn $\neg$ into the obvious negated symbol, i.e. instead of $\neg(p(\bar{X}) = 0)$ we write $p(\bar{X}) \neq 0$, and instead of $\neg(q(\bar{Y}) \in \mathcal{O})$ we write $q(\bar{Y}) \notin \mathcal{O}$.

We are now expressing more complex relations between polynomials; if we were only working with polynomials equalities over $\mathbb{C}$, the so-called *Boolean* combinations would give rise precisely to *constructible subsets*.

Finally, we apply *quantifiers* $\forall$ (for all) and $\exists$ (exists). For example,

$$\forall X_1 \forall X_2 \forall Y_1 [(X_1^2 + 3X_2 = 0) \vee \neg(X_1X_2 - Y_1 + Z_1^5 \in \mathcal{O})],$$

or

$$\forall X_1 \forall X_2 \forall Y_1 \exists Z_1 [(X_1X_2 - Y_1 + Z_1^5 \in \mathcal{O}) \rightarrow (X_1X_2 - Y_1 + Z_1^5 = 0)].$$

We have now produced, by recursively iterating these steps, what we will call *formulae*. However, not all formulae are created equal: the first one I have written is different from the second in a crucial way, since the variable Z_1 does not appear quantified. Intuitively speaking, if we work in a certain valued field, we can determine the truth value of the second formula – perhaps it is a very hard problem (depending on the valued field in question), but it has a determined truth value. The truth value of the first one is not so clear: it might very well be that it depends on what we plug in Z_1's place. We shall call the formulae where all variables are quantified *sentences*. Sentences have a defined truth value when interpreted in *structures*.

Structures. Given a certain language

$$\mathcal{L} = \underbrace{\{f_i \mid i \in I\}}_{\text{function symbols}} \cup \underbrace{\{R_j \mid j \in J\}}_{\text{relation symbols}} \cup \underbrace{\{c_k \mid k \in K\}}_{\text{constant symbols}},$$

an *$\mathcal{L}$-structure* is the data of a set M together with

$$\underbrace{\{f_i^M \colon M^{n_i} \rightarrow M \mid i \in I\}}_{\text{functions}} \cup \underbrace{\{R_j^M \subseteq M^{m_i} \mid j \in J\}}_{\text{relations}} \cup \underbrace{\{c_k \in M \mid k \in K\}}_{\text{constants}}$$

in the prescribed arities. We often drop the superscript M, if it is clear what we are thinking about.

An $\mathcal{L}_{\mathrm{vf}}$-structure is then made up of the data

$$(M, +^M \colon M^2 \rightarrow M, \; \cdot \colon M^2 \rightarrow M, - \colon M \rightarrow M, 0^M \in M, 1^M \in M, \mathcal{O}^M \subseteq M).$$

[1] The general procedure is similar, but the basic building blocks vary depending on the language. For example, in a language like $\{+, \leq, 0\}$, commonly known as the language of ordered groups, basic building blocks take the forms $\sum_{i=0}^{l} n_i X_i = 0$ and $\sum_{i=0}^{l} n_i X_i \geq 0$, where $n_0, \dots n_l \in \mathbb{N}$.

Once we pick a sentence ϕ in the language, we can then check if ϕ is true in our structure by interpreting the symbols as precisely the operations we chose. If the sentence ends up being true, then we write

$$(M, f_i^M \colon M^{n_i} \to M \mid i \in I; R_j^M \subseteq M^{m_i} \mid j \in J; c_k \in M \mid k \in K\} \vDash \phi,$$

or more often $M \vDash \phi$. We say M *models* (or *satisfies*) ϕ.

Note that the notion of a structure is just a set with a bunch of functions and specified subsets and elements; they don't have to satisfy properties of any kind, e.g. $(M, +^M, \cdot^M, 0^M, 1^M)$ does not have to be a ring.

Needless to say, we called this the language *of valued fields* because we'd like to think of structures like $(M, +^M, \cdot^M, 0^M, 1^M)$ as a field together with a valuation ring $\mathcal{O}^M$. For example,

$$(\mathbb{Q}_p, +, \cdot, 0, 1, \mathbb{Z}_p)$$

is precisely this kind of structure. But so is

$$(\mathbb{Q}_p, (x,y) \mapsto x^2 + y, (x,y) \mapsto xy + 1, 3, 7, \mathbb{Z}).$$

What distinguishes these two is what sentences are true in them, i.e. their *complete theory*

$$\mathrm{Th}_{\mathcal{L}}(M) = \{\phi \ \mathcal{L}\text{-sentence} \mid M \vDash \phi\}.$$

Theories. A theory is a set of sentences in a certain language. For example, we may consider the theory of valued fields T_0 in the language $\mathcal{L}_{\mathrm{vf}}$ that contains axioms for $+, \cdot, -, 0, 1$ that make them into the operations and elements of a field, and axioms for $\mathcal{O}$ that makes it a valuation ring. For example,

$$\forall X (X \neq 0 \to \exists Y (X \cdot Y = 1)) \in T_0,$$

and moreover

$$\forall X (X \neq 0 \to \exists Y (X \cdot Y = 1) \wedge (X \in \mathcal{O} \vee Y \in \mathcal{O})) \in T_0,$$

forcing $\mathcal{O}$ to be a valuation ring.

$\mathcal{L}_{\mathrm{vf}}$-structures M where T_0 is true (i.e. all sentences in T_0 are true) are then precisely valued fields with residue field $\mathcal{O}^M / \mathfrak{m}^M$ and value group $M^\times / (\mathcal{O}^M)^\times$. Note that we can encode

$$X \in \mathfrak{m}^M$$

by saying

$$\neg \exists Y (Y \in \mathcal{O} \wedge X \cdot Y = 1),$$

so we can use $X \in \mathfrak{m}^M$ or $X \notin \mathfrak{m}^M$ in our formulae freely.

We can now rephrase our original goal – we seek to completely characterize $\mathrm{Th}_{\mathcal{L}_{\mathrm{vf}}}(\mathbb{Q}_p)$. For simplicity, I will write $\mathrm{Th}(\mathbb{Q}_p)$, since we only use one language. Our endgoal will be characterizing $\mathrm{Th}(\mathbb{Q}_p)$ via the absolute Galois group of $\mathbb{Q}_p$; today, we will do a first simplification of this task by characterizing $\mathrm{Th}(\mathbb{Q}_p)$ in terms of simpler, explicit sentences.

2 Second stop: logic-coloured glasses on!

So, back to the original characterization:

Definition 2.1 (*Tentative*). A valued field (K, v) is *algebraically like* $\mathbb{Q}_p$ if,

1. Kv has p elements,

2. $vK \simeq \mathbb{Z}$,
3. K is complete with respect to the corresponding absolute value $|x|_v := e^{-v(x)}$,
4. $v(p)$ is the smallest positive element of vK (i.e., $v(p) = 1$ under the isomorphism above).

This definition is problematic for two reason: first, it characterizes $\mathbb{Q}_p$ up to isomorphism, something that $\mathrm{Th}(\mathbb{Q}_p)$ cannot hope to do (we will see an example in a moment). Second, because the properties are not really expressible by formulae; completeness requires us to write things like $\forall n \in \mathbb{N}$, which is not allowed by our language and construction. Similarly, we can't pin down the isomorphism type of the value group. We need to replace them with properties that are accessible via model theory.

First, we need a model theoretic version of *looking like* $\mathbb{Z}$ as an ordered abelian group.

Definition 2.2. An ordered abelian group $(\Gamma, \leq, +)$ is called a $\mathbb{Z}$*-group* if it has a minimal positive element and, further, for any $n \in \mathbb{N}$ and any $\gamma \in \Gamma$, there is an element in $\{\gamma - 1, \gamma - 2, \dots \gamma - n\}$ which is divisible by n. In short, $[\Gamma : n\Gamma] = n$, for every $n \geq 0$.

This is, incidentally, exactly a characterization of the complete theory of $(\mathbb{Z}, \leq, +)$ in the language $\mathcal{L}_{\mathrm{oag}} := \{+, \leq, 0\}$:

Theorem 2.3 (*See Theorem 4.7 in Robinson-Zakon, Elementary properties of ordered abelian groups*[2]). $\mathrm{Th}_{\mathcal{L}_{\mathrm{oag}}}(\Gamma) = \mathrm{Th}_{\mathcal{L}_{\mathrm{oag}}}(\mathbb{Z})$ if and only if $(\Gamma, \leq, +)$ is a $\mathbb{Z}$-group.

Second, we need a way to express *completeness* in a sentence. This is trickier, and it is actually the crux of the argument – in this specific setting (*mixed characteristic, unramified*) we can do away with a so-called *first-order shadow* that looks much weaker, namely *henselianity*. This can be expressed by infinitely many $\mathcal{L}_{\mathrm{vf}}$-sentences of the form

$$\forall \underbrace{X_1, \dots X_n,}_{\text{coefficients}} \underbrace{Y}_{\text{candidate root}} \; [(X_1 \in \mathcal{O} \wedge \cdots \wedge X_n \in \mathcal{O} \wedge Y \in \mathcal{O} \wedge (\underbrace{X_0 + X_1 Y + X_2 Y^2 + \cdots + X_n Y^n \in \mathfrak{m}}_{\text{residue root}}) \wedge$$
$$(\underbrace{X_1 + 2X_1 Y + \cdots + n X_n Y^{n-1} \notin \mathfrak{m}}_{\text{simple root}})) \to \exists \underbrace{Z}_{\text{real root}} \; ((X_0 + X_1 Z + \cdots + X_n Z^n = 0) \wedge (Z - Y \in \mathfrak{m}))],$$

one for each degree $n \in \mathbb{N}$. Altogether, they express that the model is a henselian valued field.

Let's put everything together.

Definition 2.4. A valued field (K, v) is *p-adically closed* if,

1. Kv has p elements,
2. ~~$vK \simeq \mathbb{Z}$~~ *vK is a $\mathbb{Z}$-group*,
3. K ~~is complete with respect to the corresponding absolute value $|x|_v := e^{-v(x)}$~~ *is henselian*,
4. $v(p)$ is the smallest positive element of vK (i.e., $v(p) = 1$ under the isomorphism above).

This can be expressed by a $\mathcal{L}_{\mathrm{vf}}$-theory. For example, condition 1. can be expressed as

$$\underbrace{\exists Z_0, \dots Z_{p-1}}_{\text{representatives for classes in the residue field}}$$
$$(\underbrace{Z_0 \in \mathfrak{m} \wedge Z_1 \in \mathcal{O}^\times \wedge \cdots \wedge Z_{p-1} \in \mathcal{O}^\times}_{\text{all but one have valuation zero}} \wedge \underbrace{Z_0 - Z_1 \notin \mathfrak{m} \wedge Z_0 - Z_2 \notin \mathfrak{m} \wedge \cdots \wedge Z_{p-2} - Z_{p-1} \notin \mathfrak{m}}_{\text{they determine different residues}}$$
$$\wedge \; \forall X(\underbrace{X \in \mathcal{O} \to (X - Z_0 \in \mathfrak{m} \vee X - Z_1 \in \mathfrak{m} \vee \cdots \vee X - Z_{p-1} \in \mathfrak{m})}_{\text{they determine \textit{all} the possible residues}})).$$

[2] Here $\mathbb{Z}$-groups are called *regularly discrete*.

Similarly, we can write that vK has a minimal positive element as

$$\exists X(X \neq 0 \wedge \underbrace{X \in \mathfrak{m}}_{v(X)>0} \wedge \forall Y(Y \in \mathfrak{m} \rightarrow \underbrace{YX^{-1} \in \mathfrak{m}}_{v(Y)>v(X)})).$$

Here is the crucial point of this: the axioms 1.-4., together with T_0, are *exactly* what describes the model theory of $\mathbb{Q}_p$. Given two $\mathcal{L}$-structures M and N, write $M \equiv N$ to mean $\mathrm{Th}_{\mathcal{L}}(M) = \mathrm{Th}_{\mathcal{L}}(N)$. This is a good approximation of *having the same model theory*, also known as being *elementarily equivalent*.

Theorem 2.5 (*See Corollary 5.4 in Prestel-Roquette, Formally p-adic fields*). A valued field (K, v) is p-adically closed if and only if $K \equiv \mathbb{Q}_p$.

Note that being p-adically closed is a purely algebraic characterization, yet it is strictly weaker than the one we have exhibited before. For example, $K = \mathbb{Q}_p \cap \overline{\mathbb{Q}}$ is a p-adically closed field, yet it is not isomorphic to $\mathbb{Q}_p$ (it is countable, because $\overline{\mathbb{Q}}$ is!).

2.1 A surprise stop: definability of valuations

We have, so far, only worked with formulae and sentences in $\mathcal{L}_{\mathrm{vf}}$. This is not really necessary: in fields similar to $\mathbb{Q}_p$ (mixed characteristic unramified henselian valued fields), one can actually *define* the valuation ring with a sentence in the pure language of rings. This is due to Julia Robinson.

Indeed, given such a valued field (K, v) of residue characteristic $p \neq 2$,

$$\mathcal{O}_v = \{x \in K \mid K \vDash \exists Y(1 + px^2 = Y^2)\}.$$

Let's check this. Let $A = \{x \in \mid K \vDash \exists Y(1 + px^2 = Y^2)\}$ (this is an example of a *definable subset* of K). We check $A = \mathcal{O}_v$: if $x \notin \mathcal{O}_v$, i.e. $v(x) < 0$, then $v(1 + px^2) = v(px^2) = 1 + 2v(x)$, hence $v(1 + px^2) \neq v(Y^2) = 2v(Y)$ for any $Y \in K$, and thus $x \notin A$. Viceversa, if $x \in \mathcal{O}_v$, i.e. $v(x) \geq 0$, then $v(px^2) > 0$ and thus $Y^2 - (1 + px^2)$ has a root by henselianity, so $x \in A$.

This means that in all formulae, we could have replaced

$$x \in \mathcal{O} \iff \exists Y(1 + px^2 = Y^2)\}$$

and all the results above (and below) hold in the language of rings.

Note that one needs to use at least one quantifier in the definition of $\mathcal{O}_v$: quantifier-free formulae in one free variables define *constructible subsets* of K, which are finite or cofinite.

3 Third stop: model completeness

The theory of p-adically closed fields satisfies a much richer family of results and properties than just the one above, which one could summarize in the fact that it is a *complete* theory (all of its models are elementarily equivalent, i.e. they share the same theory).

There is one that we will need further along the seminar: *model completeness*. This follows directly from Macintyre's proof of quantifier elimination in a certain expanded language.

Theorem 3.1 (*See Theorem 5.1 in Prestel-Roquette, Formally p-adic fields*). Let K and L be p-adically closed fields. If $K \subseteq L$, then $K \preceq L$.

The relationship $K \preceq L$ is called *elementary substructure*, and roughly encodes the idea of L being a *conservative* extension of K. To express that, we first need to clarify what we mean by a formula with *parameters*. Let's consider $\mathcal{L}$-formulae of the form $\phi(\overline{x}, \overline{y})$, whose non-quantified (*free*) variables come from the tuples $\overline{x}$ and $\overline{y}$. If we fix a set A, by $\mathcal{L}(A)$-*formula* we will mean a formula of the form $\phi(\overline{x}, \overline{a})$, where $\overline{a}$ is a tuple from the set A with the same length as $\overline{y}$. Concretely, we are writing down formulae using some special elements from the set A; think of a polynomial with some explicit coefficients (as opposed to the *generic* polynomial we wrote in the definition of henselianity). An $\mathcal{L}(A)$-*sentence* will then be an $\mathcal{L}(A)$-formula whose variables – that aren't substituted with parameters – are all quantified.

The relation $K \preceq L$ is then defined by $K \vDash \phi \iff L \vDash \phi$, for all $\mathcal{L}(K)$-sentences ϕ.

In the case of two p-adically closed fields $K \preceq L$, this implies for example that for any polynomial $p(X) \in K[X]$, $p(X)$ has a root in L if and only if it has a root in K. This is because we can work with the $\mathcal{L}(K)$-sentence $\exists X(p(X) = 0)$ and obtain

$$K \vDash \exists X(p(X) = 0) \iff L \vDash \exists X(p(X) = 0).$$