p-adic Numbers 강의록

Donghyun Park

January 21, 2026

1 2강. Construction of p-adic Numbers

지난번 review. $\Bbbk = \mathbb{Q}$ and p-adic valuation.

$$\bar{B}(0,1) = B(0,1) \cup B(1,1) \cup \cdots \cup B(p-1,1)$$

disjoint union.

Proof. Union: $|x|_p \leq 1$ then $x = \frac{a}{b}$ where $p \nmid b$. modulo p, b has inverse b'. Let $ab' \equiv c(mod\ p)$. Then our claim is $x \in B(c,1)$.

$$|x-c| = |\frac{a}{b} - c| = |\frac{a-bc}{b}| = |\frac{ab' - bb'c}{bb'}| < 1$$

Disjoint : $|i-j| = 1$ □

Other non-archimedean absolute values?
$f(t) \in F[t]$ which is polynomial with coefficients in the field F. Obvious valuation : $v_\infty(f) = -\deg(f(t))$
$F(t)$ a rational functions.. $v_\infty(\frac{f(t)}{g(t)}) = v_\infty(f(t)) - v_\infty(g(t))$
Non-archimedean absolute value $|f(t)| = e^{\deg(f)}$

Problem 1.1. *Check*
$v_\infty(f(t)g(t)) = v_\infty(f(t)) + v_\infty(g(t))$
$v_\infty(f(t)+g(t)) \geq \min(v_\infty(f(t)), v_\infty(g(t)))$

$p(t)$ irreducible polynomial. $p(t)$-adic valuation $v_{p(t)}(f) = e$ where $f(t) = p(t)^e g(t)$. Extend to $F(t)$

Problem 1.2. *Check this defines non-archimedean absolute values. Why is the 'irreducible' condition important?*

1.1 Algebra

거리를 살펴보았다. 거리 말고, 수 자체를 한번 생각해볼까요?

Definition. Commutative Ring (가환)
- $a+b = b+a$
- $a+(b+c) = (a+b)+c$
- $0 \in R$, $0 + a = a$
- $a \in R$, there exists $a' \in R$, $a + a' = 0$
- $ab = ba$
- $a(bc) = (ab)c$
- $1 \in R$, $1a = a$
- $a(b+c) = ab + ac$

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 하나는 체가 아니었습니다...

Unit: inverse가 존재하는 녀석들.
Example. $\mathbb{Z}$ unit? $\mathbb{Q}$? Field?

Definition. Ideal
$I \subset R$ such that
- $0 \in I$
- $a, b \in I$, $a+b \in I$
- $a \in I, r \in R$, $ra \in I$

Example. $\mathbb{Z}$, $n\mathbb{Z}$ is an ideal.
Example. ideal containing 1? ideal containing unit?

Definition. Quotient Ring
Congruence $a \equiv b(modI)$ if and only if $a - b \in I$
Congruence class R/I: $[a] = \{b \in R : b \equiv a\ modI\}$ then addition and multiplication.

$$[a] + [b] = [a+b]$$

$$[a][b] = [ab]$$

Problem 1.3. *Well definedness?*

Remark 1. *$R = \mathbb{Z}$, $I = n\mathbb{Z}$ then what is the congruence class?*

Group의 관점으로 보면 $[a] = a + I$ 가 성립한다. Addition 만을 단일 operation으로 본다면 이는 coset...

Theorem 1. *R/I is a commutative ring.*

Remark 2. *When does $R = \mathbb{Z}$, $I = n\mathbb{Z}$ the R/I become field?*

For $\Bbbk$ a field and non-archimedean absolute value,

$$\mathcal{O} = \{x \in \Bbbk : |x| \leq 1\}$$

closed under addition, multiplication.
is a "local ring" and called **Valuation Ring**. 다음으로

$$\mathfrak{B} = \{x \in \Bbbk : |x| < 1\}$$

are called **Valuation ideal**
The quotient $\kappa = \mathcal{O}/\mathcal{B}$ is a **Residue field** of $|\cdot|$.

Problem 1.4. *Is each of them local ring and ideal and field?*

Proof. Closed under the operation by non-archimedean absolute value properties. $\mathcal{O}$ is ring.
$\mathfrak{B}$ being ideal is trivial.
For every $x \in \mathcal{O} - \mathfrak{B}$, $x \neq 0$ so there exists $1/x$ which also lie in $\mathcal{O}$. Thus, every element in $\mathcal{O} - \mathfrak{B}$ is invertible in $\mathcal{O}$. That means, every proper ideal is contained in $\mathfrak{B}$. $\mathcal{O}$ is a local ring with maximal ideal $\mathfrak{B}$.
Immediate conclusion... residue κ is a field □

Proposition 1. *$\Bbbk = \mathbb{Q}$ with p-adic absolute value,*

$$\mathcal{O} = \{a/b \in \mathbb{Q} : p \nmid b\} = \mathbb{Z}_{(p)}$$

and its valuation ideal is $p\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b, p \mid a\}$ with residue field $\mathbb{F}_p$

Proof. Residue field?

$$\{[0], [1], \cdots, [p-1]\}$$

Combinig Problem 1.2 with

$$\bar{B}(0,1) = B(0,1) \cup B(1,1) \cup \cdots \cup B(p-1,1)$$

□

1.2 p-adic Numbers

그동안 무얼 했나. p-adic valuation on $\mathbb{Q}$으로부터 p-adic absolute value.
- $|\cdot|$: 평범한 usual absolute value
- $|\cdot|_p$

양쪽 모두 유리수에서 정의한 것.

1.2.1 Ostrowski theorem

유리수의 absolute value에는 어떤 것들이 있을까? 더 있을까?
"Equivalence of absolute value"
Definition. Two absolute value $|\cdot|_1$ and $|\cdot|_2$ on a field $\Bbbk$ is equivalent if open sets are the same.

Proposition 2. *FSAE.*
(a) $|\cdot|_1$ and $|\cdot|_2$ are equivalent
(b) $x_n \to a$ w.r.t $|\cdot|_1$ iff it does in $|\cdot|_2$
(c) $|x|_1 < 1$ iff $|x|_2 < 1$
(d) $|x|_1 = |x|_2^\alpha$ for some positive real α

Proof. (a) then (b):
(b) then (c): $|x| < 1$ is equivalent to $x^n \to 0$
(c) then (d): x_0 be an element $|x_0|_1 < 1$. Then by (c) $|x_0|_2 < 1$ so α determined.
If $x \in \Bbbk$, $x \neq 0$ satisfies $|x|_1 = |x_0|_1$ then $|x|_2 = |x_0|_2$ by (c).
If $|x|_1 = 1$ then by (c) we must have $|x|_2 = 1$
Also if $|x|_1 = |x|_2^\alpha$ then it holds for all x^n, integer n.
Now general choice of x, assume $|x|_1 < 1$ and $|x|_1 = |x|_2^\beta$.
n, m two positive integers.
$|x|_1^n < |x_0|_1^m$ equivalent to $|x|_2^n < |x_0|_2^m$
So

$$\frac{n}{m} < \frac{\log|x_0|_1}{\log|x|_1} \iff \frac{n}{m} < \frac{\log|x_0|_2}{\log|x|_2}$$

So $\alpha = \beta$
(d) then (a): $|x-a|_1 < r \iff |x-a|_2 < r^{1/\alpha}$ ☐

Problem 1.5. *If p, q are different primes, then the p-adic and q-adic absolute values are not equivalent.*
p-adic absolute value and ∞ absolute value are not equivalent.

Theorem 2 (Ostrowski)**.** *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for prime p or $p = \infty$.*

Proof. Case 1. $|\cdot|$ is archimedean.
n_0 a least positive integer for which $|n_0| > 1$. We can find positive real number α, $|n_0| = n_0^\alpha$
Claim: $x \in \mathbb{Q}$, $|x| = |x|_\infty^\alpha$
Or, just proving $|n| = n^\alpha$.

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k$$

where $0 \leq a_i \leq n_0 - 1$, $a_k \neq 0$.

$$|n| \leq |a_0| + |a_1| n_0^\alpha + \cdots + |a_k| n_0^{k\alpha}$$

But n_0 is a least integer whose absolute value greater than 1, $|a_i| \leq 1$

$$|n| \leq 1 + n_0^\alpha + \cdots + n_0^{k\alpha} \leq n_0^{k\alpha} \frac{n_0^\alpha}{n_0^\alpha - 1} = C n_0^{k\alpha} \leq C n^\alpha$$

$$|n^N| \leq C n^{N\alpha}$$

$$|n| \leq n^\alpha$$

This is proof for $k \geq 1$ and for $k = 0$, obvious.
Opposite direction, $n_0^{k+1} > n \geq n_0^k$,

$$n_0^{(k+1)\alpha} = |n_0^{k+1}| \leq |n| + |n_0^{k+1} - n|$$

$$\begin{aligned} |n| &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n)^\alpha \\ &\geq n_0^{(k+1)\alpha} - (n_0^{k+1} - n_0^k)^\alpha \\ &= n_0^{(k+1)\alpha}\left(1 - (1 - \frac{1}{n_0})^\alpha\right) \\ &= C' n_0^{(k+1)\alpha} > C' n^\alpha \end{aligned}$$

$$|n| \geq n^\alpha$$

Case 2. $|\cdot|$ nonarchimedean
Then $|n| \leq 1$ for all integers. Nontrivial so there exists smallest integer n_0 such that $|n_0| < 1$.
Step 1. n_0 must be a prime number. $p = n_0$.
Step 2. $n \in \mathbb{Z}$ not divisible by p, $|n| = 1$. Divide $n = rp + s$ then minimality.
Step 3. $n = p^v n'$ then $|n| = |p|^v = c^{-v}$ equivalent to p-adic absolute value. ☐

Proposition 3 (Product Formula)**.** *For any $x \in \mathbb{Q}^\times$, we have*

$$\prod_{p \leq \infty} |x|_p = 1$$

Proof. Prove first for the positive integers. $n = p_1^{a_1} \cdots p_k^{a_k}$
Trivially extends to negative, and $\mathbb{Q}$ ☐

1.2.2 Construction of p-adic Numbers

The field with absolute value is 'Complete' if every Cauchy sequence has a limit in $\Bbbk$.
$x_n \in \Bbbk$ is Cauchy sequence if $|x_n - x_m| < \epsilon$, $\forall \epsilon \exists N$

$S \subset \Bbbk$ is dense in $\Bbbk$ if every open ball $B(x, \epsilon) \cap S \neq \phi$
Example. Real Number $\mathbb{R}$ 완비성 공리... Nested Sequence...
Example. $\mathbb{Q}$ with absolute value $|\cdot|_\infty$ extends to $\mathbb{R}$ and $\mathbb{Q}$ is dense in $\mathbb{R}$

Lemma 1. *For non-archimedean absolute value field $\Bbbk$, $\{x_n\}$ is Cauchy sequence iff*

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

Proof. $|x_n - x_m| = |x_n - x_{n-1} + \cdots + x_{m+1} - x_m| \leq \max(|x_n - x_{n-1}|, \cdots, |x_{m+1} - x_m|)$ ☐

Lemma 2. *$\mathbb{Q}$ with p-adic absolute value is not complete*

Proof. Motivation: $\sqrt{2}$ in $\mathbb{R}$
Suppose $p \neq 2$.
$a \in \mathbb{Z}$ that is not square in $\mathbb{Q}$, p not dividing, $X^2 \equiv a(modp)$ has a solution
x_0 a solution. Choose $x_1 \equiv x_0(modp)$ and $x_1^2 \equiv a(modp^2)$.
$x_1 = x_0 + pb$...
In general, $x_n \equiv x_{n-1}(modp^n)$ and $x_n^2 \equiv a(modp^{n+1})$
Above lemma gives it is Cauchy. Also $x_n^2 - a$ is Cauchy. x_n limit exist, then it solves square root of a.
Suppose $p = 2$ ☐

We now 'complete' $\mathbb{Q}$ by considering Cauchy sequences...

$$\mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ Cauchy}\}$$

$(x_n)+(y_n) = (x_n+y_n)$, $(x_n)\cdot(y_n) = (x_n y_n)$ ring structure.

Problem 1.6. *What is 1, 0?*

Lemma 3. *$\tilde{x} = \{(x)\}$ then $x \mapsto \tilde{x}$ is injective. Preserving ring structure.*

Ideal

$$\mathcal{N} = \{(x_n) : x_n \to 0\}$$

Problem 1.7. *Ideal?*

Definition. Field of p-adic numbers $\mathbb{Q}_p = \mathcal{C}/\mathcal{N}$

Problem 1.8. *Field?*
Solution: (x_n) Cauchy sequence, not tending to zero. $|x_n| \geq c > 0$ for $n \geq N$. Set y_n by $y_n = 0$ for $n < N$ and $y_n = 1/x_n$ for $n \geq N$.

$$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| \leq \frac{|x_{n+1} - x_n|}{c^2} \to 0$$

Cauchy...
$\tilde{1} - (x_n)(y_n) \in \mathcal{N}$

Natural inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$

왜 이렇게까지 해야하나? 우리가 첫 시간에 배웠던 p-adic number은 다 좋고 직관적인데... 수학적이지 않은 정의... 이런 방식의 정의로부터 실제로 다루는 것에 비해 '수학적'으로는 할 수 있는게 더 많아짐. 직관은 첫 시간에 했던 것들을 유지하되, 수학적으로 증명하는 연습을 해보는 것이 중요.

이제 위 field에서 p-adic absolute value 를 정의해봅시다.

Lemma 4. *$(x_n) \in \mathcal{C} - \mathcal{N}$ then $|x_n|_p$ is eventually stationary.*

Proof. $|x_n| \geq c > 0$ if $n \geq N_1$
$n, m \geq N_2$ then $|x_n - x_m| < c$
모든 삼각형은 이등변삼각형 □

Definition. $\lambda \in \mathbb{Q}_p$ then $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$

Problem 1.9. *Well defined?*

- $|\lambda|_p = 0$ iff $\lambda = 0$
proof: Eventually stationary... Lemma so $\lambda \in \mathcal{N}$ 즉 0이어야한다.
- $|\cdot|_p$ is non-archimedean absolute value
proof: Integer에 대해서 1보다 작거나 같은... $\tilde{n}$
- $|\cdot|_p$ extends it does at $\mathbb{Q}$

Proposition 4. *Image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset.*

Proof. $\lambda \in \mathbb{Q}_p$, let $B(\lambda, \epsilon)$
(x_n) a Cauchy sequence representing λ. $\epsilon' < \epsilon$. N exists, $|x_n - x_m|_p < \epsilon'$.
$y = x_N$ and $\tilde{y} \in B(\lambda, \epsilon)$ is our claim.
$\lambda - \tilde{y}$ represented by $(x_n - y)$.

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

□

Theorem 3. *$\mathbb{Q}_p$ is complete w.r.t. $|\cdot|_p$*

Proof. $\lambda_1, \lambda_2, \cdots$ 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?)
$(|\tilde{y}_n - \tilde{y}_m|_p \leq |\tilde{y}_n - \lambda_n|_p + |\tilde{y}_m - \lambda_m|_p + |\lambda_n - \lambda_m|_p)$
$\lambda = (y_n)$. 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 $\tilde{y}_n$... □

Theorem 4. *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, $\mathbb{Q} \hookrightarrow K$.
$x_n \in \mathbb{Q}$ and look at the Cauchy sequence (x_n) in both $\mathbb{Q}_p$ and K. Both is Cauchy sequence ($\mathbb{Q}$ absolute value is extended) so converges.
$\lambda \in \mathbb{Q}_p$, there is a Cauchy sequence (x_n) whose limit is λ.
Their image in K is also Cauchy, there exists a limit $f(\lambda)$.
$f : \mathbb{Q}_p \to K$ is identity on $\mathbb{Q}$.
(Well defined?)
f is an isomorphism and preserving absolute values. □

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