p-adic Numbers 강의록

Donghyun Park

January 8, 2026

1 3강. Structure of p-adic numbers

지난 시간에 이어서...
$\mathbb{Q} \hookrightarrow \mathbb{Q}_p$가 dense한 것을 보이는 과정에서 subtle한 포인트가 있었습니다. $\mathbb{Q}_p$에 metric을 주지 않았었으니, open set (topology)를 정의할 수 없었던...

Lemma 1 ([Gou20] Lemma 3.2.10). *Let $(x_n) \in \mathcal{C}_p(\mathbb{Q}) - \mathcal{N}$. The sequence of real numbers $|x_n|_p$ is eventually stationary, that is, there exists an integer N that $|x_n|_p = |x_m|_p$ for $m, n \geq N$*

Proof. x_n do not tend to zero (in other words, $\lim_{n\to\infty} |x_n|_p = 0$이 아니다) There exists c such that $|x_n| \geq c > 0$ for $n \geq N_1$.
Also x_n is Cauchy sequence so there exists an integer N_2, $n, m \geq N_2$ then $|x_n - x_m| < c$
Recall: 모든 삼각형은 이등변삼각형이며 같은 두 변의 길이가 다른 변의 길이보다 길다.
$|x_m| = |x_n$ for $n, m \geq \max(N_1, N_2)$. □

즉 이를 바탕으로 p-adic absolute value on $\mathbb{Q}_p$를 정의할 수 있습니다.

Definition. $\lambda \in \mathbb{Q}_p$ and (x_n) is any Cauchy sequence representing λ, we define

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

(Well defined?)
(x_n)과 (y_n)이 λ를 represent하면 ($\lambda \neq 0$ $(x_n - y_n) \in \mathcal{N}$. $|x_n - y_n| \to 0$. 이제 lemma에 의해 $|x_n|$와 $|y_n|$가 eventually stationary 하고, 모든 삼각형은 이등변삼각형에 같은 변의 길이가 길게 되므로

$$\lim_{n\to\infty} |x_n| = \lim_{n\to\infty} |y_n|$$

반대로 0, 즉 $\mathcal{N}$의 원소들은 정의상 $\lim_{n\to\infty} |x_n| = 0$이었으므로... well defined!

Problem 1.1 ([Gou20] Problem 94). *This $|\cdot| : \mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\}$ is* ***non-archimedean absolute value***

2개를 보여야합니다... absolute value axiom을 만족하는지? non-archimedean인지?

Problem 1.2 ([Gou20] Problem 95). *We have defined $\tilde{x} = (x, x, \cdots)$ for $x \in \mathbb{Q}$ so the injective ring homomorphism $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$.*
Show that $|\tilde{x}|_p = |x|_p$

즉, dense함을 보이는 증명에서 metric은 field $\mathbb{Q}_p$에 주어진 absolute value로 induce된 metric.
$\lambda, \mu \in \mathbb{Q}_p$고 $(x_n), (y_n)$이 이 둘을 represent하는 cauchy sequence in $\mathbb{Q}$이면

$$d(\lambda, \mu) = |\lambda - \mu|_p = \lim_{n\to\infty} |x_n - y_n|_p$$

이제 마무리를 해봅시다.

Theorem 1. *$\mathbb{Q}_p$ is complete w.r.t. $|\cdot|_p$*

Proof. $\lambda_1, \lambda_2, \cdots$ be a Cauchy sequence of $\mathbb{Q}_p$.
$(x_k^{(i)})$ the Cauchy sequence representing λ_i
There exists $y_i \in \mathbb{Q}$ that

$$|\lambda_i - \tilde{y}_i|_p < \frac{1}{i}$$

By the denseness of rational numbers in $\mathbb{Q}_p$.
The sequence $(\tilde{y_n})$ is Cauchy. (Why?)
So the sequence (y_n) is Cauchy.
$(|\tilde{y}_n - \tilde{y}_m|_p \leq |\tilde{y}_n - \lambda_n|_p + |\tilde{y}_m - \lambda_m|_p + |\lambda_n - \lambda_m|_p)$
$\lambda = (y_n)$. Then for $\epsilon > 0$, since Cauchy, $|y_n - y_m| < \epsilon/2$ for $n, m \geq N$ so

$$|\lambda - \tilde{y}_n|_p = \lim_{m\to\infty} |y_m - y_n|_p \leq \frac{1}{2}\epsilon < \epsilon$$

$(\tilde{y}_n)$ converges to λ...
Combining λ_n and $\tilde{y}_n$... λ_n converges to λ. □

Theorem 2. *For each prime p, there exists a field $\mathbb{Q}_p$ with a non-archimedean absolute value $|\cdot|_p$ such that*
(a) $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ inclusion and the absolute value extending $\mathbb{Q}$ (p-adic)
(b) The image of $\mathbb{Q}$ under this inclusion is dense in $\mathbb{Q}_p$
(c) $\mathbb{Q}_p$ is complete w.r.t. $|\cdot|_p$
The field $\mathbb{Q}_p$ satisfying (a),(b),(c) is ***unique up to unique isomorphism*** *preserving absolute values.*

Proof. K a another field, $\mathbb{Q} \hookrightarrow K$. Preserving the absolute value of $\mathbb{Q}$.
$x_n \in \mathbb{Q}$ and look at the Cauchy sequence (x_n) in both $\mathbb{Q}_p$ and K ($\mathbb{Q}$ 에서의 absolute value, 즉 metric은 똑같기 때문에). Both are Cauchy sequence ($\mathbb{Q}$ absolute value is extended) so converges.
$\lambda \in \mathbb{Q}_p$, there is a Cauchy sequence (x_n) with $x_n \in \mathbb{Q}$ whose limit is λ. (Since $\mathbb{Q}$ is dense). Their image in K is also Cauchy, there exists a limit : $f(\lambda)$ (Since K is complete).
$f : \mathbb{Q}_p \to K$ which is identity on $\mathbb{Q}$.

(1) (Well defined?)
(2) $f(\lambda_1 + \lambda_2) = f(\lambda_1) + f(\lambda_2)$
(3) $f(\lambda_1\lambda_2) = f(\lambda_1)f(\lambda_2)$

(2), (3)의 경우 $\mathbb{Q} \times \mathbb{Q}$가 $K \times K, \mathbb{Q}_p \times \mathbb{Q}_p$에서 dense하고, $K \times K \underset{+}{\overset{\cdot}{\to}} K, \mathbb{Q}_p \times \mathbb{Q}_p \underset{+}{\overset{\cdot}{\to}} \mathbb{Q}_p$가 continuous하기 때문이라고 하면 되겠습니다.
f is field homomorphism. And in the same way, map $g : K \to \mathbb{Q}_p$ is defined, is an inverses. Thus f is an isomorphism.
(4) f is continuous, g is continuous
(5) absolute value is continuous function $\mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\}$, $K \to \mathbb{R}^+ \cup \{0\}$
Finally, f preserves absolute value. □

Unique up to unique isomorphism. Only one way to define isomorphism.

Remark 1. *Unique up to unique isomorphism이 아닌 것? 대표적으로는 vector space (dimension 같으면 isomorphism 인데, 그 isomorphism 이 unique하지 않죠. Field extension 또한 그렇습니다.*

We have defined p-adic number by completing rational numbers with p-adic absolute value.

Lemma 2 ([Gou20] Lemma 4.1.2)**.** *For each $x \in \mathbb{Q}_p$ there exists an integer $v_p(x)$ such that $|x|_p = p^{-v_p(x)}$. p-adic valuation extends to $\mathbb{Q}_p$*

1.1 p-adic integers

Definition. Valuation ring of p-adic numbers is called p-adic integers

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

Proposition 1 ([Gou20] Proposition 4.2.2)**.** *The ring $\mathbb{Z}_p$ of p-adic integers is a local ring whose maximal ideal is the principal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Furthermore,*
(a) $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$
(b) The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has a dense image. For $n \geq 1$, there exists a unique $\alpha \in \mathbb{Z}$, $0 \leq \alpha \leq p^n - 1$ such that $|x - \alpha|_p \leq p^{-n}$.
(c) For any $x \in \mathbb{Z}_p$, there exists a Cauchy sequence (α_n) converging with
- $\alpha_n \in \mathbb{Z}$ satisfies $0 \leq \alpha_n \leq p^n - 1$
- For every $n \geq 2$ we have $\alpha_n \equiv \alpha_{n-1} (mod\ p^{n-1})$

Proof. Local ring: In 2강...
(a) 는 자명하다.
(b) $\mathbb{Q}$ 가 dense 하므로, $a/b \in \mathbb{Q}$, $|x - \frac{a}{b}| \leq p^{-n}$ 가 존재한다. $|\frac{a}{b}|_p \leq \max(|x|_p, |x - \frac{a}{b}|_p) \leq 1$ 이므로 $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$ 안에 존재한다. $p \nmid b$. 즉 $bb' \equiv 1 (mod\ p^n)$인 $b' \in \mathbb{Z}$가 존재.

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

이므로 $ab' \in \mathbb{Z}$. 이제 Congruence로 p^n 보다 작은 범위로 내리면 성립.
(c) (b)를 만족하는 정수가 단 한개 뿐이므로, α_n sequence는 coherent. □

Corollary 1 ([Gou20] Corollary 4.2.3)**.** *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$*

Corollary 2 ([Gou20] Corollary 4.2.4)**.** *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$. For every $x \in \mathbb{Q}_p$, there exists $n \geq 0$ such that $p^n x \in \mathbb{Z}_p$. $\mathbb{Q}_p \to \mathbb{Q}_p$ given by $x \mapsto px$ is a homeomorphism. $p^n\mathbb{Z}_p$ forms a fundamental system of neighborhood of $0 \in \mathbb{Q}_p$ which covers all of $\mathbb{Q}_p$*

Proof. $x \in \mathbb{Q}_p$에서 $v_p(x)$ 가 Well-defined 되고, $v_p(x)$가 negative이면 $p^{-v_p(x)}x \in \mathbb{Z}_p$.
Recall: Non-archimedean absolute value giving distance function,
$B(a, r)$ and $\bar{B}(a, r)$ for $r \neq 0$ is both open and closed set. $\mathbb{Z}_p$ is thus open subset.
Fundamental system of neighborhood means other neighborhood contains one of them. □

The sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is exact if $im(f) = ker(g)$

Corollary 3 ([Gou20] Corollary 4.2.5)**.** *For any $n \geq 1$, the sequence*

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

is exact. Each map is continuous when $\mathbb{Z}/p^n\mathbb{Z}$ is the discrete topology (every point set is open, or in point of distance function, every two points are in distance ∞)

Proof. $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p$. Injectivity is well-checked.
$\mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$: kernel contains image is obvious. $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ becomes zero if $x \in \bar{B}(0, p^{-n})$, so the kernel is exactly the same with image.
Surjectivity: $0, \cdots, p^n - 1 \in \mathbb{Z}_p$ gives image
Continuity checking! □

The sets $a + p^n\mathbb{Z}_p$ with $a \in \mathbb{Q}$ and $n \in \mathbb{Z}$ are closed balls in $\mathbb{Q}_p$ and is open. They cover all $\mathbb{Q}_p$ because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

Corollary 4 ([Gou20] Corollary 4.2.6)**.** *$\mathbb{Q}_p$ is a totally disconnected Hausdorff topological space.*

Ultrametric 공간에 의해 totally disconnected. Hausdorff는 두 점 x, y distinct가 있을 때 U, V open set이 있어 $x \in U, y \in V$ $U \cap V = \phi$인 것이 있는 것.

1.2 Compactness

Definition of compact, locally compact
Compact: Every open cover of an set has a finite open cover.
Locally compact: Every point has a neighborhood which contains a compact set.
Example. $\mathbb{R}$ is locally compact.

Corollary 5 ([Gou20] Corollary 4.2.7)**.** *$\mathbb{Z}_p$ is compact, and $\mathbb{Q}_p$ is locally compact*

Proof. $\mathbb{Z}_p$ is complete (as a closed set of a complete field). Also is totally bounded; every $\epsilon > 0$, we can cover $\mathbb{Z}_p$ with finitely many balls of radius ϵ.
$\epsilon = p^{-n}$ then

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

so the p^n balls

$$a + p^n\mathbb{Z}_p = \bar{B}(a, p^{-n})$$

covers $\mathbb{Z}_p$. □

Theorem 3 (Generalized Heine-Borel Theorem)**.** (X, d_X) *a metric space. Then X is compact if and only if X is complete (every Cauchy sequence in X converges to a point in X) and totally bounded (for every $\epsilon > 0$, there exists a finite covering of X by balls of radius ϵ*

Proof. We prove (complete, totally bounded) then (compact)
Open cover $\{U_i\}$ that does not have finite subcover then,
For $\cup_{n=1}^{n_1} B(x_{1n}, 1)$ covering X, at least one ball must not be covered by finite $\{U_i\}$.
Choose $B(x_{11}, 1)$. Cover this ball with 1/2 balls. $B(x_{11}, 1) = \cup_{n=1}^{n_2} B(x_{2n}, \frac{1}{2})$ at least one ball must not be covered by finite $\{U_i\}$.
These sequence $x_{11}, x_{21}, \cdots$ is cauchy sequence so converges to the point $x \in X$. This is covered by U_i. There exists $\epsilon > 0$ such that $B(x, \epsilon) \subset U_i$.
Thus, there exists x_{n1} such that $B(x_{n1}, \frac{1}{2^{n-1}}) \subset U_i$ contradiction. □

1.3 Return to our motivation

How does this description relates to our motivation?
$x \in \mathbb{Z}_p$, we have the coherent sequence converging to x.
- $\alpha_n \in \mathbb{Z}$, $0 \leq \alpha_n \leq p^n - 1$
- $\alpha_{n+1} \equiv \alpha_n (mod\ p^n)$

we checked this sequence is unique.
Conversely, every limit of a Cauchy sequence of integers must be an element of $\mathbb{Z}_p$.

Problem 1.3. *Show that every limit of a Cauchy sequence of integers must be an element of $\mathbb{Z}_p$.*

So we will **Identify $\mathbb{Z}_p$ with the sequences**
Basic setup: $\varphi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} = A_n$
Obvious map $\psi_n : A_n \to A_{n-1}$ sending a mod p^n to a mod p^{n-1}.

Proposition 2 ([Gou20] Proposition 4.3.1)**.** *The projection maps φ_n give an inclusion*

$$\varphi : \mathbb{Z}_p \hookrightarrow \prod_{n\geq 1} A_n$$

which identifies $\mathbb{Z}_p$ as a closed subring of $\prod A_n$ consisting of the coherent sequences.

Now, we can write α_n with base p.

$$\alpha_1 = b_0$$
$$\alpha_2 = b_0 + b_1 p$$
$$\alpha_3 = b_0 + b_1 p + b_2 p^2$$
$$\alpha_4 = b_0 + b_1 p + b_2 p^2 + b_3 p^3$$

Lemma 3 ([Gou20] Lemma 4.3.2)**.** *Given any $x \in \mathbb{Z}_p$, the series*

$$b_0 + b_1 p + b_2 p^2 + \cdots$$

converges to x

Proof. Partial sum is α_n. Now $|x - \alpha_n|_p \leq p^{-n}$. thus it converges to x. □

Corollary 6 ([Gou20] Corollary 4.3.3)**.** *Every $x \in \mathbb{Z}_p$ can be written in the form*

$$x = b_0 + b_1 p + \cdots$$

and this representation is unique.

Corollary 7 ([Gou20] Corollary 4.3.4)**.** *Every $x \in \mathbb{Q}_p$ can be written in the form*

$$x = b_{-m}p^{-m} + \cdots + b_{-1}p^{-1} + b_0 + b_1 p + \cdots$$

and $-m = v_p(x)$. This representation is unique.

1.4 Visuallizing p-adic numbers

Imagine $\mathbb{Q}$ with $\mathbb{R}$. We can image a straight line. Totally disconnected however not discrete. Compact set whose points are not discretely spaced out but also not connected to each other?
Actually $\mathbb{R}$ visualization preserves distance. However, expressing distance is difficult... we just try to represent $\mathbb{Z}_p$ preserving 'open sets' . (Convergent sequences in $\mathbb{Z}_p$ is convergent in pictures)

Theorem 4 ([Gou20] Theorem 4.4.1)**.** *$\mathbb{Z}_2$ is homeomorphic to the Cantor set C.*

Proof. Homeomorphic : f continuous such that f is bijective and f^{-1} is continuous.
Any cantor number can be represnted as

$$y = \frac{a_1}{3} + \frac{a_2}{3^2} + \cdots$$

where $a_i \in \{0, 2\}$. Every $z \in \mathbb{Z}_2$ has expansion

$$y = b_0 + b_1 2 + b_2 2^2 + \cdots$$

$b_i \in \{0, 1\}$. So define function $f : \mathbb{Z}_2 \to C$

$$f(b_0 + b_1 2 + \cdots + b_n 2^n + \cdots) = \frac{2b_0}{3} + \frac{2b_1}{3^2} + \cdots + \frac{2b_n}{3^{n+1}} + \cdots$$

Is a bijection, continuous with continuous inverse. □

(Nontrivial) 거기에 정말 비자명하게도, $\mathbb{Z}_p$ 또한 homeomorphic to Cantor set.
Fractal set을 떠올리면..
https://www.nt.th-koeln.de/fachgebiete/mathe/knospe/p-adic/