MATH8510
Lecture 8 Notes

Charlie Conneen

September 9, 2022

Elementary Properties of $\mathbb{Q}_p$ (continued)

The following proposition lists a few easy but useful equivalences to keep in mind.

Proposition. *If $x, y \in \mathbb{Z}_p$ and $n \in \mathbb{N}$, the following are equivalent:*

1. $|x-y|_p \le p^{-n}$;
2. $x \equiv y \mod p^n\mathbb{Z}_p$;
3. $x + p^n\mathbb{Z}_p = y + p^n\mathbb{Z}_p$;
4. $\mathrm{ord}_p(x-y) \ge n$.

Recall the "tree-like" structure we saw on $\mathbb{Z}_p$ from last lecture. The fact that every node in that tree has only finitely many branches is a consequence of the fact that the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is finite. We can still draw the same kind of tree picture for other valuation rings, but the number of branches will be instead the cardinality of the residue field.

We also make a note of the fact that ord_p is *discrete*, i.e. $\mathrm{ord}_p(\mathbb{Z}_p) = \mathbb{Z}$ is a discrete subgroup of $\mathbb{R}$. The fact that the tree diagram from last lecture is accurate is due to this fact, and the story will not be the same in $\overline{\mathbb{Q}_p}$ nor in $\mathbb{C}_p$.

Theorem. *For each prime p, $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact.*

Proof. Fix $\varepsilon > 0$ and choose $n \in \mathbb{N}$ sufficiently large such that $p^{-n} \le \varepsilon$. Then

$$\mathbb{Z}_p = \bigcup_{d=0}^{p^n-1} (d + p^n\mathbb{Z}_p) = \bigcup_{d=0}^{p^n-1} B_{p^{-n}}(d) = \bigcup_{d=0}^{p^n-1} B_\varepsilon(d).$$

Since we can do this for all $\varepsilon > 0$, this shows that $\mathbb{Z}_p$ is totally bounded. So to show compactness, it suffices to check that $\mathbb{Z}_p$ is complete with respect to $|\cdot|_p$. This is easily checked. So $\mathbb{Z}_p$ is complete and totally bounded, hence compact.

Now take any $x_0 \in \mathbb{Q}_p$. Since the map $\mathbb{Z}_p \to x_0 + \mathbb{Z}_p$ is a homeomorphism (by a homework problem), we can see that $x_0 + \mathbb{Z}_p$ is a compact open neighbourhood of x_0. This shows that $\mathbb{Q}_p$ is locally compact. ■

Building Towards Hensel's Lemma

Proposition. *Let R be a ring, $q(X) = c_0 + c_1 X + \cdots + c_d X^d \in R[X]$ a polynomial in R. The formal derivative of $q(x)$:*

$$q'(x) \coloneqq c_1 + 2c_2 X + 3c_3 X^2 + \cdots + dc_d X^{d-1}$$

and the polynomial $\widetilde{q}(X, Y) \in R[X, Y]$ given by

$$\widetilde{q}(X, Y) \coloneqq \sum_{i=0}^{d-2} c_{i+2} \sum_{j=0}^{i} \binom{i+2}{j+2} X^{i-j} Y^j$$

satisfy the following equality:

$$q(X + Y) = q(X) + Y q'(X) + Y^2 \widetilde{q}(X, Y).$$

Proof. This can be verified directly. ∎

Corollary. *If $q(X) \in \mathbb{Z}_p[X, Y]$ and $q : \mathbb{Z}_p \to \mathbb{Z}_p$ is the evaluation map associated to $q(X)$, then the following are true:*

1. *If $c \in \mathbb{Z}_p$, then either $q(c + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$ or $q(c + p\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times$.*
2. *If $c \in \mathbb{Z}_p$ satisfies $q'(c) \in \mathbb{Z}_p^\times$, then there exists at most one $x \in c + p\mathbb{Z}_p$ such that $q(x) = 0$.*

Proof. Suppose $c \in \mathbb{Z}_p$. For each $x \in c + p\mathbb{Z}_p$, we have

$$q(x) = q(c + (x - c)) = q(c) + (x - c)q'(c) + (x - c)^2 \widetilde{q}(x, x - c).$$

This means $q(x) = q(c) + (x - c)z$ for some $z \in \mathbb{Z}_p$. There are two cases: if $q(c) \in p\mathbb{Z}_p$, then

$$|q(x)| \leq \max\left\{ |q(c)|_p, |(x - c)z|_p \right\} \leq 1$$

So $q(x) \in p\mathbb{Z}_p$. So this would mean that $q(c + p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$. Otherwise, $q(c) \in \mathbb{Z}_p^\times$, which would yield $|q(c)|_p = 1 \geq |(x - c)z|_p$. Then the strong triangle *equality* says

$$|q(x)|_p = \max\left\{ |q(c)|_p, |(x - c)z|_p \right\} = 1.$$

Then $q(x) \in \mathbb{Z}_p^\times$, so $q(c + p\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times$.

As for (b), suppose $c \in \mathbb{Z}_p$ satisfies $q'(c) \in \mathbb{Z}_p^\times$ (i.e. $|q'(c)|_p = 1$). Then if $x, y \in c + p\mathbb{Z}_p$ and $q(x) = q(y) = 0$, then

$$0 = q(y) = q(x + (y - x)) = q(x) + (y - x)q'(x) + (y - x)^2 \widetilde{q}(x, y - x)$$

meaning $(y - x)(q'(x) + (y - x)\widetilde{q}(x, y - x)) = 0$. So $q'(x) \in \mathbb{Z}_p^\times$ by part (a), so $|q'(x)|_p = 1$, and $|\widetilde{q}(x, y - x)|_p \leq 1$, and thus

$$|(y - x)\widetilde{q}(x, y - x)|_p < 1.$$

So the strong triangle inequality yields $|q'(x) + (y - x)\widetilde{q}(x, y - x)|_p = 1$. So $x = y$. ∎