MATH-480 Senior Seminar Feb 9-18, 2016

P-adic Numbers

Lecturer: David Yao *Lecture 3-6*

Contents

1 Introduction: Hensel's Analogy

Consider the ring $\mathbb{C}[x]$. By Fundamental Theorem of Algebra, every element can be written as the product of linear terms. This is the unique factorization in this ring, and the linear polynomials in the form $x - \alpha$ generate exactly all the prime ideals in the ring, hence are the primes in $\mathbb{C}[x]$.

Now pick a prime $x - \alpha$, each element in $\mathbb{C}[x]$ also has a Taylor expansion around α, namely

$$p(x) = \sum_{i=0}^{n} a_i (x - \alpha)^i$$

In fact, let $\mathbb{C}(x)$ be the field of fractions of $\mathbb{C}[x]$, that is, all rational functions. From complex analysis, we have the Laurent expansion around α, written as

$$\frac{p(x)}{q(x)} = \sum_{i=n_0}^{\infty} a_i (x - \alpha)^i$$

where n_0 can be negative. We then say that the function has a pole at α of order $-n_0$. Here we consider the expansion as formal objects, thus not worrying about the convergence.

All the formal finite-tailed (finite on the negative end) Laurent series in $(x - \alpha)$ actually form a field, $\mathbb{C}((x - \alpha))$. Note that this field is larger than $\mathbb{C}(x)$, since from calculus we know that the functions e^x or $sin(x)$ have Taylor expansions in $\mathbb{C}((x - \alpha))$ but are not rational functions. Therefore we have the following injections:

$$Frac(\mathbb{C}[x]) \cong \mathbb{C}(x) \hookrightarrow \mathbb{C}((x - \alpha))$$

Analogously, in $\mathbb{Z}$, we can pick a prime p. Each positive integer has a base-p expansion:

$$m = \sum_{i=0}^{n} a_i p^i$$

where $0 \leq a_i < p$. Formally, we can then write each positive rational number in $Frac(\mathbb{Z}) \cong \mathbb{Q}$ in terms of powers of p by "long division", just as in the Laurent expansion:

$$\frac{a}{b} = \frac{\sum_{i=0}^{n} a_i p^i}{\sum_{i=0}^{m} b_i p^i} = \sum_{i=n_0}^{\infty} c_i p^i$$

where $0 \leq c_i < p$.

Example: $p = 3$, $a = 24 = 2p + 2p^2$, $b = 17 = 2 + 2p + p^2$, $\frac{24}{17} = \frac{2p+2p^2}{2+2p+p^2} = p + p^3 + 2p^5 + \ldots$

Example: $-1 = \frac{-1}{1} = (p-1) + (p-1)p + (p-1)p^2 + \ldots$, true for any prime p.

All such finite-tailed expansions form a field $\mathbb{Q}_p$, hence we have the injection:

$$Frac(\mathbb{Z}) \cong \mathbb{Q} \hookrightarrow \mathbb{Q}_p$$

where $\mathbb{Q}_p$ is the field of p-adic numbers.

2 Absolute value and Ultrametric space

2.1 Basics

Definition 2.1 *Let $\mathbb{K}$ be a field, and $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$. An absolute value on $\mathbb{K}$ is a function*

$$|\cdot| : \mathbb{K} \to \mathbb{R}_+$$

that satisfies:

1. $|x| = 0$ *iff* $x = 0$
2. $\forall x, y \in \mathbb{K}, |xy| = |x||y|$
3. $\forall x, y \in \mathbb{K}, |x + y| \leq |x| + |y|$

We say an absolute value on $\mathbb{K}$ is non-archimedean if it satisfies a stronger triangle inequality, and call $\mathbb{K}$ with the non-archimedean absolute value "ultrametric".

4. $\forall x, y \in \mathbb{K}, |x + y| \leq \max\{|x|, |y|\}$

The trivial absolute value is defined by $|x| = \begin{cases} 0, & x = 0 \\ 1, & o.w. \end{cases}$

Lemma 2.2 *For any absolute value on $\mathbb{K}$, we have*

1. $|1| = 1$
2. *If $x \in \mathbb{K}$ and $|x^n| = 1$, then $|x| = 1$*
3. $|-1| = 1$
4. $|-x| = |x|$
5. *If $\mathbb{K}$ is finite, then $|\cdot|$ is trivial.*

Proof

1. $|1| = |1^2| = |1|^2$, $|1| \neq 0$, so $|1| = 1$
2. $|x|^n = 1$, $|x| \geq 0$, so $|x| = 1$
3. $|-1|^2 = |1| = 1$, so $|-1| = 1$
4. $|-x| = |-1||x| = |x|$
5. For any $x \neq 0$, $\exists n, x^n = 1$, $|x^n| = 1$, so $|x| = 1$ ■

Proposition 2.3 *Let $\mathbb{K}$ with $|\cdot|$ be an ultrametric space. If $|x| \neq |y|$ then*

$$|x+y| = \max\{|x|, |y|\}$$

Proof WLOG, suppose $|x| > |y|$, then $|x+y| \leq |x|$.
But $x = (x+y) + (-y)$, so $|x| \leq \max\{|x+y|, |y|\}$. Since $|x| > |y|$, we have $|x| \leq |x+y|$.
Therefore $|x| = |x+y|$. ■

Corollary 2.4 *In an ultrametric space, all triangles are isosceles.*
Proof If $|x-y| \neq |y-z|$ then $|x-z| = \max\{|x-y|, |y-z|\}$. ■

2.2 Algebra

Definition 2.5 *Let $\mathbb{K}$ be a field, a valuation v on $\mathbb{K}$ is a map*

$$v : \mathbb{K} \to \mathbb{R} \cup \{\infty\}$$

satisfying
1. $v(xy) = v(x) + v(y)$
2. $v(x+y) \geq \min\{v(x), v(y)\}$
3. $v(x) = \infty$ *iff* $x = 0$.

The image of $\mathbb{K}^\times$ under v is an additive group called the value group of v.
Remark If v is a valuation, then $|x|_v = e^{-v(x)}$ defines a non-archimedean absolute value on $\mathbb{R}$. Conversely, if $|\cdot|$ is a non-archimedean absolute value, then $-\log|\cdot|$ is a valuation.

Proposition 2.6 *Let $\mathbb{K}$ be a field, let $|\cdot|$ be a non-archimedean absolute value, the set*

$$\mathcal{O} = \overline{B}(0,1) = \{x \in \mathbb{K} : |x| \leq 1\}$$

is a subring of $\mathbb{K}$. Its subset

$$\mathcal{B} = B(0,1) = \{x \in \mathbb{K} : |x| < 1\}$$

is a maximal ideal of $\mathcal{O}$, and every element in $\mathcal{O} \setminus \mathcal{B}$ is invertible in $\mathcal{O}$.
Proof 1. $\mathcal{O}$ is a subring: $0, 1 \in \mathcal{O}$, and it is closed under multiplication, taking negative and addition, by the non-archimedean property.

2. $\mathcal{B}$ is closed under addition, has 0 and $x \in \mathcal{O}, y \in \mathcal{B}$, $|xy| < 1$ so $xy \in \mathcal{B}$.

3. $x \in \mathcal{O} \setminus \mathcal{B}$, $|x| = 1$ so $|x^{-1}| = 1$, $x^{-1} \in \mathcal{O} \setminus \mathcal{B}$. In fact, $\mathcal{O}^\times = \mathcal{O} \setminus \mathcal{B}$ since all elements in $\mathcal{B}$ are not invertible in $\mathcal{O}$ as their inverses have norm greater than 1. It follows that $\mathcal{B}$ is a maximal ideal, and $\mathcal{O}/\mathcal{B}$ is a field. ■

Definition 2.7 *The ring $\mathcal{O}$ is called the valuation ring of $|\cdot|$, the ideal $\mathcal{B}$ is called the valuation ideal, and the quotient $\mathcal{K} = \mathcal{O}/\mathcal{B}$ is called the residue field.*

2.3 p-adic valuation

Definition 2.8 *Fix a prime $p \in \mathbb{Z}$, the p-adic valuation v_p on $\mathbb{Z}$ is given by letting $v_p(n)$ be the unique positive integer satisfying*

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'$$

To extend v_p to the field of rational numbers: if $x = \frac{a}{b} \in \mathbb{Q}^\times$, then

$$v_p(x) = v_p(a) - v_p(b)$$

Definition 2.9 *For $x \in \mathbb{Q}$, we define the p-adic absolute value of x by $|x|_p = p^{-v_p(x)}$.*

Observation 2.10 *It is a non-archimedean absolute value.*

Proposition 2.11 *For $\mathbb{Q}$, let $|\cdot|_p$ be the p-adic absolute value, then*
1. *the associated valuation ring is $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$;*
2. *the valuation ideal is $p\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b, p \mid a\}$;*
3. *the residue field is $\mathbb{F}_p$, the finite field of p elements.*

Proof Idea All follows from the definition. ■

3 p-adic numbers

3.1 $\mathbb{Q}_p$ as completion of $\mathbb{Q}$

Lemma 3.1 *Suppose $|\cdot|$ is non-archimedean, A sequence $\{x_n\} \subset \mathbb{Q}$ is Cauchy if*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0$$

Proof Given $\epsilon > 0$, $\exists N$ s.t. $\forall n \geq N$, $|x_{n+1} - x_n| < \epsilon$. Then for all $m > n \geq N$,

$$|x_m - x_n| = |\sum_{i=n+1}^{m} x_i - x_{i-1}| \leq \max\{|x_{i+1} - x_i| : N \leq n < i \leq m\} < \epsilon$$

■

Lemma 3.2 *Fix odd prime p, and some integer $n \geq 1$. For any x s.t $p \nmid x$, $x^2 \equiv a \pmod{p^n}$ for some integer a. Then $\exists y$ s.t. $y \equiv x \pmod{p^n}$ and $y^2 \equiv a \pmod{p^{n+1}}$.*

Proof Since $p \nmid x$, there is z s.t. $2xz \equiv 1 \pmod{p}$, or equivalently $2xz = 1 + kp$ for some integer k. $x^2 = a + mp^n$ for some $m \in \mathbb{Z}$.

Let $y = x - zmp^n$, then $y \equiv x \pmod{p^n}$,

$$y^2 = x^2 - 2zxmp^n + z^2m^2p^{n+1}p^{n-1} \equiv a + mp^n - (1 + kp)mp^n \equiv a \pmod{p^{n+1}}$$

■

Proposition 3.3 *$\mathbb{Q}$ is not complete with respect to $|\cdot|_p$.*

Proof We will show incompleteness for odd p.

Choose integer $a \in \mathbb{Z}$ such that a is not a square in $\mathbb{Q}$, $p \nmid a$ and $x^2 \equiv a \pmod{p}$ has a solution. Let x_0 be any such solution.

For each $n > 0$, choose x_n so that $x_n \equiv x_{n-1} \pmod{p^n}$ and $x_n^2 \equiv a \pmod{p^{n+1}}$. One can always find such solutions by Lemma 3.2.

$|x_{n+1} - x_n| \leq p^{-n-1} \to 0$, so this is a Cauchy sequence. But $|x_n^2 - a| \leq p^{-n-1} \to 0$, so square root of a is the limit of the sequence, which is not in $\mathbb{Q}$.

For $p = 2$, one can use analogous methods to construct a sequence tending to $\sqrt[3]{3}$. ■

Fact 3.4 (Alexander Ostrowski, 1916) *Every non-trivial norm on $\mathbb{Q}$ is equivalent to either the usual absolute value or a p-adic absolute value.*

Remark Combined Fact 3.4 with Proposition 3.3, one can deduce that $\mathbb{Q}$ is incomplete with respect to any non-trivial norm. We will then construct $\mathbb{Q}_p$ by completing $\mathbb{Q}$.

3.2 Completing $\mathbb{Q}$

Let $\mathcal{C}$ be the set of all Cauchy sequences in $\mathbb{Q}$ with respect to norm $|\cdot|_p$. Define addition and multiplication to be term-wise, then $\mathcal{C}$ becomes a commutative ring with unity. $\mathbb{Q}$ injects into $\mathcal{C}$ as constant sequences.

Define $\mathcal{N} \subset \mathcal{C}$ to be the ideal of all sequences tending to 0. It turns out that $\mathcal{N}$ is a maximal ideal, so we can then define $\mathbb{Q}_p$ to be the quotient $\mathcal{C}/\mathcal{N}$, and use $\overline{(x_n)}$ to denote its class.

It is necessary to check that the absolute value extends from $\mathbb{Q}$ to $\mathbb{Q}_p$.

Lemma 3.5 *For a Cauchy sequence (x_n), if it does not tend to 0, then $\exists c > 0, N$ such that $\forall n \geq N$, $|x_n| \geq c > 0$.*

Proof Since (x_n) does not tend to 0, $\exists \delta > 0$ such that $\forall N, \exists n \geq N$ with $|x_n| \geq \delta$. Therefore one can choose another subsequence (x_{m_i}) such that $\forall i$, $|x_{m_i}| \geq \delta$.

Suppose $\forall N, c > 0$, $\exists n > N$ such that $|x_n| < c$, then one can choose a subsequence (x_{n_i}) such that $|x_{n_i}| < \frac{\delta}{2}$.

For i, j large enough, we have $|x_{m_i} - x_{n_j}| \geq |x_{m_i} - 0| - |x_{n_j} - 0| \geq \delta - \frac{\delta}{2} \geq \frac{\delta}{2}$, which leads to a contradiction. ■

Lemma 3.6 *For $(x_n) \in \mathcal{C} \setminus \mathcal{N}$, $\exists N$ such that $\forall n, m \geq N$, $|x_n| = |x_m|$*

Proof By Lemma 3.5, $\exists c, N_1 > 0$ s.t. $n \geq N_1$ implies $|x_n| \geq c > 0$.

Since the sequence is Cauchy, $\exists N_2$ s.t. $n > m \geq N_2$ implies $|x_n - x_m| < c$.

Let $N = \max\{N_1, N_2\}$, then for $n > m \geq N$, $|x_n - x_m| < c \leq |x_n|$, so $|x_n - x_m| < |x_n|$.

By Corollary 2.4, $|x_n| = |x_m|$. ■

Definition 3.7 *For $\lambda \in \mathbb{Q}_p$, let (x_n) be any Cauchy sequence representing λ, we define*

$$|\lambda|_p = \lim_{n \to \infty} |x_n|_p$$

Remark One can check that the absolute value is well-defined, is non-archimedean, and coincides with $|\cdot|_p$ on $\mathbb{Q}$. Furthermore, the image of $\mathbb{Q}_p$ under this norm is the same as the image of $\mathbb{Q}$, i.e. $\forall \lambda \in \mathbb{Q}_p$, $|\lambda|_p = p^n$ for some $n \in \mathbb{Z}$.

Proposition 3.8 *$\mathbb{Q}$ is dense in $\mathbb{Q}_p$.*

Proof Given $\lambda \in \mathbb{Q}_p$ and $\epsilon > 0$, we show that $\exists y \in \mathbb{Q}$ such that $|\overline{(y)} - \lambda| < \epsilon$.

Choose $0 < \epsilon' < \epsilon$, and choose any representation (x_n) of λ. $\exists N$ s.t. $|x_n - x_m| < \epsilon'$ if $n, m \geq N$. Let $y = x_N$, then

$$\lim_{n \to \infty} |x_n - y| \leq \epsilon' < \epsilon$$

So $|(y) - \lambda| < \epsilon$, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. ■

Remark It remains to check that $\mathbb{Q}_p$ is complete with respect to the extended norm. This will be left as a tedious exercise.

3.3 p-adic expansion

Theorem 3.9 *Let $\mathbb{Z}_p$ be the valuation ring of $\mathbb{Q}_p$.*

1. It is a local ring with maximal ideal $p\mathbb{Z}_p$, and is a PID.

2. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$

3. $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and in fact for all $x \in \mathbb{Z}_p$ and all $n \geq 1$, there is unique $\alpha \in \mathbb{Z}$ s.t. $0 \leq \alpha \leq p^n - 1$ and $|x - \alpha| \leq p^{-n}$

4. $\forall x \in \mathbb{Z}_p$, there is unique $(\alpha_n) \subset \mathbb{Z}$ s.t. $\alpha_n \to x$, $0 \leq \alpha_n \leq p^n - 1$ and $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$

Proof

1. By Proposition 2.6, $\mathbb{Z}_p$ is a ring with maximal ideal $p\mathbb{Z}_p$. Since all non-units are in this ideal, it must be the unique maximal ideal, so the ring is local. Any element in the ring is of the form up^n for some $u \in \mathbb{Z}_p^\times$. Let I be any ideal in the ring, let n be the minimal integer for which $up^n \in I$ for some unit u. Then $(p^n) \subset I$. Suppose by way of contradiction that $\exists up^k \in I \setminus (p^n)$, then $k < n$ which leads to a contradiction. Therefore $I = (p^n)$.

2. Follows from Proposition 2.11.

3. Given $x \in \mathbb{Z}_p$, $n \geq 1$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can find $\frac{a}{b} \in \mathbb{Q}$ s.t. $|x - \frac{a}{b}| \leq p^{-n} < 1$. $|\frac{a}{b}| \leq \max\{|x|, |x - \frac{a}{b}|\} \leq 1$, so $\frac{a}{b} \in \mathbb{Z}_{(p)}$. Therefore $p \nmid b$, $|b| = 1$ and we can find $b' \in \mathbb{Z}$ s.t. $bb' \equiv 1 \pmod{p^n}$.

   Now, since $a \equiv abb' \pmod{p^n}$, $p^n \mid a - abb'$, so $|a - abb'| \leq p^{-n}$.

$$|\frac{a}{b} - ab'| = \frac{|a - abb'|}{|b|} = |a - abb'| \leq p^{-n}$$

   Pick $\alpha \in \mathbb{Z}$, so that $0 \leq \alpha \leq p^n - 1$ and $\alpha \equiv ab' \pmod{p^n}$, then

$$|\alpha - ab'| \leq p^{-n}$$

   With $|x - \frac{a}{b}| \leq p^{-n}$, we have

$$|x - \alpha| \leq \max\{|x - \frac{a}{b}|, |\frac{a}{b} - ab'|, |ab' - \alpha|\} \leq p^{-n}$$

   Therefore such α exists.

   Suppose we have α' with the same properties, then

$$|\alpha - \alpha'| \leq \max\{|\alpha - x|, |x - \alpha'|\} \leq p^{-n}$$

   so $\alpha \equiv \alpha' \pmod{p^n}$.

4. Follows from part 3. Choosing $n = 1, 2, \ldots$, we have (α_n) such that $0 \leq \alpha_n \leq p^n - 1$ and $|x - \alpha_n| \leq p^{-n}$, so $\alpha_n \to x$.

$$|\alpha_n - \alpha_{n+1}| \leq \max\{|\alpha_n - x|, |x - \alpha_{n+1}|\} \leq \max\{p^{-n}, p^{-n-1}\} \leq p^{-n}$$

   Therefore $\alpha_{n+1} \equiv \alpha_n \pmod{p^n}$.

   Suppose we have (β_n) with the same properties. Note that for $m > n$, $\beta_m \equiv \beta_n \pmod{p^n}$. Choose any n, we can find $N > n$ s.t. $|\beta_N - x| \leq p^{-n}$.

$$|\alpha_n - \beta_N| \leq \max\{|\alpha_n - x|, |x - \beta_N|\} \leq p^{-n}$$

   So $\alpha_n \equiv \beta_N \equiv \beta_n \pmod{p^n}$. Since $0 \leq \alpha_n, \beta_n \leq p^n - 1$, $\alpha_n = \beta_n$. Therefore the sequence is unique.

■

Corollary 3.10 *For $x \in \mathbb{Z}_p$, $x = \sum_{n=0}^{\infty} b_n p^n$ where $0 \leq b_n \leq p - 1$ and such expression is unique.*

Proof From Thoerem 3.9, we have $\alpha_n \to x$ with $\alpha_n \equiv \alpha_{n+1} \pmod{p^n}$.

Therefore for each $n \geq 1$, $\alpha_{n+1} = \alpha_n + b_n p^n$ for some $0 \leq b_n \leq p - 1$. Let $b_0 = \alpha_1$, we have

$$\alpha_m = \sum_{n=0}^{m-1} b_n p^n$$

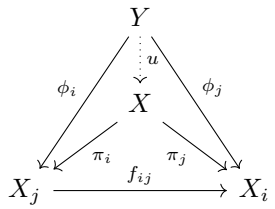

Figure 1: Inverse Limit

and

$$x = \lim_{m\to\infty} \alpha_m = \sum_{n=0}^{\infty} b_n p^n$$

Each b_n is uniquely determined.

Conversely, if $x = \sum_{n=0}^{\infty} b_n p^n$, one can recover the corresponding (α_n). Therefore (b_n) is unique by the uniqueness of (α_n). ■

Corollary 3.11 *Every $x \in \mathbb{Q}_p$ can be written in the form*

$$x = \sum_{n\geq -n_0} b_n p^n$$

with $0 \leq b_n \leq p-1$ and $-n_0 = v_p(x)$. This representation is unique.

Proof Given $x \in \mathbb{Q}_p$, $|x| = p^{n_0}$ for some $n_0 \in \mathbb{Z}$. So $|p^{n_0}x| = p^{-n_0}p^{n_0} = 1$, $p^{n_0}x = y \in \mathbb{Z}_p$.

By Corollary 3.10,

$$y = \sum_{n\geq 0} a_n p^n$$

with $0 \leq a_n \leq p-1$. Let $b_n = a_{n+n_0}$, we have

$$x = p^{-n_0}y = \sum_{n\geq -n_0} b_n p^n$$

The expression is unique because the expansion for y is unique. $v_p(x) = -\log|x| = -n_0$ ■

Remark This also implies that $\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$, i.e. the ring of p-adic integers is the inverse (or projective) limit, where the homomorphic maps are just modulo p^n. In the language of Category Theory, the inverse limit can be defined with a universal property of a inverse system, with the diagram in Fig 1.

Corollary 3.12 *For any $n \geq 1$, the sequence*

$$0 \to \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z} \to 0$$

where the map $\psi : \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p$ is given by $x \mapsto p^n x$, is exact. In particular,

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

Proof The proof goes in 5 steps.

1. Define the map $\phi : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ as follows:

   By Theorem 3.9, for each $x \in \mathbb{Z}_p$, there is unique integer $0 \leq \alpha \leq p^n - 1$ such that $|\alpha - x| \leq p^{-n}$. Set $\phi(x) = \overline{\alpha}$, where $\overline{\alpha}$ is the equivalent class of α in $\mathbb{Z}/p^n\mathbb{Z}$.

2. Show ϕ is a ring homomorphism. Take $x, y \in \mathbb{Z}_p$ and let $\overline{a} = \phi(x)$, $\overline{b} = \phi(y)$.

   $$|(x + y) - (a + b)| \leq \max\{|x - a|, |y - b|\} \leq p^{-n}$$

   so $\phi(x + y) = \overline{a + b} = \phi(x) + \phi(y)$.

   $$|xy - ab| = |xy - ay + ay - ab| \leq \max\{|x - a||y|, |a||y - b|\} \leq p^{-n}$$

   since $y, a \in \mathbb{Z}_p \Rightarrow |a|, |y| \leq 1$. Therefore $\phi(xy) = \phi(x)\phi(y)$

3. It is clear that ψ, multiplication by p^n, is injective. Take any $\overline{a} \in \mathbb{Z}/p^n\mathbb{Z}$, $a \in \mathbb{Z} \subset \mathbb{Z}_p$, and $\phi(a) = \overline{a}$, so ϕ is surjective.

4. If $\phi(x) = \overline{0}$, then $|x| = |x - 0| \leq p^{-n}$. Therefore $|\frac{x}{p^n}| \leq p^{-n}p^n = 1$, $\frac{x}{p^n} \in \mathbb{Z}_p$, so $x \in p^n\mathbb{Z}_p$. $Im(\psi) = Ker(\phi)$

5. By the Isomorphism Theorem,

   $$Im(\phi) \cong \mathbb{Z}_p/Ker(\phi) \Leftrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

■

Observation 3.13 *When $n = 1$, the residue field of $\mathbb{Q}_p$ is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$*

4 Lattices and their equivalent classes in $\mathbb{Q}_p$

4.1 Basics

Definition 4.1 *A lattice in $\mathbb{Q}_p^2$ is any finitely generated $\mathbb{Z}_p$-submodule that spans $\mathbb{Q}_p^2$ as a vector space.*
Remark An example would be $\mathbb{Z}_p^2$, generated by the canonical basis vectors.

Proposition 4.2 *Every lattice in $\mathbb{Q}_p^2$ is free over $\mathbb{Z}_p$ of rank 2.*
Proof Let the lattice be L with t generators, and let M_L be the 2-by-t matrix whose columns are the generators. For M_L, there are three types of integral column (row) operations:

(a) permutation of columns (rows)

(b) multiplying one column (row) by an element in $\mathbb{Z}_p^\times$

(c) adding to any column (row) an $\mathbb{Z}_p$ multiple of another

These column (row) operations correspond to multiplying on the right (left) by a matrix in $GL_t(\mathbb{Z}_p)$ ($GL_2(\mathbb{Z}_p)$). The column operations in particular do not change the lattice L.

Since the lattice need to span $\mathbb{Q}_p^2$, there is at least one non-zero element in the first row, take the one with maximum norm, we can move it to the top left corner by (a) and use column operations of type (b) to get it in the form p^n and use (c) to reduce the rest of the row to 0, since n is the smallest among the row.

Similarly, we can transform the second row (for columns 2 to t) and reduce M_L to

$$\begin{bmatrix} p^n & 0 \\ up^k & p^m \end{bmatrix}$$

One can see that the two generators are now linearly independent. ■

Proposition 4.3 *Given g in $GL_2(\mathbb{Q}_p)$, there are $k_1, k_2 \in GL_2(\mathbb{Z}_p)$ and unique diagonal d in the form*

$$\begin{bmatrix} p^m & 0 \\ 0 & p^n \end{bmatrix}$$

with $m \leq n$ such that

$$g = k_1 d k_2$$

Proof Idea This is just Gaussian elimination, using both column and row operations defined earlier. ■

Corollary 4.4 (Invariant Factor Theorem) *If L and M are two lattices, there is a basis (e, f) of L and integers $m \leq n$ such that $(p^m e, p^n f)$ is a basis of M.*
Sketch of Proof By change of basis of $\mathbb{Q}_p^2$ one can assume $L = \mathbb{Z}_p^2$. Let g be the matrix in $GL_2(\mathbb{Q}_p)$ with column vectors as generators of M. Then apply Prop 4.3, the column of k_1 form a basis of $L = \mathbb{Z}_p^2$ and those of $gk_2^{-1} = k_1 d$ form one of M. ■

Remark The tuple (p^m, p^n) is well-defined for each pair of lattices L and M.
Remark The group $GL_2(\mathbb{Q}_p)$ clearly acts transitively on the set of lattices, since it acts transitively on their bases. The stabilizer for $\mathbb{Z}_p^2$ is, unsurprisingly, $GL_2(\mathbb{Z}_p)$, so the set of lattices of rank 2 on $\mathbb{Q}_p^2$ is isomorphic (as $GL_2(\mathbb{Q}_p)$-sets) to the set of left cosets $GL_2(\mathbb{Q}_p)/GL_2(\mathbb{Z}_p)$.

4.2 Similarity Classes of Lattices

We want to consider lattices that differ by a constant factor as being equivalent. We know that every element in $\mathbb{Q}_p$ can be written as up^n for some unit $u \in \mathbb{Z}_p^\times$ and $n \in \mathbb{Z}$. If $n = 0$, then multiplying by just a constant unit in $\mathbb{Z}_p$ actually does not change the lattice. However, multiplying by p is like scaling the lattice, so we also call these equivalent lattices "similar".

There is an analogy between reals and the p-adic numbers that kind of motivates consideration of such similarity classes of lattices. In real functional analysis, given the unit open ball K in a normed vector space V. One can define the Minkowski functional p on V by

$$p(x) = \inf\{r > 0 : x \in rK\}$$

which is the same function as the norm on V with K being the unit ball.

Similarly, choosing a lattice L in $\mathbb{Q}_p^n$ defines a norm

$$\|v\|_L = \inf\{|c| : v \in cL\}$$

So similarity classes of lattices in $\mathbb{Q}_p^n$ are like unit balls in $\mathbb{R}^n$

Note that now the action of group $GL_2(\mathbb{Q}_p)$ on the set of similarity classes of L now factors through all the scalar matrices, i.e. the center of the group. We can now consider the transitive action of the projective linear group $PGL_2(\mathbb{Q}_p) = GL_2(\mathbb{Q}_p)/\{\lambda I : \lambda \in \mathbb{Q}_p\}$ on the similarity classes. $PGL_2(\mathbb{Z}_p)$ still stabilizes the class of $\mathbb{Z}_p^2$, we thus have that the set of similarity classes of lattices is isomorphic to $PGL_2(\mathbb{Q}_p)/PGL_2(\mathbb{Z}_p)$.

4.3 Graph of Similarity Classes

I will now consider the graph consisting of the similarity classes of lattices. We can write the similarity class of L as $[L]$, which is the set $\{p^n L\}$. I will call them "nodes". Note that by the invariant factor theorem, we have a tuple (p^m, p^n) defined for a pair of lattices L and M. The difference $n - m$ is an

invariant of the similarity class of L and M. One can define a symmetric invariant on the equivalence classes $inv([L],[M]) = n - m$. This invariant is 1 if and only if the two nodes have representatives L and M with

$$pL \subset M \subset L$$

It is symmetric because if above holds, then

$$pM \subset pL \subset M$$

and M and pL are representatives of $[M]$ and $[L]$, respectively. In this case, I will connect $[L]$ and $[M]$ with an undirected edge and call them neighbors.

For example, the class of $\mathbb{Z}_p^2$ and the class of $\mathbb{Z}_p \times p\mathbb{Z}_p$ are neighbors.

Proposition 4.5 *Every node in the graph has degree $p+1$.*
Sketch of Proof Note that the action of $GL_2(\mathbb{Q}_p)$ preserves the edges of nodes. Since the action is transitive, we know that the degree is the same for each node.

If $[L]$ and $[M]$ are connected, we can find L and M such that

$$pL \subset M \subset L$$

so $M/pL \subset L/pL$. If L is generated by u, v, then

$$L/pL \cong (\mathbb{Z}_p u \times \mathbb{Z}_p v)/(p\mathbb{Z}_p u \times p\mathbb{Z}_p v) \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^2 = \mathbb{F}_p^2$$

M thus corresponds to subspaces (lines) of $\mathbb{F}_p^2$. Connecting $(0,0)$ with $(0,1)$ or $(1,x)$ for $x = 0, 1, \ldots, p-1$ gives the $p+1$ distinct lines. ■

4.4 Chains

Definition 4.6 *A chain is a finite or half-infinite sequence of nodes linked by edges. Every chain may be represented by a sequence of lattices*

$$L_0 \supset L_1 \supset \ldots$$

with

$$L_n \supset L_{n+1} \supset pL_n$$

for all n. The standard chain is represented by

$$\mathbb{Z}_p \times \mathbb{Z}_p \supset p\mathbb{Z}_p \times \mathbb{Z}_p \supset p^2\mathbb{Z}_p \times \mathbb{Z}_p \supset \ldots$$

whether finite or infinite. Call the nodes in the standard chain $T_0, T_1, \ldots$.

A chain is simple if, like the standard one, it does not backtrack.

Proposition 4.7 *Every finite simple chain in the graph may be transformed to a standard one by an element of $GL_2(\mathbb{Q}_p)$. It is still true for infinite chains.*
Proof Proceed by induction on the length of the chain $L_0 \supset \ldots \supset L_n$.

WLOG, we can always find $g \in GL_2(\mathbb{Q}_p)$ transforming L_0 to $\mathbb{Z}_p^2$, so we may assume $L_0 = T_0$.

If $n = 1$, the image of L_1 in L_0/pL_0 is a line. We can find matrix $\overline{g} \in GL_2(\mathbb{F}_p)$ transforming it to the line through $(0,1)$, which has pre-image T_1. So lift $\overline{g}$ to $g \in GL_2(\mathbb{Z}_p)$, we have $gL_1 = T_1$. Note that g preserves $L_0 = T_0$.

Now suppose we have a chain (L_i), $0 \le i \le n+1$ with $L_i = T_i$ for $i \le n$. Let $M = L_{n+1} \subset L = L_n$. We know

$$pL \subset pL_{n-1} \subset L$$

and

$$pL \subset M \subset L$$

Since the chain is simple, $pL_{n-1} \neq M$. We can consider their images in L/pL. pL_{n-1} corresponds to the line through $(1,0)$, hence M corresponds to the line through $(y,1)$ for some $y \in \mathbb{F}_p$. The matrix $\overline{g} \in GL_2(\mathbb{F}_p)$

$$\begin{bmatrix} 1 & -y \\ 0 & 1 \end{bmatrix}$$

takes the line through $(y,1)$ to $(0,1)$. Lifting $\overline{g}$ to $GL_2(\mathbb{Z}_p)$, we have

$$g = \begin{bmatrix} 1 & p^n(p-y) \\ 0 & 1 \end{bmatrix}$$

so that $gM = T_{n+1}$.

Notice that g preserves the classes of T_0 thorough T_n.

By induction, call the matrix we select at each step $g_n \in GL_2(\mathbb{Z}_p)$, and its upper right entry $p^n x_n \in p^n\mathbb{Z}$. Then the matrix we finally select is

$$g = \prod_{i=1}^{\infty} g_i = \begin{bmatrix} 1 & \sum p^i x_i \\ 0 & 1 \end{bmatrix}$$

which converges in $GL_2(\mathbb{Q}_p)$ since $\mathbb{Q}_p$ is complete. ■

Corollary 4.8 *The graph of similarity classes is an infinite, connected tree.*
Sketch of Proof Let M be any lattice, we can find basis (e,f) of T_0 such that some $(p^m e, p^n f)$ is a basis of M. Replace M by a multiple of itself, we can assume $n \geq m = 0$. Then we can have a standard chain of lattices $(e, p^k f)$ from T_0 to M. Therefore the graph is connected. Since all chains can be sent to the standard chain which does not backtrack, there is no loop in the graph, hence it is a tree. ■

Remark This tree is called the Bruhat-Tits tree.

Acknowledgement

I would like to thank Professor Igor Frenkel for introducing me to the topic of Bruhat-Tits tree and helping me identify the relevant references. I would also like to thank all the other students in the seminar, i.e. Teddy Weisman, Mark Hamilton, Tommy Tang, Vicky Tu, Alex Reinking, Albert Jiao and Joshua Ryu, for pointing out the mistakes in my original notes and providing helpful suggestions.

5 References

Section 1 through 3 are from the book *P-adic Numbers: An Introduction* by Fernando Gouvea, available for free online via Springer here. Section 4 is based on Bill Casselman's *Notes on the Bruhat-Tits Tree*, PDF available on his personal site here.