p-adic Numbers

Working towards p-adic expansions

Siyan Daniel Li-Huerta

September 15, 2020

Let's start with generalities on absolute values. Let F be a field, and let $|\cdot|$ be a norm on F. Note that $|1| = 1$ since $|1| \cdot |1| = |1^2| = |1|$. Also, any m-th root of unity ζ in F has norm 1, because $|\zeta|^m = |\zeta^m| = |1| = 1$. For all $x \neq 0$ in F, we similarly see that $|x^{-1}| = |x|^{-1}$.

Proposition

The following are equivalent:

1. For all x in F, we have $|x+1| \leq \max\{|x|, 1\}$,
2. For all x and y in F, we have $|x+y| \leq \max\{|x|, |y|\}$,
3. The set $|\mathbb{Z}|$ lies in $[0,1]$,
4. The set $|\mathbb{Z}|$ is bounded.

Proof.

(1) $\Longrightarrow$ (2): If $y = 0$, this becomes $|x| \leq \max\{|x|, 0\} = |x|$. If $y \neq 0$, dividing by $|y|$ shows this is equivalent to $|\frac{x}{y} + 1| \leq \max\{|\frac{x}{y}|, 1\}$.
(2) $\Longrightarrow$ (3): Since $|\pm 1| = 1$, this follows from induction via $|n \pm 1| \leq \max\{|n|, |\pm 1|\}$.
(3) $\Longrightarrow$ (4): Immediate, as $[0,1]$ is bounded.

Proposition

The following are equivalent:

1. For all x in F, we have $|x+1| \leq \max\{|x|, 1\}$,
2. For all x and y in F, we have $|x+y| \leq \max\{|x|, |y|\}$,
3. The set $|\mathbb{Z}|$ lies in $[0, 1]$,
4. The set $|\mathbb{Z}|$ is bounded.

Proof (continued).

(4) $\implies$ (1): Say $|\mathbb{Z}|$ lies in $[0, B]$ for some $B > 0$. For all x in F, we have

$$|x+1|^n = \left|\sum_{k=0}^{n} \binom{n}{k} x^k\right| \leq \sum_{k=0}^{n} \left|\binom{n}{k}\right| \cdot |x|^k \leq B \sum_{k=0}^{n} |x|^k \\ \leq B(n+1)\max\{|x|^n, 1\}.$$

Taking n-th roots yields $|x+1| \leq \sqrt[n]{B(n+1)}\max\{|x|, 1\}$, and taking $n \to \infty$ finishes the proof. □

Definition

If $|\cdot|$ satisfies these equivalent conditions, we say $|\cdot|$ is *nonarchimedean*. Otherwise, we say $|\cdot|$ is *archimedean*.

Condition (2) is called the *strong* or *ultrametric* triangle inequality.

Example

- For any prime p, the p-adic norm $|\cdot|_p$ on $\mathbb{Q}$ is nonarchimedean,
- Let F be field of positive characteristic. Then any norm on F is nonarchimedean,
- Let F be any field, and let $|\cdot|_0 : F \to \mathbb{R}_{\geq 0}$ be the indicator function on $F^\times$. This is the *trivial norm*, and it's always nonarchimedean.

Remark

These are sometimes called "rank-1" norms, since it's useful to let $|F^\times|$ take values in other totally ordered groups, like $\mathbb{R}^r_{>0}$ with the lexicographical order. This case would be "rank-r" norms. We will only work with rank-1 norms in this course.

We have an order-preserving bijection $\log : \mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{R}$, so we can interpret nonarchimedean norms as follows.

Definition

Let F be a field. A *valuation* on F is a function $v : F \to \mathbb{R} \cup \{\infty\}$ such that

- For all x in F, we have $v(x) = \infty$ if and only if $x = 0$,
- For all x and y in F, we have $v(xy) = v(x) + v(y)$,
- For all x and y in F, we have $v(x + y) \geq \min\{v(x), v(y)\}$.

Two valuations v_1 and v_2 on F are *isomorphic* if $v_1 = cv_2$ for some $c > 0$.

Choose $e > 1$. We see that valuations v and nonarchimedean norms $|\cdot|$ are equivalent concepts via setting $v(x) = -\log_e |x|$ and $|x| = e^{-v(x)}$. Different choices of e yield isomorphic valuations and norms.

Example

For any x in $\mathbb{Q}^\times$, write $x = \frac{a}{b}p^r$, where a and b are integers not divisible by p, and r is an integer. Then the map $v_p : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ sending $0 \mapsto \infty$ and $x \mapsto r$ is a valuation. We call this the *p-adic valuation*.

Let F be a field, and let $|\cdot|$ be a norm on F. Recall this induces a metric on F given by $(x, y) \mapsto |x - y|$, and the induced topological space structure on F makes it a *topological ring*, i.e. the addition and multiplication maps are continuous.

Proposition

Suppose $|\cdot|$ is nonarchimedean.

1. The unit closed ball $\mathcal{O} = \{x \in F \mid |x| \leq 1\}$ is a subring, and the unit open ball $\mathfrak{m} = \{x \in F \mid |x| < 1\}$ is the unique maximal ideal of $\mathcal{O}$.
2. A sequence $\{x_n\}_{n=1}^{\infty}$ in F is Cauchy if and only if $|x_n - x_{n+1}| \to 0$ as $n \to \infty$.

Proof.

1. Homework problem.
2. Cauchy immediately implies $|x_n - x_{n+1}| \to 0$ as $n \to \infty$. Conversely, let $\epsilon > 0$, and suppose $|x_n - x_{n+1}| < \epsilon$ for all $n \geq N$. Then, for all $m' \geq m \geq N$, we have

$$|x_m - x_{m'}| \leq \max\{|x_m - x_{m+1}|, \ldots, |x_{m'-1} - x_{m'}|\} < \epsilon.$$

□

Remark

Let $r > 0$. Your argument for (1) will also show that $B_c(0, r) = \{x \in F \mid |x| \leq r\}$ and $B_o(0, r) = \{x \in F \mid |x| < r\}$ are subgroups. Because $B_o(0, r)$ lies in $B_c(0, r)$, the latter is a union of $B_o(0, r)$-cosets, so this implies $B_c(0, r)$ is also open! As $r \to 0$, note that the $B_c(0, r)$ forms a basis of **open and closed** neighborhoods of 0. So F is *totally disconnected*.

Recall we defined the p-adic numbers $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$. Our $|\cdot|_p$ extends uniquely to $\mathbb{Q}_p$, and by continuity it continues to take values in $\{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$.

Definition

The *p-adic integers*, denoted by $\mathbb{Z}_p$, is the completion of $\mathbb{Z}$ with respect to the metric induced by $|\cdot|_p$.

Recall that this is also the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$. Also observe that, for x in $\mathbb{Z}$ and any non-negative integer r, we have $v_p(x) \geq r$ if and only if p^r divides x. Hence "small" in the p-adic norm means divisible by a large power of p.

Let's find a hands-on way to describe elements of $\mathbb{Z}_p$. Form the projective system $(\mathbb{Z}/p^m\mathbb{Z})_{m=1}^{\infty}$, where $\mathbb{Z}/p^m\mathbb{Z}$ has the discrete topology, and the maps $\mathbb{Z}/p^{m'}\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ are given by reduction mod p^m for $m' \geq m$.

Proposition

We have an isomorphism of topological rings $\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$.

Proof.

Let $\{x_n\}_{n=1}^{\infty}$ be a Cauchy sequence in $\mathbb{Z}$. Then the image of $\{x_n\}_{n=1}^{\infty}$ in $\mathbb{Z}/p^m\mathbb{Z}$ is eventually constant. Call it c_m. The Cauchyness of $\{x_n\}_{n=1}^{\infty}$ implies that $(c_m)_{m=1}^{\infty}$ is an element of $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$. If $x_n \to 0$, we see that $c_m = 0$, so the assignment $\{x_n\}_{n=1}^{\infty} \mapsto (c_m)_{m=1}^{\infty}$ yields a well-defined map $\mathbb{Z}_p \to \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$. Since reduction mod p^m is a ring homomorphism, so is this map.

In the other direction, let $(y_m)_{m=1}^{\infty}$ be in $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$, and choose representatives $\widetilde{y}_m$ of y_m in $\mathbb{Z}$. For $m' \geq m \geq N$, we have $\widetilde{y}_m \equiv y_N \equiv \widetilde{y}_{m'}$ mod p^N, so $\{\widetilde{y}_m\}_{m=1}^{\infty}$ is a Cauchy sequence in $\mathbb{Z}$. Any other choice of representatives differs from $\{\widetilde{y}_m\}_{m=1}^{\infty}$ by a sequence converging to 0, so the assignment $(y_m)_{m=1}^{\infty} \mapsto \{\widetilde{y}_m\}_{m=1}^{\infty}$ gives a well-defined map.

Proposition

We have an isomorphism of topological rings $\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$.

Proof (continued).

We immediately see $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}_p \to \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$ is the identity. For the other composition, let $\{x_n\}_{n=1}^{\infty}$ be a Cauchy sequence in $\mathbb{Z}$, form $(c_m)_{m=1}^{\infty}$ in $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$ as before, and choose representatives $\widetilde{c}_m$ of c_m in $\mathbb{Z}$. We see that the image of $\{x_n - \widetilde{c}_n\}_{n=1}^{\infty}$ in $\mathbb{Z}/p^m\mathbb{Z}$ stabilizes to 0 as soon as the image of $\{x_n\}_{n=1}^{\infty}$ in $\mathbb{Z}/p^m\mathbb{Z}$ stabilizes to c_m, so $\{x_n - \widetilde{c}_n\}_{n=1}^{\infty}$ converges to 0.

Note $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$ is compact and $\mathbb{Z}_p$ is Hausdorff. Therefore to check that this bijection is a homeomorphism, it suffices to check that $\mathbb{Z}_p \to \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$ is open. We can check this on neighborhoods of 0, and the image of $\{x \in \mathbb{Z}_p \mid |x|_p \leq 1/p^N\}$ is the intersection of $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$ with $(\prod_{m=N+1}^{\infty} \mathbb{Z}/p^m\mathbb{Z}) \times \{0\}^N$, which is open. □

In particular, note that $\mathbb{Z}_p$ is compact.

Corollary

1. *Let a be an integer not divisible by p. Then a is invertible in $\mathbb{Z}_p$.*
2. *The subset $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ equals the closed unit ball $\{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$.*

Proof.

1. The image of a is invertible in $\mathbb{Z}/p^m\mathbb{Z}$ and hence in $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$.
2. As $|\mathbb{Z}|_p$ lies in $[0,1]$, we see $\mathbb{Z}_p$ lies in the closed unit ball. Conversely, let $\{x_n\}_{n=1}^{\infty}$ be a Cauchy sequence in $\mathbb{Q}$ representing an element of the closed unit ball. Then $|x_n|_p$ is eventually constant with value ≤ 1. Therefore these x_n can be written as $\frac{a}{b}p^r$, where a and b are integers not divisible by p, and r is a non-negative integer. By (1), x_n lies in $\mathbb{Z}_p$, so its limit x also lies in $\mathbb{Z}_p$. □

As $|\cdot|_p$ takes values in $\{0\} \cup \{p^r \mid r \in \mathbb{Z}\}$, we see the open unit ball in $\mathbb{Q}_p$ is $p\mathbb{Z}_p$. We have $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p = \mathbb{Z}_p[\frac{1}{p}]$. For integers $N \geq 0$, note that $p^N\mathbb{Z}_p$ is the kernel of $\varprojlim_m \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^N\mathbb{Z}$, so we have $\mathbb{Z}_p/p^N\mathbb{Z}_p \xrightarrow{\sim} \mathbb{Z}/p^N\mathbb{Z}$.