p-adic Expansions

(and more on valued fields)

Siyan Daniel Li-Huerta

September 17, 2020

Base-p expansions give every element of $\mathbb{Z}/p^m\mathbb{Z}$ a unique representative in $\mathbb{Z}$ of the form

$$a_0 + a_1 p + \cdots + a_{m-1} p^{m-1},$$

where the $a_0, \ldots, a_{m-1}$ lie in $\{0, 1, \ldots, p-1\}$. For $m' \geq m$, an element of $\mathbb{Z}/p^{m'}\mathbb{Z}$ reduces to an element of $\mathbb{Z}/p^m\mathbb{Z}$ if and only if their digits $a_0, \ldots, a_{m-1}$ are equal. Hence elements of $\mathbb{Z}_p$ can be uniquely written as $a_0 + a_1 p + \cdots$, where the $a_0, a_1, \ldots$ lie in $\{0, 1, \ldots, p-1\}$. This is the element's *p-adic expansion*. Ring operations on p-adic expansions are performed via the classic digit-by-digit algorithm.

Example

- We have $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$. Indeed, one sees that adding 1 to the right-hand side yields 0.
- We have $\frac{1}{1-p} = 1 + p + p^2 + \cdots$. Indeed, one sees that multiplying the right-hand side by $1 - p$ yields 1.

So p-adic integers look like formal power series in the variable p, with coefficients in $\{0, 1, \ldots, p-1\}$.

Because $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, elements of $\mathbb{Q}_p$ can be uniquely written as

$$a_N p^N + a_{N+1} p^{N+1} + \cdots,$$

where N is an integer, the $a_N, a_{N+1}, \ldots$ lie in $\{0, 1, \ldots, p-1\}$, and $a_N \neq 0$. So p-adic numbers look like formal Laurent series in the variable p, with coefficients in $\{0, 1, \ldots, p-1\}$.

A *topological field* is a topological ring F that is a field such that the inverse map $F^\times \to F^\times$ is continuous.

Corollary

The topological field $\mathbb{Q}_p$ is locally compact.

Proof.

We already noted $\mathbb{Q}_p$ is Hausdorff. Inverses commute with $|\cdot|_p$, so the inverse map is continuous. Now the neighborhood $\mathbb{Z}_p$ of 0 is also closed, so it's its own closure. And it's compact. □

Note that $\mathbb{Q}_p$ and $\mathbb{R}$ are both complete locally compact topological fields!

Let F be a field. We can distinguish absolute values on F as follows:

Proposition

Let $|\cdot|_1$ and $|\cdot|_2$ be nontrivial norms on F.The following are equivalent:

1. $|\cdot|_1$ and $|\cdot|_2$ are isomorphic,
2. $|\cdot|_1$ and $|\cdot|_2$ induce the same topology on F,
3. Let x be in F. If $|x|_1 < 1$, then $|x|_2 < 1$.

Proof.

(1) $\implies$ (2): Open balls for $|\cdot|_1$ are precisely open balls for $|\cdot|_2$.
(2) $\implies$ (3): Note that $|x|_i < 1$ if and only if $x^n \to 0$ in the $|\cdot|_i$-topology.
(3) $\implies$ (1): By nontriviality, choose y in F with $|y|_1 > 1$. Then $|y^{-1}|_1 < 1$, so $|y^{-1}|_2 < 1$ and thus $|y|_2 > 1$.

For any x in $F^\times$, we have $|x|_1 = |y|_1^\alpha$ for some real α. Let a_n/b_n be a sequence of rationals converging to α from above with positive b_n. Then $|x|_1 < |y|_1^{a_n/b_n} = |y^{a_n}|_1^{1/b_n}$ and hence $|x^{b_n}/y^{a_n}|_1 < 1$, so $|x^{b_n}/y^{a_n}|_2 < 1$. Unraveling shows that $|x|_2 \leq |y|_2^\alpha$. Using a_n/b_n converging to α from below instead gives us $|x|_2 \geq |y|_2^\alpha$. Therefore $|\cdot|_1 = |\cdot|_2^{\log|y|_1/\log|y|_2}$. □

We'll use this to study what happens when F has multiple absolute values.

Theorem (Weak approximation)

Let $|\cdot|_1, \ldots, |\cdot|_d$ be nonisomorphic nontrivial norms on F, let $x_1, \ldots, x_d$ be in F, and let $\epsilon > 0$. Then there exists x in F such that $|x - x_i|_i < \epsilon$ for all $1 \leq i \leq d$.

Proof.

It suffices to find θ_i in F, for all $1 \leq i \leq d$, such that $|\theta_i|_i > 1$ and $|\theta_i|_j < 1$ for all $j \neq i$. To see this, note that $\frac{\theta_i^n}{1+\theta_i^n}$ converges to 1 with respect to $|\cdot|_i$ and to 0 with respect to $|\cdot|_j$. So we can take $x = \frac{x_1\theta_1^n}{1+\theta_1^n} + \cdots + \frac{x_d\theta_d^n}{1+\theta_d^n}$ for sufficiently large n.

Without loss of generality, we find θ_1. We induct on d. We have ρ and σ in F such that $|\rho|_1 < 1$, $|\rho|_d \geq 1$, $|\sigma|_1 \geq 1$, and $|\sigma|_d < 1$. So when $d = 2$, we can set $\theta_1 = \sigma/\rho$. Inductively, say we found θ_1' for $d - 1$. If $|\theta_1'|_d \leq 1$, then we can set $\theta_1 = \theta_1'^m \sigma/\rho$ for sufficiently large m. If $|\theta_1'|_d > 1$, then we can set $\theta_1 = \frac{\theta_1'^m}{1+\theta_1'^m}\sigma/\rho$ for sufficiently large m. □

Let $|\cdot|$ be a norm on F, and write $\widehat{F}$ for the completion of F. We'll study the following kind of normed fields.

Definition

We say $|\cdot|$ is *discretely valued* if the subgroup $|F^\times| \subseteq \mathbb{R}_{>0}$ is isomorphic to $\mathbb{Z}$.

Example

- For any prime p, the p-adic norm on $\mathbb{Q}$ or $\mathbb{Q}_p$ is discretely valued,
- The classic absolute value on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ is not discretely valued,
- Let F be any field. Then the trivial norm on F is not discretely valued.

Note that if $|\cdot|$ is discretely valued in F, it remains so on $\widehat{F}$.

Theorem (Ostrowski)

If $|\cdot|$ is archimedean and F is complete, then they are isomorphic to $\mathbb{R}$ or $\mathbb{C}$ with the classic absolute value.

Because we have a continuous field homomorphism $F \to \widehat{F}$, we see that if $|\cdot|$ is discretely valued, it must be nonarchimedean.

Now suppose $|\cdot|$ is nonarchimedean.

Definition

The *valuation ring* (or *ring of integers*) of F, denoted by $\mathcal{O}$, is the closed unit ball $\{x \in F \mid |x| \leq 1\}$.

Recall that the open unit ball $\mathfrak{m} = \{x \in F \mid |x| < 1\}$ is the unique maximal ideal of $\mathcal{O}$, i.e. $\mathcal{O}$ is a *local ring*. So $F = \mathcal{O}[\frac{1}{x}]$ for any x in $\mathfrak{m}$.

Example

- For the p-adic norm on $\mathbb{Q}_p$, we saw its valuation ring is $\mathbb{Z}_p$, with maximal ideal $p\mathbb{Z}_p$.
- For the p-adic norm on $\mathbb{Q}$, we see its valuation ring is the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at the prime ideal (p), with maximal ideal $p\mathbb{Z}_{(p)}$.
- For the trivial norm on any field, we see its valuation ring is F, with maximal ideal (0).

Let's also assume $|\cdot|$ is discretely valued, and let e be the smallest value it takes that's > 1. Then the associated valuation v takes values in $\mathbb{Z} \cup \{\infty\}$.

Definition

Let π be in F. We say π is a *uniformizer* if $v(\pi) = 1$.

Example

The element p is a uniformizer for $\mathbb{Q}_p$ with the p-adic norm. And so is $-p$, $p + p^{2020}$, and $p + p^2 + p^3 + \cdots$.

Choose a uniformizer π of F. Note that $\pi\mathcal{O} = \mathfrak{m}$.

Proposition

The nonzero ideals of $\mathcal{O}$ are all of the form $\pi^m\mathcal{O}$ for non-negative m.

Proof.

Let I be a nonzero ideal of $\mathcal{O}$, and let $m = \min\{v(x) \mid x \in I\}$. As $I \subseteq \mathcal{O}$, we see $m \geq 0$. For y in I attaining $v(y) = m$, we see $v(y/\pi^m) = 0$ and hence y/π^m lies in $\mathcal{O}$. So $\pi^m = (\pi^m/y)y$ is in I. For any x in I, we have $v(x) \geq m$ and thus $v(x/\pi^m) \geq 0$. So $x = \pi^m(x/\pi^m)$ lies in $\pi^m\mathcal{O}$. □

Proposition

The valuation ring $\mathcal{O}_F$ of F is dense in the valuation ring $\mathcal{O}_{\widehat{F}}$ of $\widehat{F}$.

Therefore $\mathcal{O}_{\widehat{F}}$ is also the completion of $\mathcal{O}_F$ with respect to $|\cdot|$.

Proof.

Let $\{x_n\}_{n=1}^{\infty}$ be a Cauchy sequence in F representing an element of $\mathcal{O}_{\widehat{F}}$. Then $|x_n|$ is eventually constant with value ≤ 1. Therefore these x_n lie in $\mathcal{O}_F$, so every element of $\mathcal{O}_{\widehat{F}}$ is the limit of a sequence in $\mathcal{O}_F$. □

Corollary

Inclusion $\mathcal{O}_F \to \mathcal{O}_{\widehat{F}}$ *yields an isomorphism* $\mathcal{O}_F/\pi^m\mathcal{O}_F \xrightarrow{\sim} \mathcal{O}_{\widehat{F}}/\pi^m\mathcal{O}_{\widehat{F}}$.

Proof.

As $\pi^m\mathcal{O}_F = \{x \in F \mid v(x) \geq m\}$, we have $\pi^m\mathcal{O}_{\widehat{F}} \cap \mathcal{O}_F = \pi^m\mathcal{O}_F$. Hence the above map is injective. For surjectivity, let x be in $\mathcal{O}_{\widehat{F}}/\pi^m\mathcal{O}_{\widehat{F}}$, and choose a representative $\widetilde{x}$ of x in $\mathcal{O}_{\widehat{F}}$. By the above, there exists y in $\mathcal{O}_F$ with $|\widetilde{x} - y| < 1/e^m$. Thus the image of y in $\mathcal{O}_F/\pi^m\mathcal{O}_F$ maps to x. □