CONSTRUCTIONS OF THE p-ADIC NUMBERS

ALEJANDRO GINORY

Contents

1. Introduction

As with many students of mathematics, I learned to construct the p-adic numbers in two seemingly different ways. The first way was as the fraction field of the projective limit of the family of commutative rings $\mathbb{Z}/p^n\mathbb{Z}$ under the canonical maps $(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to (\mathbb{Z}/p^n\mathbb{Z})$. The second was as the (metric) completion of the rational numbers under the p-adic metric. It is probably more 'natural' to learn it in the opposite order but my first exposure came from Jean-Pierre Serre's wonderful book *A Course in Arithmetic* where he mentions the second construction in passing.

While the two constructions exhibit striking similarities, it is not immediately obvious that they yield the same field (up to natural isometric isomorphism). In this article, we work out their equivalence.

2. p-adic Completion of $\mathbb{Q}$

In this approach, we redefine the notion of 'closeness' to reflect divisibility by a prime number of interest. Let p be a prime and and note that every nonzero rational number can be written in the form $p^n(a/b)$ where $a, b, n \in Z$ and

$$\gcd(a, p) = \gcd(b, p) = 1.$$

It is easy to see that n is uniquely determined, prompting the following definition.

Definition 2.1. Let $x = p^n(a/b) \in \mathbb{Q} - \{0\}$ where $a, b, n \in Z$ and $\gcd(a, p) = \gcd(b, p) = 1$ then the **p-adic absolute value** (sometimes referred to, somewhat inappropriately, as **p-adic norm**) of x, denoted $|x|_p$, is p^{-n}. We also define $|0|_p = 0$.

Definition 2.2. The **p-adic metric** (or **p-adic distance**) on $\mathbb{Q}$ is defined $d_p(x, y) = |x - y|_p$.

Before we continue, it is good manners to show that the above definitions make sense. It is enough to show for the absolute value.

Definition 2.3. Let R be a ring then a function $|\cdot| : R \to \mathbb{R}$ is called an **Archimedean absolute value on** R if it satisfies:

(i) (Positive Definite) For all $x \in R$, $|x| \geq 0$ with equality iff $x = 0$,
(ii) (Multiplicative) For all $x, y \in R$, $|x \cdot y| = |x| \cdot |y|$,
(iii) (Triangle Inequality) For all $x, y \in R$, $|x + y| \leq |x| + |y|$.

If property (iii) is replaced by the stronger property:

(iii)* For all $x, y \in R$, $|x + y| \leq \max\{|x|, |y|\}$,

then $|\cdot|$ is called a **non-Archimedean absolute value**.

Proposition 2.4. *The p-adic absolute value is a non-Archimedean absolute value on* $\mathbb{Q}$.

Proof. We run through the checklist. As noted in the first paragraph of this section, $|\cdot|_p$ is positive definite. Second, let $x = p^m(a/b)$ and $y = p^n(c/d)$ where all of the variables are integers, $cd \neq 0$, and p does not divide a, b, c, or d, then

$$|x \cdot y|_p = \left|p^{m+n}\left(\frac{ac}{bd}\right)\right|_p = p^{-(m+n)} = |x|_p \cdot |y|_p.$$

If $y = 0$, then clearly $|x \cdot 0|_p = |x|_p \cdot |0|_p$. As for the non-Archimedean property $|x + y|_p \leq \max\{|x|_p, |y|_p\}$, if both are 0 then it is clear. Let $x = p^m(a/b)$ and $y = p^n(c/d)$ as before but where $x \neq 0$ and $n \geq m$, then

$$|x + y|_p = \left|p^m\left(\frac{a + p^{n-m}c}{bd}\right)\right|_p \leq p^{-m} = \max\{|x|_p, |y|_p\}.$$

□

Recall that for any metric space M with metric d_M a Cauchy sequence $\{x_i\}_{i=1}^{\infty}$ is a sequence of points $x_i \in M$, $i \geq 1$, so that for all $\varepsilon > 0$ we can find a large enough N so that for all $i, j \geq N$, $d_M(x_i, x_j) < \varepsilon$. Let X is the set of all Cauchy sequences of M, the **completion of** M**,** denoted $\overline{M}$, is the set

$$\overline{M} = X/\sim$$

where $\{x_i\}_{i=1}^{\infty} \sim \{y_i\}_{i=1}^{\infty}$ if and only if $\lim_{i\to\infty} d_M(x_i, y_i) = 0$. An analogous definition applies to fields with absolute values, where we add and multiply (equivalence classes of) Cauchy sequences 'component-wise'. A *complete metric space* (resp. field) is a metric space (resp. field) where all Cauchy sequences converge. Completions of metric space and fields are complete.

Definition 2.5. The **p-adic numbers**, denoted $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the p-adic distance.

Note that every element of $\mathbb{Q}_p$ can be approximated by rational numbers a_i/b_i, $i \geq 1$, so that $\frac{a_i b_j - a_j b_i}{b_i b_j}$ are highly divisible by p as i and j both tend to infinity. To make this definition less 'wild' seeming, consider the following lemma.

Lemma 2.6. *For every Cauchy sequence $\{x_i\}_{i=1}^{\infty}$ in $\mathbb{Q}$, there exists a sequence $\{p^n k_i\}_{i=1}^{\infty}$ such that*

$$\{x_i\}_{i=1}^{\infty} \sim \{p^n k_i\}_{i=1}^{\infty}$$

where $n \in \mathbb{Z}$ is fixed, $k_i \in \mathbb{Z}$, and, when $\{x_i\}_{i=1}^{\infty}$ does not converge to 0,

$$\lim_{i\to\infty} |x_i|_p = p^{-n}.$$

Moreover, when $\{x_i\}_{i=1}^{\infty}$ does not converge to 0 we can choose the k_i so that $p \nmid k_i$.

Proof. If $\{x_i\}_{i=1}^{\infty}$ converges to 0, then the constant sequence $0, 0, \ldots$ does the trick. Suppose $\{x_i\}_{i=1}^{\infty}$ does not converge to zero and has no zero terms. Since non-Archimedean absolute values satisfy the triangle inequality, it follows that

$$|\, |x_i|_p - |x_j|_p \,| \leq |x_i - x_j|_p$$

(where the outside absolute values on the left are the standard ones) and so the sequence $\{|x_i|_p\}_i$ converges in $\mathbb{R}$. By the assumption that the sequence does not converge to zero, it converges to some p^{-n} for $n \in \mathbb{Z}$, since the complement $\{0\} \cup \{p^i\}_{i\in\mathbb{Z}}$ is open. This will be the n used in the desired sequence.

Choose $N > 0$ large enough so that $|x_i|_p = p^{-n}$ for all $i \geq N$. This means that we can write $x_i = p^n(a_i/b_i)$ where $p \nmid a_i b_i$ for all $i \geq N$. This means that $[b_i] \in \mathbb{Z}/p^i\mathbb{Z}$ is invertible and so there is an integer k_i, for $i \geq N$, so that

$$k_i b_i \equiv a_i \pmod{p^i}.$$

Note also that $p \nmid k_i$. It follows that the sequence $\{p^n k_i\}_{i\in\mathbb{N}}$, where $k_i (i < N)$ are arbitrarily chosen non-multiples of p, is equivalent to $\{x_i\}_{i\in\mathbb{N}}$ and $\lim_{i\to\infty} |x_i|_p = p^{-n}$. □

This little lemma will prove to be very useful in the upcoming discussion. Note, though, that the choice of the k_i in the proof is only unique modulo p^i as long as i is large enough. We will revisit this point of view after discussing the algebraic construction.

3. Algebraic Construction

As before, fix a prime number p and consider the system of commutative rings $\{\mathbb{Z}/p^n\mathbb{Z}\}_{n\geq 1}$ along with the canonical maps

$$\sigma_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$
$$[k] \mapsto [k], \quad \text{for } k \in \mathbb{Z}.$$

It is clear that this is a well-defined homomorphism for each $n \geq 1$. For the algebraic construction of the p-adic numbers, we require the notion of projective limit for rings.

Definition 3.1. Let $(\Lambda, \preceq)$ be a partially ordered set and $\{R_\lambda\}_{\lambda\in\Lambda}$ be a family of rings along with homomorphisms

$$\rho_{\alpha\beta} : R_\beta \to R_\alpha$$

for $\alpha \preceq \beta$ satisfying

$$\rho_{\alpha\alpha} = \mathrm{id}_{R_\alpha} \text{ and } \rho_{\alpha\beta} \circ \rho_{\beta\gamma} = \rho_{\alpha\gamma},$$

for $\alpha \preceq \beta \preceq \gamma$. The **projective limit** of $\{R_\lambda\}_{\lambda\in\Lambda}$ (and the homomorphisms) is

$$\varprojlim_{\lambda\in\Lambda} R_\lambda := \left\{ r \in \prod_{\lambda\in\Lambda} R_\lambda : \rho_{\alpha\beta}(\pi_\beta(r)) = \pi_\alpha(r) \text{ for } \alpha \preceq \beta \right\}$$

where π_λ are the natural projection maps.

Definition 3.2. Using the data in the first paragraph of this section (with the partially ordered set being the positive integers), the **p-adic integers** is the projective limit

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

The **p-adic numbers** is the fraction field $\mathbb{Q}_p := Frac(\mathbb{Z}_p)$.

We can represent elements in $\mathbb{Z}_p$ as sequences $([k_1], [k_2], \ldots, [k_n], \ldots)$ where $k_i \in \mathbb{Z}$ and $[k_i] \in \mathbb{Z}/p^i\mathbb{Z}$ with the property that for any $i, j \geq 1$ such that $i \leq j$,

$$k_j \equiv k_i \pmod{p^i}.$$

Again, the situation may seem rather 'wild' but, as in the previous section, there is some order.

Lemma 3.3. *Every element $x \in (\mathbb{Z}_p - \{0\})$ can be uniquely factored $x = p^n u$ where u is invertible in $\mathbb{Z}_p$ and $n \in \mathbb{N}$.*

Proof. Let $x = ([x_1], \ldots, [x_i], \ldots)$, then $x \neq 0$ implies that $[x_i] \neq 0$ for some i. Let n be the unique integer so that $[x_i] = 0$ for $i \leq n$ and $[x_j] \neq 0$ for $j > n$. This means that $p^n | x_j$ and $p^{n+1} \nmid x_j$ for all $j > n$, so we may write $u_j = x_j/p^n$. For $i \leq n$, recursively find u_i so that $[u_i] = \sigma_i([u_{i+1}])$ and, once this is done, notice that $[u_j] \neq 0$ for all $j \geq 1$. It follows that $[u_j]$ has an inverse $[v_j]$ in $\mathbb{Z}/p^j\mathbb{Z}$ and so

$$([u_1], \ldots, [u_j], \ldots) \cdot ([v_1], \ldots, [v_j], \ldots) = ([1], [1], \ldots).$$

Setting $u = ([u_1], \ldots, [u_j], \ldots)$ it is clear that $x = p^n u$ with u invertible.

Uniqueness follows from this computation

$$p^n u = p^m v$$

$$p^n u v^{-1} = p^m \cdot ([1], [1], \ldots),$$

where u, v are invertible, since it implies that $n = m$ (count the zeros) and that $[u_i]([v_i]^{-1}) = [1]$ for all $i > n$. The lower indexed terms are uniquely determined by the system's homomorphisms. □

Corollary 3.4. *Every element $x \in (\mathbb{Q}_p - \{0\})$ can be uniquely factored $x = p^n u$ where u is invertible in $\mathbb{Z}_p$ and $n \in \mathbb{Z}$.*

Using these facts, we can define an absolute value $|\cdot|_p$ on $\mathbb{Q}_p$ by $|p^n u| = p^{-n}$ for $u \in \mathbb{Z}_p$ invertible and $n \in \mathbb{Z}$, along with $|0|_p = 0$. The reader is encouraged to verify that this is a well-defined non-Archimedean absolute value.

4. Equivalence of Constructions

It is natural to ask if the completion of $\mathbb{Q}$ with respect to the p-adic absolute value, which we will denote $\overline{\mathbb{Q}}$ in this section, and the fraction field of the projective limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$, $n \geq 1$, with the p-adic absolute value are 'the same'. By the same, we mean a field isomorphism that preserves the absolute value, i.e., an isometric field isomorphism. The following theorem answers this in the affirmative.

Theorem 4.1. *The fields $\overline{\mathbb{Q}}$ and $Frac\left(\varprojlim \mathbb{Z}/p^n\mathbb{Z}\right)$, with their respective p-adic absolute values, are isometrically isomorphic as fields.*

Proof. Write $F = Frac\left(\varprojlim \mathbb{Z}/p^n\mathbb{Z}\right)$ for convenience. We will construct an isomorphism

$$\varphi : \overline{\mathbb{Q}} \to F$$

by systematically choosing a distinguished representative from each element of $\overline{\mathbb{Q}}$. Let $x \in \overline{\mathbb{Q}} - \{0\}$, then the lemma in the second section showed that x can be represented by a Cauchy sequence of the form $\{p^n k_i\}_{i=1}^{\infty}$ for $n, k_i \in \mathbb{Z}$, and where $p \nmid k_i$ for all $i \geq 1$. Since $\{p^n k_i\}_{i=1}^{\infty}$ is a Cauchy sequence, we can find a subsequence

$$\{p^n k_{N_1}, \ldots, p^n k_{N_2}, \ldots, p^n k_{N_i}, \ldots\}$$

satisfying

$$|k_{N_i} - k_{N_j}|_p \leq p^{-i}, \text{ for all } j \geq i.$$

Set $y_i = k_{N_i}$ and notice that

$$(*) \quad y_j \equiv y_i \pmod{p^i},\ j \geq i$$

for all $i \geq 1$. This assignment $x \mapsto \{p^n y_i\}_i$ is not unique, but it is well-behaved modulo powers of p in the following sense. If $\{p^n y_i'\}_i$ is another equivalent Cauchy sequence satisfying the property $(*)$ above, then for each $i \geq 1$,

$$y_j - y_j' \equiv y_i - y_i' \pmod{p^i},\ j \geq i,$$

but, by their equivalence, the left hand side goes to 0, i.e., p^i eventually divides the left side for all $j > N$ for some N. This means that $y_i' \equiv y_i \pmod{p^i}$. We can make the choice unique by choosing $y_i \in [1, \ldots, p^i - 1]$.

Now we can define the isomorphism as

$$\varphi(x) = p^n([y_1], [y_2], \ldots, [y_i], \ldots)$$

where $\{p^n y_i\}_i \in x$ is the distinguished representative discussed above and $\varphi(0) = 0$. The map is well-defined since the y_i satisfy $(*)$. The important thing to notice is that $([y_1], [y_2], \ldots)$ is a unit since $p \nmid y_i$ for $i \geq 1$. The map is clearly surjective by fact that every element of F can be written $p^n u$ where u is invertible (shown in the last lemma of section three) and if $u = ([u_1], [u_2], \ldots)$, $u_i \in \mathbb{Z}$, then $\{u_i\}_i$ is a Cauchy sequence. To show that it is injective, suppose $\varphi(x) = 0$, then $[y_{n+1}] = 0, [y_{n+2}] = 0, \ldots$, which implies that $x = 0$. It remains to show that φ preserves the absolute value, but indeed if $|x|_p = p^{-n}$ then

$$|\varphi(x)|_p = |p^n([y_1], \ldots)|_p = p^{-n}$$

since $([y_1], \ldots)$ is a unit. It follows that $\overline{\mathbb{Q}} \cong F$ isometrically. □

Department of Mathematics, Rutgers, The State University Of New Jersey, Piscataway, NJ 08854

E-mail address: aginory@math.rutgers.edu

URL: www.math.rutgers.edu/∼ag930