Explicit Constructions of Ω_p and Other Spherically Complete Valued Fields

Dallas Anderson

(unknown date)

1 Introduction

There are many different ultrametric fields extending the field of p-adic numbers, $\mathbb{Q}_p$. First of all, we have the algebraic closure of $\mathbb{Q}_p$, denoted $\overline{\mathbb{Q}}_p$. The way to extend the absolute value in $\mathbb{Q}_p$ onto $\overline{\mathbb{Q}}_p$ is as follows:

Definition 1.1. Take $a \in \overline{\mathbb{Q}}_p$, and let $f(x)$ be the unique monic irreducible polynomial over $\mathbb{Q}_p$ with a as a root. If c is the constant term of f, then we define $|a| = |c|^{\frac{1}{n}}$.

One downside to taking the algebraic closure of $\overline{\mathbb{Q}}_p$ is that the resulting field is no longer complete.

Theorem 1.2. *$\overline{\mathbb{Q}}_p$ is not complete.*

The thing that is tempting to do whenever one encounters a field that isn't complete is to complete it.

Definition 1.3. $\mathbb{C}_p$ is defined as the metric completion of the space $\overline{\mathbb{Q}}_p$.

Fortunately, this retains the property of algebraic closure that $\overline{\mathbb{Q}}_p$ established.

Theorem 1.4. *$\mathbb{C}_p$ is algebraically closed.*

So, $\mathbb{C}_p$ is both algebraically closed and complete. However, there is a stronger form of completeness that $\mathbb{C}_p$ still doesn't satisfy.

Definition 1.5. Let $\mathbb{F}$ be a field with an absolute value. Let S be a collection of closed balls in $\mathbb{F}$ such that if $B, C \in S$ then $B \subseteq C$ or $C \subseteq B$. (I.e. S is a chain with respect to the subset ordering.) If, for any choice of S, the intersection of all elements of S is nonempty, we say that $\mathbb{F}$ is *spherically complete*.

We do the same thing again, completing $\mathbb{C}_p$ with respect to the spherical completeness property.

Definition 1.6. A *spherical completion* of an absolute value field $\mathbb{F}$ is a spherically complete (absolute value) field $\mathbb{K}$ containing $\mathbb{F}$ such that if $\mathbb{L}$ is spherically complete with $\mathbb{F} \leq \mathbb{L} \leq \mathbb{K}$, then $\mathbb{L} = \mathbb{K}$. A spherical completion of $\mathbb{C}_p$ is called Ω_p.

Notice the phrasing "a spherical completion". The unfortunate thing about spherical completions is that they are, in general, not unique. In particular, there are multiple spherical completions of $\mathbb{C}_p$, with no consensus on which one deserves to be called Ω_p. Instead, mathematicians generally study the collection of fields Ω_p, looking at the commonalities between their properties. For example:

Theorem 1.7. *All Ω_p fields are algebraically closed.*

They're also all complete, since completeness is a consequence of spherical completion.

Theorem 1.8. *All spherically complete absolute value fields are complete.*

This makes Ω_p a "universal" p-adic field, in a sense, because it satisfies all the important closure properties. Although the collection of fields we call "Ω_p" behave so nicely, it would be better if we could construct an explicit Ω_p field to do analysis over. In order to do that, we'll have to dive deeper into *Kaplansky Theory*, a field of study all about spherical completions.

2 Valued Fields

Before we get into the details of Kaplansky theory and explicit Ω_p fields, let us introduce some basic notions. First, a reminder of the definition of absolute values on fields:

Definition 2.1. Let $\mathbb{F}$ be a field. An *absolute value* on $\mathbb{F}$ is a function $|\cdot| : \mathbb{F} \to \mathbb{R}$ satisfying the following properties:

- $|0| = 0$, and $|x| > 0$ if $x \neq 0$.
- $|xy| = |x| \cdot |y|$.
- $|x + y| \leq |x| + |y|$.

We call $\mathbb{F}$ under $|\cdot|_p$ a *valued field.* If the absolute value satisfies the stronger inequality $|x+y| \leq \max(|x|, |y|)$, we call it an *ultrametric absolute value.*

Here are some examples of valued fields:

Example 2.2. The fields $\mathbb{Q}$ and $\mathbb{R}$ under the ordinary absolute value function are valued fields. The complex numbers $\mathbb{C}$ under the function $|a + bi| = \sqrt{a^2 + b^2}$ form a valued field as well.

None of the above satisfy the ultrametric property, since, for instance $|1 + 1| > \max(|1|, |1|)$. However, consider the next example:

Definition 2.3. Fix a prime p, and let $r \in \mathbb{Q}$. Let $r = \frac{a}{b} \neq 0$ for integers a, b, and let d and e be the exponents of p in the prime factorizations of a and b, respectively. The *p-adic valuation* of r is defined as $v_p(r) = d - e$. (You can check for yourself that this is well-defined.) The *p-adic absolute value* is defined as $|r|_p = p^{-v_p(r)}$ if $r \neq 0$ and $|0|_p = 0$.

The absolute value defined above satisfies the ultrametric property, making $\mathbb{Q}$ under it an ultrametric valued field. Completing this gives another ultrametric valued field, $\mathbb{Q}_p$.

Definition 2.4. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is referred to as $\mathbb{Q}_p$, or the *p-adic numbers.*

This field takes on the same range of possible absolute values as $\mathbb{Q}$, namely $\{0\} \cup \{p^n : n \in \mathbb{Z}\}$.

Now, recall the valuation v_p over the rational numbers. That function essentially contains the same information as $|\cdot|_p$, they just have different codomains. In fact, look back at the properties for ultrametric absolute values:

- $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$.
- $|xy| = |x| \cdot |y|$.
- $|x + y| \leq \max(|x|, |y|)$.

Nowhere is the addition of two absolute values ($|x| + |y|$) ever relevant, since we replaced the property $|x + y| \leq |x| + |y|$ with the stronger ultrametric version. The only things that matter over the codomain of $|\cdot|$ are multiplication and ordering. In the case of $|\cdot|_p$, if we convert to v_p (writing that $v_p(0) = \infty$), the three structural properties become the following:

- $v_p(x) = \infty$ iff $x = 0$.
- $v_p(xy) = v_p(x) + v_p(y)$.
- $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

In this case, the codomain of v_p is $\mathbb{Z} \cup \{\infty\}$, with $+$ and $\leq$ being the only relevant structural information about $\mathbb{Z}$. We can generalize ultrametric valued fields to include artitrary codomains, so long as they're abelian ordered groups:

Definition 2.5. Let K be a field and let $(\Gamma, +, \leq)$ be a totally ordered abelian group. Adjoin an element ∞ to Γ and extend $+$ and $\leq$ in the following ways:

- $x \leq \infty$ for all $x \in \Gamma \cup \{\infty\}$ and $\infty \not\leq x$ if $x \in \Gamma$.
- $\infty + x = x + \infty = \infty$ for all $x \in \Gamma \cup \{\infty\}$.

Now, consider a function $v : K \to \Gamma \cup \{\infty\}$ satisfying the following properties:

- $v(x) = \infty$ iff $x = 0$.
- $v(xy) = v(x) + v(y)$
- $v(x + y) \geq \min(v(x), v(y))$.
- $v : K \to \Gamma \cup \{\infty\}$ is a surjective function.

We say that v is a *Krull valuation*, or simply *valuation* if the context is clear. We call K equipped with v a *valued field*, with Γ its *valuation group*.

From now on, the above is what we will mean when we talk about valuations and valued fields, unless stated otherwise.

Remark 2.6. If we didn't require v to be surjective, its image would be some subgroup $\Gamma' \leq \Gamma$ unioned with ∞. In that case, we could just restrict the valuation group to Γ' instead and we'd still have a perfectly fine valued field. To remove the artificial inconvenience of extra elements, we simply require that v hit all elements of $\Gamma \cup \{\infty\}$.

Remark 2.7. The reason that Γ is written in additive notation and that inequalities are reversed [e.g. $v(x+y) \geq \min(v(x), v(y))$] is that the function v is inspired by the p-adic valuation $v : \mathbb{Q} \to \mathbb{Z}$ rather than the p-adic absolute value function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$. One could just as easily write everything in multiplicative notation and make inequalities match with $|\cdot|_p$, but for fields with Krull valuations the convention is otherwise.

For extensions of $\mathbb{Q}_p$ with real-valued absolute values, we can define valuation functions $v(x) = -\log_p(|x|)$ (with $v(0) = \infty$). Then, the valuation group for $\mathbb{Q}$ and $\mathbb{Q}_p$ is $\mathbb{Z}$, whereas the fields $\overline{\mathbb{Q}}_p$, $\mathbb{C}_p$ and Ω_p all have valuation group $\mathbb{Q}$ (under addition). Now, let's get into some basic definitions and theorems related to valued fields.

Definition 2.8. Let K be a valued field. The *valuation ring* $\mathfrak{o}_K$ (or just $\mathfrak{o}$) is defined as

$$\mathfrak{o}_K = \{x \in K : v(x) \geq 0\}.$$

We also write

$$\mathfrak{m} = \mathfrak{m}_K = \{x \in K : v(x) > 0\}$$

(note the strict inequality here).

In $\mathbb{R}$ or $\mathbb{C}$, the set $\mathfrak{o}$ is analogous to the closed unit disk centered at 0. The analogue of $\mathfrak{m}$ is the open unit disk centered at 0. Neither of these disks satisfy remotely nice algebraic properties in $\mathbb{R}$ or $\mathbb{C}$, since they aren't even closed under addition. This is quite different from the behavior of $\mathfrak{o}$ and $\mathfrak{m}$ in K:

Theorem 2.9. *The subset $\mathfrak{o} \subseteq K$ is an integral domain, and $\mathfrak{m} \subseteq \mathfrak{o}$ is an ideal. In fact, $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{o}$.*

Proof. It is routine to check that $\mathfrak{o}$ is an integral domain and $\mathfrak{m}$ is an ideal. To show $\mathfrak{m}$ is uniquely maximal, consider some element $u \in \mathfrak{o}$ that's not in $\mathfrak{m}$. What this means is that $v(u) = 0$. In particular, $v(u^{-1}) = -v(u) = 0$ as well, so $u^{-1} \in \mathfrak{o}$. Thus, the elements in $\mathfrak{o} \setminus \mathfrak{m}$ are precisely the units of $\mathfrak{o}$. If $\mathfrak{a}$ is another proper ideal of $\mathfrak{o}$, we know it doesn't contain units, so $\mathfrak{a} \subseteq \mathfrak{m}$. Therefore, $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{o}$. □

A basic fact of ring theory is that if you have a maximal ideal I of an integral domain R, the quotient R/I is a field. In particular:

Definition 2.10. With notation as above, we call $k := \mathfrak{o}/\mathfrak{m}$ the *residue field* of K.

Residue fields are an important actor in the study of valued fields. In particular, they allow you to define *immediate extensions* of valued fields. To start, let's define extensions:

Definition 2.11. Let K and L be valued fields with valuation groups Γ_K and Γ_L, and valuation maps v_K and v_L, respectively. Let $f : K \to L$ be a field homomorphism, and let $F : \Gamma_K \to \Gamma_L$ be a strictly increasing group homomorphism. We call the pair (f, F) an *extension map*, and say that L is an *extension* of K, if $v_L(f(x)) = F(v_K(x))$ for $x \in K \setminus \{0\}$.

Now let k_K and k_L be the residue fields of K and L, respectively. The extension f (or (f, F) to be explicit) naturally induces a field extension $\overline{f} : k_K \to k_L$ by taking $\overline{f}(x + \mathfrak{m}_K) = f(x) + \mathfrak{m}_L$. With this, we can define *immediate extensions*:

Definition 2.12. With notation as above, if $\overline{f}$ and F are both bijective, we say that L is an *immediate extension* of K.

In other words, immediate extensions are extensions that don't expand the valuation group or the residue field.

Example 2.13. The extension $\mathbb{Q} \leq \mathbb{Q}_p$ is immediate since they both have valuation group $\mathbb{Z}$ and residue field $\mathbb{F}_p$. The extensions $\overline{\mathbb{Q}}_p \leq \mathbb{C}_p \leq \Omega_p$ are all immediate since the fields have valuation group $\mathbb{Q}$ and residue field $\overline{\mathbb{F}}_p$, the algebraic closure of $\mathbb{F}_p$. However, notice that both the valuation group *and* the residue field increase upon extending $\mathbb{Q}_p$ to $\overline{\mathbb{Q}}_p$, so this extension is certainly not immediate.

Now, here's the big important connection between immediate extensions and spherical completeness:

Theorem 2.14. [2] *A valued field K is spherically complete if and only if it has no proper immediate extensions (i.e. the only immediate extension maps (f, F) are isomorphisms).*

Thus, in a sense, the spherically complete fields are the "maximal" valued fields with their respective valuation groups and residue fields. Let's now look at a certain kind of spherically complete field and its uniqueness properties.

3 Fields of Hahn Series

Definition 3.1. Let k be a field and Γ be an abelian ordered group. The *Field of Hahn Series* (or *Mal'cev-Neumann field*) over k with value group Γ (denoted $k[[T^\Gamma]]$) is the set of formal expressions of the form

$$\sum_{e \in \Gamma} c_e T^e$$

(in the indeterminant T) where the set $S = \{e \in \Gamma : c_e \neq 0\}$ is well-ordered. The sum and product of $f = \sum_{e \in \Gamma} c_e T^e$ and $g = \sum_{e \in \Gamma} d_e T^e$ are given by

$$f + g = \sum_{e \in \Gamma} (c_e + d_e) T^e$$

and

$$fg = \sum_{e \in \Gamma} \left(\sum_{s \in \Gamma} c_s d_{e-s} \right) T^e.$$

Note that the coefficient is a finite sum upon removing zeroes due to the well-ordering property above. The valuation $v : K \to \Gamma \cup \{\infty\}$ is defined so that $v(f)$ is the smallest $e \in \Gamma$ such that $c_e \neq 0$ (unless $f = 0$, in which case $v(f) = \infty$).

As the notation suggests, this field has value group Γ and residue field k.

Theorem 3.2. *The valued field $K := k[[T^\Gamma]]$ has value group Γ and residue field k.*

Proof. The first statement is true by definition. As for the residue field, we start by noting that $\mathfrak{o}_K$ contains precisely those Hahn series

$$f = \sum_{e \in \Gamma} c_e T^e$$

such that $c_e = 0$ for all $e < 0$. If we add the condition that $c_0 = 0$ as well, we get $\mathfrak{m}_K$. Thus, one can see that the ideals of $\mathfrak{m}_K$ in $\mathfrak{o}_K$ are described by $cT^0 + \mathfrak{m}_K$ for $c \in k$, and $i(c) = cT^0 + \mathfrak{m}_K$ is an isomorphism from k to $\mathfrak{o}_K / \mathfrak{m}_K$. □

Now let's prove spherical completeness:

Theorem 3.3. $K := k[[T^\Gamma]]$ *is spherically complete.*

Proof. Let S be a totally ordered set, with a closed ball $B_s = \overline{B_{e_s}}(x_s)$ for each $s \in S$ such that $B_s \subseteq B_t$ iff $s \geq t$. Here, the closed ball $B_e(x)$ just means the set of all $y \in K$ such that $v(y-x) \geq e$. Now, let

$$x_s = \sum_{e \in \Gamma} c_{e,s} T^e.$$

What the statement $y \in \overline{B_{e_s}}(x_s)$ means for Hahn series is that the coefficients of y and x agree up to, but maybe not including the T^{e_s} term. If $e < e_s$, then everything in B_s has coefficient $c_{e,s}$ in the T^e term. For the sake of this proof, we will call $c \in K$ a *stable coefficient* for $e \in \Gamma$ if there is an $s \in S$ such that $e_s > e$ and $c_{e,s} = c$.

Now, let's show that any $e \in \Gamma$ has at most one stable coefficient. Let c, d be stable coefficients of e. This means that there are $s, t \in S$ such that $e < e_s, e_t$, $c_{e,s} = c$ and $c_{e,t} = d$. Without loss of generality, assume $s \geq t$. This means that $B_s \subseteq B_t$, and in particular $x_s \in B_t$. We know that for any $e' < e_s$, the coefficient of $T^{e'}$ matches in x_s and x_t, so setting $e' = e$ gives $c_{e,s} = c_{e,t}$, or $c = d$.

It's obvious that if e has a stable coefficient and $e' < e$ then e' has one as well, since $e < e_s$ implies $e' < e_s$. This is saying that the set $A \subseteq \Gamma$ of elements with stable coefficients is closed downward. For $e \in A$, denote a_e for the stable coefficient of e, and if $e \notin A$ write $a_e = 0$ (the latter is arbitrary). We want to define an element

$$a = \sum_{e \in \Gamma} a_e T^e,$$

but in order for this to be well-defined we need the set $B = \{e : a_e \neq 0\} \subseteq A$ to be well-ordered. Let $B' \subseteq B$ be nonempty. We know that there exists $b \in B'$. In particular, $b \in A$, so there's some $s \in S$ such that $b < e_s$. By the uniqueness of stable coefficients, we know that for all $e < e_s$, x_s has coefficient a_e in the T^e component. Now, since x_s is a well-defined element of K, it must be true that there's a smallest $b' \in B'$ such that $c_{b',s} \neq 0$, or there's no such b'. However, $b \in B'$ is such that $c_{b',s} = a_b \neq 0$, so the smallest such b' does actually exist and is $\leq b$.

Now, if $g \in B'$ is an element $\geq e_s$, then we know that $b' \leq g$ since $b' \leq b < e_s \leq g$. If $g < e_s$, we know that $c_{g,s} = a_g \neq 0$, so $b' \leq g$. Thus b' is the smallest element of B' in general, and we're done proving B is well-ordered. This means that a is a well-defined Hahn series in K.

The last thing to prove is that a is actually in all the balls B_s. If $e < e_s$, we know that $c_{e,s}$ is a stable coefficient for e, so $c_{e,s} = a_e$. What this means is that a agrees with x_s in all places lower than the e_s place, i.e. $a \in \overline{B_{e_s}}(x_s) = B_s$. Thus the intersection of all the balls is nonempty, containing a in particular. This completes the proof that K is spherically complete. □

This is quite convenient, because you can plug in any Γ and k you like, and you'll automatically get an explicit spherically complete field with that valuation group and residue field. So, does this mean we're done? Have we explicitly constructed a field Ω_p?

4 Rings of Witt Vectors (potentially rename)

Unfortunately, it's not that simple. Let's take a look back at $\mathbb{C}_p$. This is a valued field with valuation group $\mathbb{Q}$ and residue field $\overline{\mathbb{F}}_p$. A spherical completion of $\mathbb{C}_p$, then, is really just a maximal immediate extension of $\mathbb{C}_p$ by Theorem 2.14. Since $\mathbb{C}_p$ has characteristic 0, any spherical completion Ω_p must also have characteristic 0, but the residue field $\overline{\mathbb{F}}_p$ has characteristic $p \neq 0$. This difference in characteristics has a name.

Definition 4.1. Let K be a valued field, with residue field k. If K and k have the same characteristic, we say that K is in *equal characteristic*, and otherwise we say K is in *mixed characteristic*.

Theorem 4.2. *All fields of Hahn series are in equal characteristic.*

Proof. Let $K = k[[T^\Gamma]]$, and let $i : k \to K$ be defined by $i(c) = cT^0$. We have that i is injective, that $cT^0 + dT^0 = (c+d)T^0$, and that $(cT^0)(dT^0) = cdT^0$, meaning that i is a field embedding. If k can be embedded into K, then in particular they must have the same characteristic. □

Unfortunately, this means that Ω_p cannot be realized as a field of Hahn series since it is in mixed characteristic. The field $\overline{\mathbb{F}}_p[[T]^{\mathbb{Q}}]$ is a perfectly fine valued field, but since it has characteristic p it can't be an extension of $\mathbb{C}_p$, particularly a maximal immediate one. This is one of the ways in which equal characteristic valued fields behave cleaner than mixed characteristic ones. We can still utilize the idea of Hahn series in the mixed case, but we need to add a little twist.

Let's look back at the way we express numbers in $\mathbb{Q}_p$. Each number can be written as a p-mal expansion

$$\sum_{n=N}^{\infty} a_n p^n$$

where $a_n \in \{0, 1, \ldots, p-1\}$ and $N \in \mathbb{Z}$. This looks a lot like Hahn series, particularly in the case $\Gamma = \mathbb{Z}$ and $k = \mathbb{F}_p$. The important difference, however, is carrying. For example, if $x, y \in \mathbb{Z}_5$ with last digits 3 and 4 respectively, the sum is 12 in pentimal, so the 1 needs to be carried to the next place. This differs from the Hahn series case, in which each pair of coefficients of the same term would just be added modulo 5, not affecting any other terms in the series. A similar carrying phenomenon arises when you multiply two numbers in $\mathbb{Q}_p$.

Now, choosing the set $\{0, 1, \ldots, p-1\}$ for the digits of numbers is a completely arbitrary choice; we might as well choose any other set of $p-1$ elements of $\mathbb{Z}_p$, one in each residue class modulo p. One example of a possible selection of digits is the *Teichmüler representatives* of $\mathbb{Z}_p$:

Definition 4.3. The *Teichmüler representatives* of $\mathbb{Z}_p$ are the elements $x \in \mathbb{Z}_p$ such that $x^p = x$. For each $a \in \mathbb{F}_p$, there is one Teichmüler representative $x \equiv a \pmod{p}$.

Example 4.4. The Teichmüler representatives in $\mathbb{Z}_5$ are

$$0,\ 1,\ \cdots 02303243112,\ \cdots 21412013233,\ -1 = 44444444444,$$

expansions expressed in usual digits.

In some sense, the Teichmüler representatives are a better digit system to work with than the integers $\{0, 1, \ldots, p-1\}$. For example, they are multiplicative:

Theorem 4.5. *If x, y are Teichmüler representatives over $\mathbb{Z}_p$, then xy is also one.*

Proof. We have $(xy)^p = x^p y^p = xy$. □

Restricting our focus to $\mathbb{Z}_p$ rather than $\mathbb{Q}_p$, we can express any element as a sum

$$x = \sum_{n=0}^{\infty} x_n p^n$$

where x_n is a Teichmüler representative for each n. In order to look at how these representations tie into addition and multiplication, we first need to define a few polynomials.

Definition 4.6. For $n \geq 0$, define the nth *Witt polynomial* $W_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n]$ as

$$W_n(X_0, \ldots, X_n) = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}.$$

Make the abbreviations $X = (X_0, \ldots, X_n)$ and $Y = (Y_0, \ldots, Y_n)$. Next, the polynomials $S_n, M_n \in \mathbb{Z}[X_0, \ldots, X_n; Y_0, \ldots, Y_n]$ are defined as the unique set of polynomials satisfying

$$W_n(S_0, S_1, \ldots S_n) = W_n(X) + W_n(Y)$$

and

$$W_n(M_0, M_1, \ldots M_n) = W_n(X) W_n(Y),$$

where $S_i = S_i[X_0, \ldots, X_i; Y_0, \ldots, Y_i]$ and $M_i = M_i[X_0, \ldots, X_i; Y_0, \ldots, Y_i]$.

The intuition here is that S_n are the "addition polynomials" and M_n are the "multiplication polynomials", and we define them around making

$$W(x) := (W_0(x_0), W_1(x_0, x_1), W_2(x_0, x_1, x_2), \ldots)$$

a ring homomorphism. Formally stated:

Definition 4.7. Let R be a commutative ring with identity. We define the *Ring of Witt-Vectors* $W_p(R)$ (or $W(R)$ if p is clear) as the set of series $(x_0, x_1, x_2, \ldots)$ for $x_n \in R$. Addition and multiplication are defined by

$$(x_n) + (y_n) = (S_n(x_0, \ldots, x_n; y_0, \ldots, y_n))_{n=0}^{\infty}$$

and

$$(x_n) \cdot (y_n) = (M_n(x_0, \ldots, x_n; y_0, \ldots, y_n))_{n=0}^{\infty}.$$

The equations that S_n and M_n have to satisfy are uniquely satisfied by a certain formula.

Theorem 4.8. [1] *We have*

$$S_n(x_0, \ldots, x_n; y_0, \ldots, y_n) = \frac{W_n(X) + W_n(Y) + \sum_{i=0}^{n-1} p_i S_i^{p^{n-i}}}{p^n}$$

and

$$M_n(x_0, \ldots, x_n; y_0, \ldots, y_n) = \frac{W_n(X)W_n(Y) \sum_{i=0}^{n-1} p_i M_i^{p^{n-i}}}{p^n}.$$

Remark 4.9. Note that the divisions by p^n are only there because these polynomials are in simplified form. If you expanded everything out, everything in the numerator would be divisible by p^n and these polynomials would be integer polynomials. If R has characteristic $p > 0$, you must cancel out the p^n before plugging things in and evaluating over R.

This construction is most relevant to us in the case that R is a field, with some extra conditions:

Theorem 4.10. *If k is a perfect field with characteristic p, then the ring $W_p(k)$ is an integral domain.*

The property of being an integral domain is particularly nice because we can consider its field of fractions, $\text{Frac}(W_p(k))$. So far, though, this is just a field. We need to introduce a valuation!

Definition 4.11. Let k be a perfect field of characteristic p. We define the valuation $v : W_p(k) \to \mathbb{Z} \cup \{\infty\}$ by $v(x_0, x_1, x_2, \ldots) = n$, where n is the smallest integer such that $x_n \neq 0$. (And $v(0, 0, \ldots) = \infty$ since this is the 0 element.) Next, if k is a perfect field of characteristic p, we can extend the valuation v onto $\text{Frac}(W(k))$ by defining $v\left(\frac{x}{y}\right) = v(x) - v(y)$. This still has codomain $\mathbb{Z} \cup \{\infty\}$.

Example 4.12. Let k be the field $\mathbb{F}_p$ (note that $\mathbb{F}_p$ is a perfect field). Then, the construction $W_p(k)$ yields $\mathbb{Z}_p$, with $(a, 0, 0, \cdots)$ being the Teichmüler representative congruent to a modulo p. Since $W_p(k) = \mathbb{Z}_p$, it's not too surprising that $\text{Frac}(W_p(k)) = \mathbb{Q}_p$.

Here's the main result about fraction fields of rings of Witt vectors:

Theorem 4.13. *Let k be a perfect field of characteristic p. We have that Frac$(W_p(k))$ is a spherically complete valued field with value group $\mathbb{Z}$, residue field k, and characteristic* 0.

This is in the right direction, but it's restrictive in two ways. The first is that k has to be a perfect field. As for Ω_p, the desired residue field $\overline{\mathbb{F}}_p$ is perfect, so no problem there. The second, more important restriction is that this only works when the valuation group is $\mathbb{Z}$. The desired valuation group for Ω_p is $\mathbb{Q}$. To accommodate this, we need to extend our Witt vector construction to include arbitrary valuation groups.

5 Twisted Hahn Series

To start, note that the construction of fields of Hahn series can be generalized with the residue field k being a ring instead:

Definition 5.1. Let R be a field and Γ be an abelian ordered group. The *Ring of Hahn Series* (or Mal'cev-Neumann ring) over R with value group Γ (denoted $R[[T^\Gamma]]$) is the set of formal expressions of the form

$$\sum_{e\in\Gamma} c_e T^e$$

where the set $S = \{e \in \Gamma : c_e \neq 0\}$ is well-ordered. The sum and product of $f = \sum_{e\in\Gamma} c_e T^e$ and $g = \sum_{e\in\Gamma} d_e T^e$ are given by

$$f + g = \sum_{e\in\Gamma}(c_e + d_e)T^e$$

and

$$fg = \sum_{e\in\Gamma}\left(\sum_{s\in\Gamma} c_s d_{e-s}\right)T^e,$$

as before.

We could define a valuation on rings of Hahn series, but we won't need that for our purposes.

Let k be a perfect field of characteristic p, and let Γ be an abelian ordered group, with a fixed positive element $1 > 0$. We want a field of series of the form

$$\sum_{e\in\Gamma} c_e p^e,$$

with p standing in for t. We start by considering the ring $W_p(k)[[T^\Gamma]]$. This consists of Hahn series in T with Witt vectors over k as coefficients. The problem with this construction is that some elements, like $-p + T^1$, "ought to be" 0 if we want to equate T with p. Whenever we have a ring with unequal things that we want to be equal, the thing to do is to quotient it out by an ideal.

In order to do that, we have to create a rigorous rule for which elements we want to equal 0. Whenever we have a term aT^1 where a is a Witt vector, we should equate this to $(ap)T^0$. More generally, a term like aT^{e+n} should be equated to $(ap^n)T^e$ for $e \in \Gamma$ and $n \in \mathbb{Z}$. (Note that $\mathbb{Z}$ can be embedded into Γ using the fixed element $1 \in \Gamma$ as a generator.) If we look at a sum

$$\alpha = \sum_{e\in\Gamma} \alpha_e T^e \in W_p(k)[[T^\Gamma]],$$

we can restrict our view to the terms

$$\sum_{n\in\mathbb{Z}} \alpha_{e+n} T^{e+n}$$

for a fixed $e \in \Gamma$. Factoring out T^e, we have that

$$\sum_{n\in\mathbb{Z}} \alpha_{e+n} T^{e+n} = 0$$

if and only if

$$\sum_{n\in\mathbb{Z}} \alpha_{e+n} T^n = 0.$$

If $T = p$, this should be equivalent to the criterion that

$$\sum_{n\in\mathbb{Z}} \alpha_{e+n} p^n = 0$$

as a series in $\mathrm{Frac}(W_p(k))$. This leads us to the following rigorous definition:

Definition 5.2. Let
$$\alpha = \sum_{e\in\Gamma} \alpha_e T^e \in W_p(k)[[T^\Gamma]].$$
We say that α is a *null series* if, for all $e \in \Gamma$,
$$\sum_{n\in\mathbb{Z}} \alpha_{e+n} p^n = 0$$
over $\mathrm{Frac}(W_p(k))$. Note that $\alpha_{e+n} = 0$ for n sufficiently negative by the well-ordering property of Hahn series, and that $v(\alpha_{e+n}p^n) \geq n$ for n, so the series above always converges in $\mathrm{Frac}(W_p(k))$.

Theorem 5.3. [3] *Let k and Γ be as before, and let N be the set of null series in $W_p(k)[[T^\Gamma]]$. Then N is an ideal, and $W_p(k)[[T^\Gamma]]/N$ is a field. This field is called the field of twisted Hahn series or Hahn-Witt Series and is denoted $W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$.*

As always, we need to define a valuation on this field. This is a little more involved than usual. Let's say we have an element $\alpha \in W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$, and a representation
$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e$$
over $W_p(k)[[T^\Gamma]]$. A naive way to define the valuation v is to let $v(\alpha) = c$, where $c \in \Gamma$ is the smallest element such that $\alpha_c \neq 0$. However, a problem arises if α_c isn't a unit. If $\alpha_c = pa$ for some $a \in W_p(k)$, then we can just change $\alpha_c p^c$ to ap^{c+1}, so that c is no longer the smallest exponent with a nonzero coefficient. Thus the new representation of α would give $v(\alpha) > c$. This is a problem! The solution is easy: We simply require that α_c be a unit.

Theorem 5.4. *Let $\alpha \in W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ be nonzero. There is a unique $c \in \Gamma$ such that α has a representation*
$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e$$
where α_c is a unit and $\alpha_e = 0$ for $e < c$. Moreover, any series expansion
$$\alpha = \sum_{e\in\Gamma} \beta_e p^e$$
satisfies the property that its lowest nonzero term has index $\leq c$.

Proof. To start, let's show that at most one such c exists. Let
$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e = \sum_{e\in\Gamma} \beta_e p^e,$$
where c, d exist such that α_c, β_d are units, $\alpha_e = 0$ for $e < c$, and $\alpha_e = 0$ for $e < d$. Our goal is to prove that $c = d$. For the sake of contradiction, suppose that $c \neq d$. By symmetry, we may assume without loss of generality that $c < d$. Note that
$$\sum_{e\in\Gamma} (\alpha_e - \beta_e) p^e = 0.$$
What this means over $W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ is that for all e,
$$\sum_{n\in\mathbb{Z}} (\alpha_{e+n} - \beta_{e+n}) p^n = 0$$
over $\mathrm{Frac}(W_p(k))$. In particular, we have
$$\sum_{n\in\mathbb{Z}} (\alpha_{c+n} - \beta_{c+n}) p^n = 0.$$

Since c is the smallest $e \in \Gamma$ such that $\alpha_e \neq 0$ and $d > c$ is the smallest $e \in \Gamma$ such that $\beta_e \neq 0$, we can write the above equation as

$$\sum_{n=0}^{\infty} (\alpha_{c+n} - \beta_{c+n}) p^n = 0.$$

However, we know that $\alpha_c - \beta_c = \alpha_c$ has valuation 0 in $\mathrm{Frac}(W_p(k))$, but the rest of the terms have valuation > 0 since they have p's in them. The total series thus has valuation 0 and can't be equal to 0, a contradiction.

Note that β_e being a unit (i.e. of valuation 0) wasn't relevant to this proof, so d can represent the lowest term in any possible series representation for α. This means we've actually shown that any series representation in $W_p(k)[[T^\Gamma]]$ for α has lowest nonzero term of index $\leq c$, since $d > c$ leads to a contradiction.

The second part is to show that c actually exists. Suppose we have some representation

$$\alpha = \sum_{e \in \Gamma} \alpha_e p^e.$$

We want to convert this into the desired form. Let $\Gamma' \subseteq \Gamma$ be a set of coset representatives for $\Gamma/\mathbb{Z}$. For each $e \in \Gamma'$, consider the sum

$$\sum_{n \in \mathbb{Z}} \alpha_{e+n} p^n.$$

This can be realized as an element in $\mathrm{Frac}(W_p(K))$ since it involves only integer powers of p. Therefore we may write it as

$$\sum_{n \in \mathbb{Z}} \alpha_{e+n} p^n = \beta_e p^{k_e}$$

for some integer $k_e \in \mathbb{Z}$ and unital element $\beta_e \in W_p(k)$. The only exception to this is if all the α_{e+n}'s are 0, so let $S \subseteq \Gamma'$ be the set of e for which this doesn't happen. Combining these representations for all $e \in S$, we have

$$\alpha = \sum_{e \in \Gamma} \alpha_e p^e = \sum_{e \in S} \beta_e p^{k_e + e}.$$

Since the exponents $k_e + e$ are all distinct for $e \in S$, we know that no like terms need to be combined in the above series. Additionally, since all the coefficients β_e are units, the coefficient of the lowest term in the series must certainly be a unit. This would complete the proof, assuming that the collection of values $k_e + e$ is well-ordered in Γ. Let T be the set of $e \in \Gamma$ such that $\alpha_e \neq 0$. For any $e \in S$, we know that

$$\beta_e p^{k_e + e} = \sum_{n \in \mathbb{Z}} \alpha_{e+n} p^{e+n} = \sum_{n \in U} \alpha_{e+n} p^{e+n}$$

where U is the set of n such that $\alpha_{e+n} \neq 0$ (i.e. $e + n \in T$. Notice that each term $\alpha_{e+n} p^{e+n}$ has valuation $\geq e + n$. Thus the valuation of the sum is at least as large as the smallest element of U added to e. Letting $u \in U$ be the minimal element, we have

$$v(\beta_e p^{k_e + e}) \geq u + e,$$

or

$$k_e + e \geq u + e$$

. However, we know that $k_e - u$ is an integer, so by this inequality it must be a nonnegative integer. Thus

$$k_e + e \geq (u + e) + n$$

for n some nonnegative integer. In particular, since $u + e \in U + e \subseteq T$ and $n \in \mathbb{Z}^{\geq 0}$, we have that $k_e + e \in T + \mathbb{Z}^{\geq 0}$. By Lemma 1 of [3], we know that $T + \mathbb{Z}^{\geq 0}$ is well-ordered, so the subset of $k_e + e$'s is well-ordered as well. Thus the β_e representation of α is a valid representation, completing the proof. □

This leads to a well-defined notion of valuation.

Definition 5.5. Let $\alpha \in W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ be nonzero, and let c be as in Theorem 5.4. We define the valuation function $v : W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]] \to \Gamma$ so that $v(\alpha) = c$. If $\alpha = 0$, we define $v(\alpha) = \infty$, as always.

Now we show that this is a valuation. First, though, let's define a new term for convenience.

Definition 5.6. We say that

$$\sum_{e\in\Gamma} \alpha_e p^e = \alpha$$

is a *unital representation* for α if there's a c such that α_c is a unit and $\alpha_e = 0$ for $e < c$.

Theorem 5.7. *The field $W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ along with the valuation v is a valued field with valuation group Γ and residue field k.*

Proof. To start, it's trivial that $v(0) = \infty$ and $v(\alpha) \neq \infty$ for $\alpha \neq 0$. Next, let $\alpha, \beta \in W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$. If one of them is 0, say a then $v(a + b) = \min(v(a), v(b)) = v(b)$. Otherwise, let

$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e$$

and

$$\beta = \sum_{e\in\Gamma} \beta_e p^e$$

be unital representations. Then we have

$$\alpha + \beta = \sum_{e\in\Gamma} (\alpha_e + \beta_e)p^e.$$

Let $c = \min(v(\alpha), v(\beta))$, and let d be the minimum number such that $\alpha_d + \beta_d \neq 0$. We know that $\alpha_e + \beta_e = 0$ for all $e < c$, meaning $d \geq c$. We also know that the actual valuation of $\alpha + \beta$ is $\geq d$ by Theorem 5.4. Thus $v(\alpha + \beta) \geq d \geq c = \min(v(\alpha), v(\beta))$. Next, consider $\alpha\beta$. If we multiply the series representations

$$\sum_{e\in\Gamma} \alpha_e p^e$$

and

$$\sum_{e\in\Gamma} \beta_e p^e$$

together, the lowest nonzero term is $\alpha_{v(\alpha)}\beta_{v(\beta)}p^{v(\alpha)+v(\beta)}$. We know that $\alpha_{v(\alpha)}$ and $\beta_{v(\beta)}$ are units so $\alpha_{v(\alpha)}\beta_{v(\beta)}$ is as well, and the product series representation is unital. Thus $v(\alpha\beta) = v(\alpha) + v(\beta)$. The final valuation property to check is the surjectivity of v. We know that $v(0) = \infty$, and for any $e \in \Gamma$ we have $v(1 \cdot p^e) = e$, so surjectivity is obvious.

Now we check the valuation group and residue field. By construction, it's easy to see that the valuation group is Γ. Next, let $\mathfrak{o}$ be the valuation ring and $\mathfrak{m}$ its maximal ideal. If $v(\alpha) \geq 0$, that means α has a unital representation with lowest nonzero term of index ≥ 0 (or $\alpha = 0$. Using the maximality criterion of Theorem 5.4, we can reduce this to the equivalent statement that α has some representation with only terms of index ≥ 0. That is, there's some representation

$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e$$

such that $\alpha_e = 0$ for $e < 0$. Similarly, if there's a sum

$$\alpha = \sum_{e\in\Gamma} \alpha_e p^e$$

where $\alpha_e = 0$ when $e \leq 0$, this is equivalent to saying that $v(\alpha) > 0$. This establishes $\mathfrak{o}$ and $\mathfrak{m}$. Now, define $i : k \to \mathfrak{o}/\mathfrak{m}$ by

$$i(x) = xp^0 + \mathfrak{m}.$$

Proving that $i(x + y) = i(x) + i(y)$ and $i(xy) = i(x)i(y)$ are trivial. If $x \neq 0$, then anything of the form

$$xp^0 + \sum_{e>0} \alpha_e p^e$$

has valuation 0 and can't be 0, so $i(x) \neq 0 + \mathfrak{m}$. Thus i is injective. Now, suppose that $\alpha + \mathfrak{m} \in \mathfrak{o}/\mathfrak{m}$. We know α can be expressed as

$$\alpha = \sum_{e \geq 0} \alpha_e p^e = \alpha_0 p^0 + \sum_{e>0} \alpha_e p^e \in \alpha_0 p^0 + \mathfrak{m}.$$

Thus $\alpha + \mathfrak{m} = i(\alpha_0)$, and i is surjective. What we've shown is that $i : k \to \mathfrak{o}/\mathfrak{m}$ is a field homomorphism, and so the residue field of $W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ is k. □

Now for the big result about fields of twisted Hahn series, whose proof I defer to [3]:

Theorem 5.8. *$W_p(k)[[T^\Gamma]]/W_p(k)[[\Gamma]]$ is spherically complete.*

Another important question for constructing Ω_p is when spherically complete fields are algebraically closed.

Definition 5.9. Let Γ be an abelian ordered group. We say that Γ is *divisible* if, for each $g \in \Gamma$, and integer $n > 0$, there's some $h \in \Gamma$ such that $nh = h + h + \cdots + h = g$.

Theorem 5.10. *Let K be a spherically complete field with residue field k and valuation group Γ. If k is algebraically closed and Γ is divisible, then K is algebraically closed.*

In the case of Ω_p, the valuation group and residue field we're interested in are $\mathbb{Q}$ and $\overline{\mathbb{F}}_p$, respectively. Even though the field of Hahn series in these isn't a possible Ω_p, the field of twisted Hahn series is! Specifically, $K := W_p(\overline{\mathbb{F}}_p)[[T^\mathbb{Q}]]/W_p(\overline{\mathbb{F}}_p)[[\mathbb{Q}]]$ is a maximal immediate extension of $\mathbb{C}_p$.

Theorem 5.11. *There exists an immediate valued-field embedding $f : \mathbb{C}_p \to K$. (As a result, K is a valid model for Ω_p.)*

Proof. To start, any valued field of characteristic 0 whose residue field has characteristic p has a copy of $\mathbb{Q}$ with the p-adic metric. Particularly, an embedding $a : \mathbb{Q} \to K$ exists. Since K is complete, this can be extended to a mapping $b : \mathbb{Q}_p \to K$. By Theorem 5, we know that K is algebraically closed, so b extends to a map $c : \overline{\mathbb{Q}_p} \to K$. By completness of K again, this extends to a map $f : \mathbb{C}_p \to K$.

Our next goal is to prove that f is an immediate extension. Since elements of the form $p^{\frac{m}{n}}$ are roots of $X^n - p^m$, they must be in the copy of $\overline{\mathbb{Q}}$ contained in K. The mapping $c : \overline{\mathbb{Q}_p} \to K$ has an algebraically closed image, im particular an image that contains $\overline{\mathbb{Q}}$. Thus elements $p^{\frac{m}{n}}$ get covered by c and therefore by f, so every $\frac{m}{n}$ in the valuation group $\mathbb{Q}$ gets accounted for. Thus the extension f preserves the valuation group, i.e. doesn't make it bigger.

The next thing to show is that f preserves the residue field. Suppose we have some element $\alpha + \mathfrak{m}$ in the residue field of K. We want to show that there exists some $\beta \in \mathbb{C}_p$ such that $f(\beta) + \mathfrak{m} = \alpha + \mathfrak{m}$. Since $\alpha + \mathfrak{m} \in \overline{\mathbb{F}}_p$, we know there exists a polynomial $S(x) \in \mathbb{F}_p[x]$ such that $S(\alpha + \mathfrak{m}) = 0 + \mathfrak{m}$. If we take S to be irreducible, then $\alpha + \mathfrak{m}$ is a simple root of S since $\overline{\mathbb{F}}_p$ is perfect over $\mathbb{F}_p$. By treating each coefficient of S as an integer $0 \leq n \leq p - 1$, we can lift S to a polynomial $T(x) \in \mathbb{Z}[x]$ such that $T(\alpha + \mathfrak{m}) = 0 + \mathfrak{m}$. In particular, we have that $T(\alpha) \in \mathfrak{m}$.

Since α is a simple root of T modulo $\mathfrak{m}$, the general form of Hensel's Lemma implies that there exists an $\alpha' \in \mathfrak{o}$ such that $\alpha' - \alpha \in \mathfrak{m}$ and $T(\alpha') = 0$. Since T is an integer polynomial, this particularly implies that α' is in the copy of $\overline{\mathbb{Q}}$ within K. By the same logic as befoe, we know that $\alpha' = f(\beta)$ for some $\beta \in \mathbb{C}_p$, and $f(\beta) + \mathfrak{m} = \alpha + \mathfrak{m}$. Thus f preserves the residue field, and is an immediate extension. Our proof is complete. □

This model of Ω_p is the most explicit model we currently have for a spherical completion of $\mathbb{C}_p$. The original proof that $\mathbb{C}_p$ had some maximal immediate extension used Zorn's Lemma in the construction of the extension. In our twisted Hahn series field, every element can be explicitly labelled, and addition, multiplication, and valuation are explicit constructions.

The problem with this construction, though, is that the embedding $f : \mathbb{C}_p \to \Omega_p$ is not itself explicit. In particular, the extension of the mapping $b : \mathbb{Q}_p \to K$ to $c : \overline{\mathbb{Q}_p} \to K$ is not unique nor explicit due to the weird behavior of algebraic closures. Ultimately, this caused a little bit of Zorn's Lemma (or the Axiom of Choice) to be used in our construction. In the future, we may find a more explicit way of creating a mapping $f : \mathbb{C}_p \to \Omega_p$, but we'll have to keep exploring.

References

[1] Michiel Hazewinkel. Witt vectors. part 1, 2008.

[2] Irving Kaplansky. Maximal fields with valuations. 1942.

[3] Bjorn Poonen. Maximally complete fields. *Enseign. Math*, 39(1-2):87–106, 1993.