p-adic Numbers 강의록

Donghyun Park

December 30, 2025

1 1강 Motivation, Field, Norm and Valuation

1.1 P-adic number

Complex number: Laurant series
$P(x)/Q(x)$

$$f(X) = \frac{X}{X-1} = -X - X^2 - \cdots$$
$$= \frac{2+(X-2)}{1+(X-2)} = 2 - (X-2) + (X-2)^2 - (X-2)^3 +$$

미적분학 복습: Region of convergence?

Every rational function can be expanded into a series : **rational functions ↔ Laurant series**

$$f(X) = \sum_{i \geq n_0} a_i (X-\alpha)^i$$

Remark 1. *$n_0 < 0$ 도 가능하다.*

비슷한 일을 정수에서 해봅시다.
$320 = 5 + 3 * 7 + 6 * 7^2$ 즉, $320 = 635$. $\frac{320}{49} = 6.35$
Nontrivial 예시
(1) $p = 5$

$$1/2 = 5 * (-1/2) + 3$$

$$-1/2 = 5 * (-1/2) + 2$$

$$1/2 = ...22223$$

(2) $p = 3$
$a = 24 = 220$, $b = 17 = 122$

$$\frac{24}{17} = \frac{2p+2p^2}{2+2p+p^2} = p+p^3+2p^5+p^7+p^8+2p^9 = ...2110201010$$

$$(2+2p+p^2)(p+p^3+2p^5+p^7+p^8+2p^9+...) = 2p+2p^2$$

성립하는 것을 알 수 있습니다.

철학: 우리가 주어진 함수를 Laurant series로 바꾸면 그 점 주변에서 함수를 잘 분석할 수 있었다. 그러면 위와 같이 유리수를 전개를 하면 소인수에 대해 정보를 더 담게 되지 않을까.
Nontrivial 예시 2

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$$

Problem 1.1. *$y = a_0 + a_1 p + \cdots$ 이면 $-y$는 어떻게 표현되는가*

그러면 우리는 모든 유리수를 이런 방식으로 표현할 수 있는가. p-adic expansion이라 부르자. injectivity? 이러한 수들을 p-adic numbers라 부르자.

Remark 2. *1. '체'의 구조를 띈다*
2. p-adic numbers는 유리수를 포함한다.
3. eventually periodic한 p-aidc 전개는 유리수
4. 유리수의 p진 전개는 eventually periodic
5. $1 + p + p^4 + p^9 + \cdots$ 는 유리수의 image가 아님. 즉 $\mathbb{Q}_p$는 유리수보다 큰 object

1.2 Motivation

$X^2 = 25$ 의 유리수근은 존재하는가?
헛짓거리 같아 보이지만, 조금 문제를 modify 해봅시다.

$$X^2 \equiv 25 (mod p^n)$$

(1) $p = 2$
$n = 1, X = 1$, $n = 2, X = 1, 3$, $n = 3, X = 1, 3, 5, 7$, $n \geq 4$
...
(2) $p = 5$
(3) $p \neq 2, 5$

$$X \equiv \pm 5 (mod p^n)$$

이제 $p = 3$을 봐봅시다.
$X^2 \equiv 25 (mod 3)$, $X = 1, 2 mod 3$.
$X^2 \equiv 25 (mod 9)$, $X = 1 mod 3$이라면 $X = 4 mod 9$, $X = 2 mod 3$ 이라면 $X = 5 mod 9$
$X^2 \equiv 25 (mod 27)$, $X = 4 mod 9$ 이면 $X = 22 mod 27$, $X = 5 mod 9$ 이면 $X = 5 mod 27$
1, 4, 22, 76... and 2,5,5,5...
이런 수열을 p-adically coherent. $0 \leq \alpha_n \leq p^n - 1$ s.t. $\alpha_{n+1} \equiv \alpha_n (mod p^n)$
그런데 $X = -5$의 3-adic expansion; ....22222211.

다른 example. $X^2 \equiv 2 (mod 7^n)$
mod 7로 보면 3,4. 이제 3+7k로 놓고 7^2에서 보면... (직접 해보기)
4,39,235,235 and 3,10,108,2166 무한히 지속되는가? Yes!
두 7-adic number가 있다. $x_1 = ...6213$, $x_2 = ...0454$. $X^2 = 2$ in $\mathbb{Q}_7$ has two roots.

Problem 1.2. *1. $X^2 = 2$의 solution이 $\mathbb{Q}_5$ 에서 없음을 보여라.*
2. $X^2 + 1 = 0$이 $\mathbb{Q}_5$에서 solution을 가짐을 보여라.

실제로 위의 문제들을 일반화해서 풀 수 있는 방법 (알고리즘)을 뒤에서 공부할 예정. Hensel's Lemma.
p-adic number은 유리수보다 할 수 있는게 더 많다!

1.3 Local Global Principle

Hilbert's 10th problem : 주어진 디오판틴 방정식이 주어질 때 방정식의 해가 존재하는지 여부를 결정하는 알고리즘이 존재하는가?

$$3X^2 + 2Y^2 - Z^2 = 0$$

$$X^3 + Y^3 + Z^3 = 0$$

이번 p-adic number의 중요한 application이 이 문제에 대한 국소적 해답으로 존재.

동차이차식에 대해서 주어진 디오판틴 방정식의 유리수 근이 존재할 필요충분조건은 디오판틴 방정식의 실수근과 $\mathbb{Q}_p$ 근이 존재하는 것이다.

1.4 Field

Field란 덧셈과 곱셈이 아래 성질들을 만족하는 것들.
- Associativity(결합법칙): $a+(b+c) = (a+b)+c$, $a\cdot(b\cdot c) = (a\cdot b)\cdot c$
- Commutativity(교환법칙): $a+b = b+a$, $a\cdot b = b\cdot a$
- Identity: $a+0 = 0+a = a$, $a\cdot 1 = 1\cdot a = a$
- Additive inverse: $a+(-a) = 0$
- Multiplicative inverse: $a \neq 0$ 이면 $a\cdot a^{-1} = 1$
- 분배법칙: $a\cdot(b+c) = a\cdot b + a\cdot c$

$\Bbbk$로 체를 표기하겠습니다.

예시들.
(1) $\Bbbk = \mathbb{R}, \mathbb{Q}, \mathbb{C}$. $\mathbb{Z}$ 는 체가 아님.
(2) $\mathbb{F}_p$. 원소들은 $0, 1, 2, \cdots, p-1$. 연산은 나머지 연산으로. 체인 것을 확인해보기.

Problem 1.3. *(수업시간에 풀기) $\mathbb{Z}/n\mathbb{Z}$가 체가 되기 위한 필요충분조건. n이 소수.*

1.5 Valuation

Definition : Absolute value on field $\Bbbk$ is a function $|\cdot| : \Bbbk \to \mathbb{R}^+$ that
- $|x| = 0$ if and only if $x = 0$
- $|xy| = |x||y|$
- $|x+y| \leq |x| + |y|$

Definition:
If $|x+y| \leq \max(|x|, |y|)$ holds then we call nonarchimedean. Otherwise, we call archimedean.
Example. $\Bbbk = \mathbb{Q}$, $||$ the usual absolute value. Archimedean.
Trivial Absolute Value.

Definition : for $x \in \mathbb{Q}$, define p-adic absolute value
p-adic valuation on $\mathbb{Z}$ is $v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$ such that $n = p^{v_p(n)}n'$ with $p \nmid n'$ and extend to $\mathbb{Q}$ by $x = a/b \in \mathbb{Q}^\times$,

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

with $v_p(0) = +\infty$

$$|x|_p = p^{-v_p(x)}$$

and $|0|_p = 0$

Problem 1.4. *p-adic valuation is well-defined. (Why is this important?)*

Lemma 1 ([Gou20] Lemma 2.1.3)**.** *For all $x, y \in \mathbb{Q}$,*
- $v_p(xy) = v_p(x) + v_p(y)$
- $v_p(x+y) \geq \min(v_p(x), v_p(y))$

Proposition 1 ([Gou20] Proposition 2.1.5)**.** *The function $|\cdot|_p$ is non-archimedean absolute value on $\mathbb{Q}$*

Intuition on p-adic valuations

Problem 1.5. *$|p^n|_p \to 0$ as $n \to \infty$*

1.6 Basic Properties

Lemma 2 ([Gou20] Lemma 2.2.1)**.** *For any absolute value on $\Bbbk$*
- $|1| = 1$
- $x^n = 1$ *then* $|x| = 1$
- $|-1| = 1$
- $|-x| = |x|$

1.7 Non-archimedean Property

Lemma 3 ([Gou20] Lemma 2.2.2)**.** *$\Bbbk$ is a field and absolute value. FSAE*
- $x, y \in \Bbbk$, $|x+y| \leq \max(|x|, |y|)$
- $|x+1| \leq \max(|x|, 1)$

Lemma 4 ([Gou20] Lemma 2.2.3)**.** *$\Bbbk$ a field and $|\cdot| : \Bbbk \to \mathbb{R}_+$*
(a) $|x| = 0$ iff $x = 0$
(b) $|xy| = |x||y|$
(c) $|x| \leq 1 \Rightarrow |x-1| \leq 1$
Then the function is non-archimedean absolute value on $\Bbbk$.

Proof. If $|x| \leq 1$ then by final property $|x-1| = |1-x| \leq 1$
If $|x| > 1$ then $|1/x| < 1$ so $|1 + 1/x| \leq 1$ so $|(x+1)/x| \leq 1$ □

Theorem 1 ([Gou20] Theorem 2.2.4)**.** *$A \subset \Bbbk$ the image of $\mathbb{Z}$ on $\Bbbk$. The absolute value on $\Bbbk$ is non-archimedean if and only if $|a| \leq 1$ for $a \in A$.*

Proof. Nonarchimedean then by Lemma 3 and induction
Converse direction: Prove $|x+1| \leq \max(|x|, 1)$

$$|x+1|^m = |\sum_{k=0}^{m} \binom{m}{k} x^k| \leq \sum_{k=0}^{m} |\binom{m}{k}||x|^k \leq \sum_{k=0}^{m} |x|^k$$

$$|x+1|^m \leq (m+1)\max(1, |x|^m)$$

$$|x+1| \leq \max(|x|, 1)$$

□

This is related to **Archimedean Property** : Given $x, y \in \Bbbk$, $x \neq 0$ there exists a positive integer n such that $|nx| > |y|$.
"Is there are arbitrarily big integers?"

Remark 3. *Real Number $\mathbb{R}$, 아르키메디안 법칙은 유리수 조밀성과 연관*
매우 큰 자연수가 존재하므로, $0 < \frac{1}{n} < b - a$ 가 존재. 이제 $k \cdot \frac{1}{n} > a$ 자연수 k가 존재. 이 집합의 최소 원소 m에 대해

$$a < \frac{m}{n} < b$$

1.8 Distance

Now, the distance function $d(x, y) = |x - y|$ defines metric (거리) on $\Bbbk$.
Recall the 거리공간.
- $d(x, y) \geq 0$ and $d(x, y) = 0$ iff $x = y$
- $d(x, y) = d(y, x)$
- $d(x, z) \leq d(x, y) + d(y, z)$ 삼각부등식

실수에서 당연히 성립하는 것들.
열린집합과 닫힌집합. $B(x, r) = \{y \in \mathbb{R}^n : |y - x| < r\}$. U가 열린집합 (open)인 것은 $x \in U$, $N(x, r) \subset U$

Problem 1.6. *실수가 아닌 임의의 거리공간에서도*
- 공집합과 자기자신이 열린집합
- 열린집합의 합집합은 열린집합
- 열린집합 두 개의 교집합은 열린집합
- $B(x,r)$은 항상 열린집합
! 삼각부등식의 중요성

So $\mathbb{k}$ with valuation. Axiom checking
Valuation이라 불렀던 것. distance는 valuation으로 $|x-y|$
Definition.
- $|x|=0$ if and only if $x=0$
- $|xy|=|x||y|$
- $|x+y|\leq|x|+|y|$

Non-archimedean 도 있었다...

Lemma 5 ([Gou20] Lemma 2.2.3)**.** *$d(x,y)=|x-y|$ is non-archimedean iff*

$$d(x,y)\leq\max(d(x,z),d(z,y))$$

실제로는,

Proposition 2 ([Gou20] Proposition 2.3.4)**.** *Non-archimedean absolute value on $\mathbb{k}$. If $|x|\neq|y|$*

$$|x+y|=\max(|x|,|y|)$$

즉, 모든 삼각형은 이등변삼각형. 거기에 길이가 같은 변은 다른 변의 길이보다 길다.
다시. $B(a,r)=\{x\in\mathbb{k}:|x-a|<r\}$, $\bar{B}(a,r)=\{x\in\mathbb{k}:|x-a|\leq r\}$

Proposition 3 ([Gou20] 2.3.7)**.** *Non-archimedean absolute value에 대해서*
(a) $b\in B(a,r)$ then $B(a,r)=B(b,r)$
(b) $b\in\bar{B}(a,r)$ then $\bar{B}(a,r)=\bar{B}(b,r)$
(c) $B(a,r)$ is open and closed. (proof: $d(y,a)\geq r$ then $B(y,s)$ for all $s<r$ is open ball)
(d) $r\neq0$, $\bar{B}(a,r)$ is open and closed
(e) $B(a,r)\cap B(b,s)\neq\phi$ iff $B(a,r)\subset B(b,s)$ or $B(a,r)\supset B(b,s)$ (proof: (a)에 의해 자명)
(f) $r,s\neq0$, $\bar{B}(a,r)\cap\bar{B}(b,s)\neq\phi$ iff $\bar{B}(a,r)\subset\bar{B}(b,s)$ or $\bar{B}(a,r)\supset\bar{B}(b,s)$

결국 중요한건 모든 삼각형은 이등변삼각형이고, 같은 변 길이가 가장 길다.

1.8.1 Connectedness

실수에서... 연결집합은 두 open set의 disjoint union으로 표현 불가한 것.
$S\subset\mathbb{R}$ connected iff $U\cap S\neq\phi$, $V\cap S\neq\phi$, $U\cap V\cap S=\phi$, $U\cup V\supseteq S$인 U,V do not exist
Or U,V open in S, $U\cap V=\phi$, $U\cup V=S$ do not exist
Connected component가 있었다.

Proposition 4 ([Gou20] Proposition 2.3.9)**.** *Field $\mathbb{k}$ with non-archimedean absolute value, the connected component containing $x\in\mathbb{k}$ is $\{x\}$. i.e. any set containing x, connected component is x itself.*

Proof. $B(x,r)$ is open and closed. □

Corollary 1 ([Gou20] Corollary 2.3.10)**.** *$\mathbb{k}$ with a non-archimedean absolute value, there are no non-constant continuous function $\mathbb{R}\to\mathbb{k}$*

연속함수의 정의가 뭐였더라?

References

[Gou20] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction*. 3rd. Universitext. Springer, 2020. ISBN: 978-3-030-47295-5. DOI: 10.1007/978-3-030-47295-5.