MATH8510
Lecture 6 Notes

Charlie Conneen

September 5, 2022

Basic Properties of $\mathbb{Q}_p$

For this lecture, fix a prime p. Recall that $(\mathbb{Q}_p, |\cdot|_p)$ is a complete non-Archimedean field with $\mathbb{Q}$ a dense subfield such that

$$\left|\mathbb{Q}^\times\right|_p = \left|\mathbb{Q}_p^\times\right|_p = p^{\mathbb{Z}}.$$

Definition. The **p-adic valuation** $\mathrm{ord}_p : \mathbb{Q}_p \to \mathbb{Z} \cup \{\infty\}$ is given by

$$\mathrm{ord}_p(x) := -\log_p |x|_p$$

for all $x \in \mathbb{Q}_p$.

Definition. The ring of **p-adic integers** is the closed unit ball

$$\mathbb{Z}_p := \left\{x \in \mathcal{Q}_p \mid |x|_p \leq 1\right\}$$

in $\mathbb{Q}_p$.

Note that ord_p is a *normalized* discrete valuation, i.e. $\mathrm{ord}_p : \mathbb{Q}_p^\times \twoheadrightarrow \mathbb{Z}$ is a surjective homomorphism. Since we can always restrict the codomain of a valuation to its image, this will not be a problem.

Remark. Observe that

$$\begin{aligned} p\mathbb{Z}_p &= \left\{px \in \mathbb{Q}_p \mid |x|_p \leq 1\right\} = \left\{y \in \mathbb{Q}_p \mid \left|p^{-1}y\right|_p \leq 1\right\} \\ &= \left\{y \in \mathbb{Q}_p \mid |y|_p \leq p^{-1}\right\} = \left\{x \in \mathbb{Q}_p \mid |y|_p < 1\right\} \end{aligned}$$

and that this is the unique maximal ideal in $\mathbb{Z}_p$. Consequently,

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \mid |x|_p = 1\right\} = \{x \in \mathbb{Q}_p \mid \mathrm{ord}_p(x) = 0\}.$$

Remark. The localization of $\mathbb{Z}$ at the prime (p) can be regarded as a subring of the p-adic integers:

$$\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z}\right\} = \{x \in \mathbb{Q} \mid \mathrm{ord}_p(x) \geq 0\} = \mathbb{Q} \cap \mathbb{Z}_p.$$

We can also quickly see that

$$p^n\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \operatorname{ord}_p(x) \geq n\}$$

and thus $p^n\mathbb{Z}_{(p)} = \mathbb{Q} \cap p^n\mathbb{Z}_p$ for all $n \in \mathbb{N}$.

Theorem. *The following are true:*

a. The open balls in $\mathbb{Q}_p$ are precisely the sets of the form $c + p^n\mathbb{Z}_p$ with $c \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$;

b. The proper nonzero ideals in $\mathbb{Z}_p$ are precisely the balls $p\mathbb{Z}_p, p^2\mathbb{Z}_p, p^3\mathbb{Z}_p, \ldots$

c. $\mathbb{Z}$ is a dense subring of $\mathbb{Z}_p$. Furthermore, $\mathbb{N}$ is dense in $\mathbb{Z}_p$.

Proof. For (a), given $c \in \mathbb{Q}_p$ and $r > 0$, pick the least $n \in \mathbb{Z}$ such that $p^{-n} < r$. Then

$$\begin{aligned} B_r(c) &= \left\{x \in \mathbb{Q}_p \mid |x - c|_p < r\right\} = \left\{x \in \mathbb{Q}_p \mid |x - c|_p \leq p^{-n}\right\} \\ &= \left\{c + y \in \mathbb{Q}_p \mid |y|_p \leq p^{-n}\right\} = c + p^n\mathbb{Z}_p. \end{aligned}$$

This suffices. For (b), given a proper nonzero ideal $I \subseteq \mathbb{Z}_p$, we can see that

$$\infty \subsetneq \operatorname{ord}_p(I) \subset \mathbb{N} \cup \{\infty\}$$

and so $n = \min(\operatorname{ord}_p(I))$ exists in $\mathbb{N}$, and there exists some $x_0 \in I$ such that $\operatorname{ord}_p(x_0) = n$. Therefore $x_0\mathbb{Z}_p \subseteq I \subseteq p^n\mathbb{Z}_p$. Now since $x_0^{-1}p^n \in \mathbb{Z}_p^\times$, we have that

$$x_0\mathbb{Z}_p = x_0\left(x_0^{-1}p^n\mathbb{Z}_p\right) = p^n\mathbb{Z}_p,$$

hence $I = p^n\mathbb{Z}_p$.

For (c), suppose $U = c + p^n\mathbb{Z}_p$ is an open ball in $\mathbb{Z}_p$. Then $c \in \mathbb{Z}_p$ and $n \geq 0$. We are tasked with finding some $m \in \mathbb{N}$ such that $m \in U$.

If $c = 0$ or if $n = 0$, then $m = p^n$ works. So assume $n > 0$. Now by density of $\mathbb{Q}$ in $(\mathbb{Q}_p, |\cdot|_p)$, there exists a (reduced) rational number $\frac{a}{b} \in U$. Then

$$\left|\frac{a}{b} - c\right|_p \leq p^{-n} \quad \text{and} \quad \left|\frac{a}{b}\right|_p \leq 1,$$

So we obtain $\gcd(p^n, b) = 1$, and there exists some $k \in \mathbb{Z}$ and $m \in \mathbb{N}$ such that

$$kp^n + mb = a,$$

and therefore

$$\left|m - \frac{a}{b}\right|_p = \left|\frac{-kp^n}{b}\right|_p \leq p^{-n}$$

From here, the strong triangle inequality implies

$$|m - c|_p \leq p^{-n}.$$

Therefore $m \in c + p^n\mathbb{Z}_p$. This suffices. ■

$$\begin{tikzcd}[column sep=small]
\mathbb{N} \arrow[rrrrrr, bend right, "\text{“is dense in”}"'] & \subsetneq & \mathbb{Z} & \subsetneq & \mathbb{Z}_{(p)} & \subsetneq & \mathbb{Z}_p
\end{tikzcd}$$

Theorem. *For $n \in \mathbb{N}$, there is an isomorphism of rings*

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

In particular, $\{0, 1, \ldots, p^n - 1\}$ is a complete set of representatives for the cosets of $p^n\mathbb{Z}_p \subseteq \mathbb{Z}_p$.

Proof. Fix $n \in \mathbb{N}$ and define $\varphi : \mathbb{Z} \to \mathbb{Z}_p/p^n\mathbb{Z}_p$ given by

$$\varphi(x) := x + p^n\mathbb{Z}_p.$$

One can quickly verify that this is indeed a ring homomorphism. Suppose $c + p^n\mathbb{Z}_p \in \mathbb{Z}_p/p^n\mathbb{Z}_p$. By density of $\mathbb{Z} \subseteq \mathbb{Z}_p$, there exists some $m \in \mathbb{Z}$ such that $m \in c + p^n\mathbb{Z}_p$. Then $\varphi(m) = m + p^n\mathbb{Z}_p = c + p^n\mathbb{Z}_p$, so φ is surjective. Furthermore,

$$\varphi(x) = p^n\mathbb{Z}_p \iff x \in \mathbb{Z} \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}_p,$$

so $\ker(\varphi) = p^n\mathbb{Z}$. So the first isomorphism theorem concludes the proof. ∎

Corollary. *The residue field of $\mathbb{Q}_p$ is $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.* ∎

Theorem. *Every $x \in \mathbb{Z}_p$ has a unique series representation*

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

where $d_n \in \{0, 1, \ldots, p-1\}$ for all $n \in \mathbb{N}$.

Proof. Fix $x \in \mathbb{Z}_p$. Now let $y_0 = x$ and let d_0 be the unique element of $\{0, 1, \ldots, p-1\}$ such that $y_0 \in d_0 + p\mathbb{Z}_p$. We inductively construct the sequences $(d_n)_n$ and $(y_n)_n$ as follows: for $n + 1 \in \mathbb{N}$, define

$$y_{n+1} = p^{-1}\left(y_{n-1} - d_{n-1}\right) \in \mathbb{Z}_p,$$

and let d_{n+1} be the unique element of $\{0, 1, \ldots, p-1\}$ such that $y_n \in d_n + p\mathbb{Z}_p$. Doing this for all $n \in \mathbb{N}$, we find that

$$x - \sum_{n=0}^{k-1} d_n p^n = x - \sum_{n=0}^{k-1} \left(p^n y_n - p^{n+1} y_{n+1}\right) = x - (y_0 - p^k y_k) = p^k y_k,$$

therefore $\left| x - \sum_{n=0}^{k-1} d_n p^n \right|_p \leq p^{-k}$ for all k. So $x = \lim_{n\to\infty} \sum_{n=0}^{k-1} d_n p^n = \sum_{n=0}^{\infty} d_n p^n$, as required. ∎

Corollary. *Every $x \in \mathbb{Q}_p^\times$ has a unique series expansion $x = \sum_{n=v}^{\infty} d_n p^n$ with $d_n \in \{0, 1, \ldots, p-1\}$ for all $n \in \mathbb{N}$, and $d_v \neq 0$. In this case $\operatorname{ord}_p(x) = v$.*