p-adic Numbers 강의록

Donghyun Park

January 21, 2026

1 8강. Extensions of $\mathbb{Q}_p$

K/F가 field extension일 때 다음 함수를 정의할 수 있다 (norm이라 부르는)

$$N_{K/F} : K \to F$$

Definition 1. $\alpha \in K$, the map $\alpha : K \to K$, sending $x \mapsto \alpha x$, the determinant of this linear map is $N_{K/F}(\alpha)$
Definition 2. $\alpha \in K$, $F(\alpha)$가 subextension. $r = [K : F(\alpha)]$라 두고, α를 근으로 갖는 최소 다항식

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in F[X]$$

일 때 $N_{K/F}(\alpha) = (-1)^{nr}a_0^r$
Definition 3(If K/F normal). Product of all $\sigma(\alpha)$

Equivalence checking.
1 and 2 : 우선 $K = F(\alpha)$라면, $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$이 basis를 이룬다. 다음으로 $K \neq F(\alpha)$이면 $\{\alpha^i b_j\}$꼴의 basis를 잡을 수 있다. ($K/F(\alpha)$ basis $b_1, \cdots, b_r$)

2 and 3 : $K = F(\alpha)$: $\sigma(\alpha)$는 $f(X)$의 근. 반대로 $f(X)$의 다른 근 β (in C)에 대해, $K = F(\alpha) \to F(\beta)$ sending α to β가 존재. Normal에 의해 $\beta \in K$, $\beta = \sigma(\alpha)$. 따라서 이 경우 2,3 동치. $K \neq F(\alpha)$라면 $[K : F(\alpha)]$ 만큼의 중복.

몇가지 성질을 살펴보면
- $\alpha \in F$, $N_{K/F}(\alpha) = \alpha^n$
- $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$
- $N_{L/F}(N_{K/L}(\alpha)) = N_{K/F}(\alpha)$ if $F \subset L \subset K$

Example. $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ calculate $N_{K/F}(a + b\sqrt{2})$
Definition 1. Basis를 $\{1, \sqrt{2}\}$로 잡으면 행렬표현

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$$

Determinant $a^2 - 2b^2$
Definition 2. $b = 0$ 이면 $r = 1$, $X - a$가 minimal polynomial 이므로 a^2. $b \neq 0$ 이면 $r = 2$, minimal polynomial $X^2 - 2aX + (a^2 - 2b^2)$ 따라서 $a^2 - 2b^2$
Definition 3. $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$가 automorphism.

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

이제, Norm을 도입한 이유를 들여다봅시다. $K/\mathbb{Q}_p$ field extension and normal이고 absolute value on K가 있다면, $x \to |\sigma(x)|$도 absolute value. 따라서 $|x| = |\sigma(x)|$.

$$|\prod_\sigma \sigma(x)| = |x|^n$$

따라서 $|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|}$로 정의되어야 한다.

Lemma 1 ([Gou20] Lemma 6.3.3)**.** *L, K be finite extensions of $\mathbb{Q}_p$ which $\mathbb{Q}_p \subset L \subset K$. $x \in L$, $m = [L : \mathbb{Q}_p], n = [K : \mathbb{Q}_p]$ then*

$$\sqrt[m]{|N_{L/\mathbb{Q}_p}(x)|_p} = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

Proof. $N_{K/F}(x) = N_{L/\mathbb{Q}_p}(N_{K/L}(x))$, $N_{K/L}(x) = x^{[K:L]}$ □

따라서 normal이 아니더라도 normal closure로 가서 정의한 것과 definition이 똑같고,

Proposition 1 ([Gou20] Proposition 6.3.4)**.** *If there is an absolute value on K extending the p-adic absolute value, then it must be given by the formula*

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

where $n = [K : \mathbb{Q}_p]$

Theorem 1 ([Gou20] Theorem 6.3.5)**.** *$K/\mathbb{Q}_p$ be a finite extension of degree n. $|\cdot| : K \to \mathbb{R}^+ \cup \{0\}$ defined by*

$$|x| = \sqrt[n]{|N_{K/\mathbb{Q}_p}(x)|_p}$$

is a non-archimedean absolute on K which extends the p-adic absolute value on $\mathbb{Q}_p$

Proof. $|x| = 0$ iff $N_{K/\mathbb{Q}_p}(x) = 0$, multiplication by x is degenerate so $x = 0$.
$N_{K/\mathbb{Q}_p}(xy) = N_{K/\mathbb{Q}_p}(x)N_{K/\mathbb{Q}_p}(y)$이므로 $|xy| = |x||y|$
마지막으로, $|x| \leq 1$이면 $|x - 1| \leq 1$을 보입시다. Equivalent to

$$|N_{K/\mathbb{Q}_p}(x)|_p \leq 1 \Rightarrow |N_{K/\mathbb{Q}_p}(x - 1)|_p \leq 1$$

혹은

$$N_{K/\mathbb{Q}_p}(x) \in \mathbb{Z}_p \Rightarrow N_{K/\mathbb{Q}_p}(x - 1) \in \mathbb{Z}_p$$

$K = \mathbb{Q}_p(x) = \mathbb{Q}_p(x - 1)$이라 두고, minimal polynomial of x

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

minimal poly of $x - 1$ is $f(X + 1)$. 상수항을 살펴보면 $1 + a_{n-1} + \cdots + a_1 + a_0$.

$$N_{K/\mathbb{Q}_p}(x) = (-1)^n a_0$$

$$N_{K/\mathbb{Q}_p}(x - 1) = (-1)^n(1 + a_{n-1} + \cdots + a_0)$$

이제 Lemma □

Lemma 2 ([Gou20] Lemma 6.3.6)**.** *$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ a monic irreducible polynomial with coefficients in $\mathbb{Q}_p$ and $a_0 \in \mathbb{Z}_p$, then $a_{n-1}, \cdots, a_1 \in \mathbb{Z}_p$.*

Proof. If $a_j \notin \mathbb{Z}_p$. 그러면 적절히 p^m 곱해서 $g(X) = p^m f(X) = b_n X^n + \cdots + b_0$. $b_n = p^m$, $b_0 = p^m a_0$, at least one b_i not divisible by p.

$$g(X) \equiv (b_n X^{n-k} + \cdots + b_k)X^k (mod\ p)$$

Hensel lemma for polynomials, $g(X) = p^m f(X)$ reducible so is $f(X)$. □

1.1 Finite Extensions of $\mathbb{Q}_p$

Motivation. $F_1 = \mathbb{Q}_5(\sqrt{2})$, $F_2 = \mathbb{Q}_5(\sqrt{5})$, $F_3 = \mathbb{Q}_3(\zeta, \sqrt{2})$, ζ cube root of unity
Definition. For $K/\mathbb{Q}_p$ finite extension, $|\cdot|$ be the p-adic absolute value on K. p-adic valuation is $v_p(x)$ a unique rational number satisfying

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

We know

$$v_p(x) = \frac{1}{n} v_p(N_{K/\mathbb{Q}_p}(x))$$

for $x \in K^\times$
- F_1, $x = 1+3\sqrt{2}$, $N_{K/\mathbb{Q}_p}(x) = 1^2 - 2\times 3^2 = -17$, $v_5(x) = 0$.
- F_2, $x = \sqrt{5}$, $N_{K/\mathbb{Q}_p}(x) = -5$, $v_5(x) = 1/2$
- F_3, $x = \sqrt{2}$, $N_{K/\mathbb{Q}_p}(x) = (\sqrt{2} \times -\sqrt{2})^2 = -4$, $v_3(x) = 0$.
$x = \zeta$, $N_{K/\mathbb{Q}_p}(x) = (\zeta \times \zeta^2)^2 = 1$, $v_3(x) = 0$. $x = 1 - \zeta$, $N_{K/\mathbb{Q}_p}(x) = ((1-\zeta)(1-\zeta^2))^2 = 9$, $v_3(x) = 1/2$.

Proposition 2 ([Gou20] Propsoition 6.4.2)**.** *The p-adic valuation v_p is a homomorphism from the multiplicative group $K^\times$ to the additive group $\mathbb{Q}$. Its image is the form $\frac{1}{e}\mathbb{Z}$ where e is a divisor of $n = [K : \mathbb{Q}_p]$*

So we define $e = e(K/\mathbb{Q}_p)$ the ramification index of K over $\mathbb{Q}_p$.
- $K/\mathbb{Q}_p$ is **unramified** if $e = 1$
- $K/\mathbb{Q}_p$ is **totally ramified** if $e = n$
- $K/\mathbb{Q}_p$ is **ramified** if $e > 1$
Write $f = f(K/\mathbb{Q}_p) = n/e$ be a residual degree of K over $\mathbb{Q}_p$
우리의 Motivation은 사실, F_1 unramified. F_2 totally ramified. F_3 ramified but not totally ramified extensions.

Proof. F_1 에서 $N_{F_1/\mathbb{Q}_5}(a+b\sqrt{2}) = a^2 - 2b^2$, $v_5(a^2-2b^2) = 0, 2, 4, \cdots$ 이므로 $e = 1$

F_2 에서 $N_{F_2/\mathbb{Q}_5}(a+b\sqrt{5}) = a^2 - 5b^2$, $v_5(a^2-5b^2) = 0, 1, 2\cdots$ 이므로 $e = 2 = n$

F_3에서 $\zeta \mapsto \zeta^2$, $\sqrt{2} \mapsto -\sqrt{2}$가 automorphism...
$N_{F_3/\mathbb{Q}_3}(a+b\zeta+c\zeta^2+d\sqrt{2}) = (a+b\zeta+c\zeta^2+d\sqrt{2}) \times (a+b\zeta+c\zeta^2-d\sqrt{2}) \times (a+c\zeta+b\zeta^2+d\sqrt{2}) \times (a+c\zeta+b\zeta^2-d\sqrt{2}) = (a^2+b^2+c^2-ab-bc-ca-2d^2)^2 + 6d^2(b-c)^2$
$a^2+b^2+c^2-ab-bc-ca \equiv 0, 1 (mod\ 3)$, $2d^2 \equiv 0, 2 (mod\ 3)$ so minimum divisible by 9. $v_3(a+b\zeta+c\zeta^2+d\sqrt{2}) \geq 1/2$. Equality holds when $1-\zeta$, $e = 2$. □

We define **Uniformizer**. Let $K/\mathbb{Q}_p$ be a finite extension, and $e = e(K/\mathbb{Q}_p)$. The element $\pi \in K$ is a uniformizer if $v_p(\pi) = 1/e$.

Proposition 3 ([Gou20] Proposition 6.4.5)**.** *Let notations be as above, and fix a uniformizer π in K. Then*
(a) The ideal $\mathfrak{p}_K \subset \mathcal{O}_K$ is principal, and π is a generator
(b) Any element $x \in K$ can be written in the form $x = u\pi^{ev_p(x)}$ where $u \in \mathcal{O}_K^\times$ is a unit, and therefore satisfies $v_p(u) = 0$. In particular $K = \mathcal{O}_K[1/\pi]$
(c) The residue field $\Bbbk = \mathcal{O}_K/\mathfrak{p}_K$ is a finite extension of $\mathbb{F}_p$ whose degree is less or equal to the degree $[K : \mathbb{Q}_p]$. In particular, the number of elements in $\Bbbk$ is a power of p.
(d) Any element of $\mathcal{O}_K$ is the root of a monic polynomial with coefficients in $\mathbb{Z}_p$
(e) Conversely, if $x \in K$ is the root of a monic polynomial with coefficients in $\mathbb{Z}_p$ then $x \in \mathcal{O}_K$
(f) $\mathcal{O}_K$ is a compact ring. The sets $\pi^m\mathcal{O}_K$, $m \in \mathbb{Z}$ form a fundamental system of neighborhoods of zero in K. K is a totally disconnected, Hausdorff, locally compact topological space.
(g) l be the number of elements of the residue field $\Bbbk$ and $A = \{c_1, \cdots, c_l\} \subset \mathcal{O}_K$ be a fixed set of representatives for the elements of $\Bbbk$. Then $x \in K$ has a unique representation

$$x = a_{-m}\pi^{-m} + \cdots + a_0 + a_1\pi + \cdots$$

where $a_i \in A$.

Proof. (a) $x \in \mathfrak{p}_K$ equivalent to $v_p(x) > 0$, $v_p(x) \geq 1/e$ or $v_p(\pi^{-1}x) \geq 0$ so $\pi^{-1}x \in \mathcal{O}_K$. So π generates $\mathfrak{p}_K$
(b) Is almost trivial
(c) The set of elements of $\mathcal{O}_K$ is linearly dependent over $\mathbb{Q}_p$ then their reductions modulo π is linearly dependent over $\mathbb{F}_p$. Finite extension of $\mathbb{F}_p$ is $\mathbb{F}_{p^l}$ form..
(d) Monic irreducible polynomial with coefficients in $\mathbb{Q}_p$를 잡고, 이때 $(-1)^{nr}a_0^r \in \mathbb{Z}_p$이므로, $a_0 \in \mathbb{Z}_p$ 지난번 Lemma에 의해 모든 coefficient가 다 $\mathbb{Z}_p$에 있어야한다.
(e) $|a_0| = |x||a_1 + a_2x + \cdots| \leq 1$
(f) $\mathbb{Q}_p$에서 하던 것과 같은 일
(g) 마찬가지로 $\mathbb{Q}_p$에서 했던 것과 같음 □

우리의 motivation F_1, F_2, F_3에 대해서는, $F_1 = \mathbb{Q}_5(\sqrt{2})$ $\mathcal{O} = \mathbb{Z}_5[\sqrt{2}]$, $\Bbbk = \mathbb{F}_5[\sqrt{2}]$ order 25 field.
$F_2 = \mathbb{Q}_5(\sqrt{5})$, $\mathcal{O} = \mathbb{Z}_5[\sqrt{5}]$ and $\Bbbk = \mathbb{F}_5$.
$F_3 = \mathbb{Q}_3(\zeta, \sqrt{2})$, $\mathcal{O} = \mathbb{Z}_3[\zeta, \sqrt{2}]$ and $\Bbbk$ is field of order 9.

Theorem 2 ([Gou20] Theorem 6.4.6)**.** *Still using the notations above, let $f = f(K/\mathbb{Q}_p)$ be the residual degree of K over $\mathbb{Q}_p$. Then $[\Bbbk : \mathbb{F}_p] = f$. In particular $\Bbbk = \mathbb{F}_{p^f}$*

Proof. $m = [\Bbbk : \mathbb{F}_p]$. Then if we prove $e \cdot m = n = [K : \mathbb{Q}_p]$, $m = f$.
Choose elements $\alpha_1, \cdots, \alpha_m \in \mathcal{O}_K$ such that images in $\Bbbk$ are a basis of $\Bbbk$ over $\mathbb{F}_p$.
Now, consider the elements

$$\begin{aligned} &\alpha_1, \cdots, \alpha_m, \\ &\pi\alpha_1, \cdots, \pi\alpha_, \\ &\cdots \\ &\pi^{e-1}\alpha_1, \cdots, \pi^{e-1}\alpha_m \end{aligned}$$

We claim these form a basis of K over $\mathbb{Q}_p$.
It suffices to prove for all elements in $\mathcal{O}_K$, since then every $x \in K$ satisfies $p^r x \in \mathcal{O}_K$.
$x \in \mathcal{O}_K$, reduce modulo π

$$x = x_{0,1}\alpha_1 + \cdots + x_{0,m}\alpha_m + (multiple\ of\ \pi)$$

for $x_{0,j} \in \mathbb{Z}_p$.
Repeating,

$$\begin{aligned} x = &x_{0,1}\alpha_1 + \cdots + x_{0,m}\alpha_m \\ &+ x_{1,1}\pi\alpha_1 + \cdots + x_{1,m}\pi\alpha_m \\ &+ \cdots \\ &+ x_{e-1,1}\pi^{e-1}\alpha_1 + \cdots + x_{e-1,m}\pi^{e-1}\alpha_m \\ &+ px' \end{aligned}$$

and $x_{i,j} + px'_{i,j} + p^2x''_{i,j} + \cdots$ converges to $y_{i,j}$

$$x = \sum_{i=0}^{e-1}\sum_{j=1}^{m} y_{i,j}\pi^i\alpha_j$$

so expressed by $\mathbb{Z}_p$ linear combination of $\pi^i\alpha_j$

To show that $\pi^i\alpha_j$ are independent, if there is a nontrivial linear dependence relation

$$\sum_{i,j} x_{i,j}\pi^i\alpha_j = 0$$

, $x_{i,j} \in \mathbb{Q}_p$ then we can suppose $x_{i,j}$ all lie in $\mathbb{Z}_p$ and at least one is not divisible by p.
Reducing to modulo π, gives dependence relation for the $\bar{\alpha}_j \in \Bbbk$. Thus $x_{0,j}$ are all divisible by p. If $e = 1$ then this is contradiction.
If $e > 1$, divide the whole equation by π, then $x_{1,j}$ are all divisible by p. Keep going on, $x_{i,j}$ are all divisible by p. □

1.2 Classifying Extensions of $\mathbb{Q}_p$

1.2.1 Totally ramified Extension

Totally ramified Extension $e = n$

Proposition 4 ([Gou20] Proposition 6.5.1)**.** *Let $K/\mathbb{Q}_p$ be a totally ramified finite extension of $\mathbb{Q}_p$, so that $e(K/\mathbb{Q}_p) = n = [K : \mathbb{Q}_p]$. Then $K = \mathbb{Q}_p(\pi)$, where π is a unifomizer. Furthermore π is a root of a polynomial that satisfies Eisenstein criterion*

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Q}_p[X]$$

$p \mid a_i$ for $0 \le i < n$, $p^2 \nmid a_0$.

Proof. π be a unifomizer. $v_p(\pi) = 1/n$. $f(X)$ be the minimal polynomial for π over $\mathbb{Q}_p$. If the degree of $f(X)$ is s and its last coefficient is a_0. $r = n/s$ then the norm of π is $(-1)^n a_0^r$. so

$$p^{-1/n} = |\pi| = \sqrt[n]{|a_0^r|} = \sqrt[s]{|a_0|}$$

So, $s = n$ and $|a_0| = p^{-1}$.
Thus, $\mathbb{Q}_p(\pi) = K$ when considering the degree over $\mathbb{Q}_p$. If we set the other roots $\pi_2, \cdots, \pi_n$, then they have the same norm (since they have the same minimal polynomial) so $|\pi_i| < 1$. The coefficients of $f(X)$ are divisible by p. □

Remark 1. *Eisenstein theorem shows that the polynomial of the above form is irreducible.*

1.2.2 Unramified Extension

Hensel Lemma가 성립합니다.

Theorem 3 ([Gou20] Theorem 6.5.2)**.** *Let K be a finite extension of $\mathbb{Q}_p$ and π be a uniformizer. Let $F(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial whose coefficients are in $\mathcal{O}_K$. Suppose that there exists an $\alpha_1 \in \mathcal{O}_K$ such that*

$$F(\alpha_1) \equiv 0 (mod\ \pi)$$

$$F'(\alpha_1) \not\equiv 0 (mod\ \pi)$$

Then there exists an $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv \alpha_1 (mod\ \pi)$ and $F(\alpha) = 0$.

Corollary 1 ([Gou20] Corollary 6.5.3)**.** *$K/\mathbb{Q}_p$ be a finite extension, and let $f = f(K/\mathbb{Q}_p)$. Then $\mathcal{O}_K^\times$ contains the cyclic group of $(p^f - 1)$-st roots of unity.*

Proof. $F_m(X) = X^m - 1$ have exactly m roots for each $m \mid p^f - 1$ by the Hensel's lemma. □

반대로 $(m, p) = 1$이고 $(m, p^f - 1) = 1$이며 $\zeta^m = 1$이면 $\zeta \equiv 1 (mod\ \pi)$를 보일 수 있습니다.

$$\zeta \equiv 1 (mod\ \pi)$$

이고, 어떤 r이 있어 $p^r \equiv 1 (mod\ m)$이다.

Lemma 3 ([Gou20] Lemma 6.5.4)**.** *$x \equiv 1 (mod\ \pi)$ then $x^p \equiv 1 (mod\ \pi^2)$, and more generally $x^{p^r} \equiv 1 (mod\ \pi^{r+1})$*

Proof. Binomial Theorem. □

$$\zeta = \zeta^{p^r} \equiv 1 (mod\ \pi^{r+1})$$

... Iterating, $\zeta = 1$.

Proposition 5 ([Gou20] Proposition 6.5.5)**.** *For each f, there is exactly one unramified extension of degree f. It can be obtained by adjoining to $\mathbb{Q}_p$ a primitive $(p^f - 1)$-st root of unity.*

Proof. 여기서 unique하다는 것은... $\mathbb{Q}_p$의 한 algebraic closure을 잡을 때 algebraic closure 안에 unique subfield K that is unramified of degree f 가 있다는 의미이다.
$\bar{\alpha}$ 가 $\mathbb{F}_{p^f}^\times$의 generator라고 합시다. (Nontrivial fact: finite field의 nonzero element들은 곱셈에 대해 cyclic group을 이룬다)
그러면 $\mathbb{F}_{p^f} = \mathbb{F}_p(\bar{\alpha})$, extension of degree f.

$$\bar{g}(X) = X^f + \bar{a}_{f-1}X^{f-1} + \cdots + \bar{a}_1X + \bar{a}_0$$

가 minimal polynomial for $\bar{\alpha}$ over $\mathbb{F}_p$라고 합시다. 이 계수를 $\mathbb{Z}_p$로 아무 방식으로 올리면 $g(X) \in \mathbb{Z}_p[X]$, $\mathbb{Q}_p$에서 irreducible.
α를 $g(X)$의 한 근이라고 하면 $K = \mathbb{Q}_p(\alpha)$는 degree f extension. 또한, 이 K에서 residue field는 $\bar{\alpha}$라는 $\bar{g}(X)$의 근을 가진다. 따라서 $[\Bbbk : \mathbb{F}_p] \ge f$이고,

$$f = [K : \mathbb{Q}_p] \ge [\Bbbk : \mathbb{F}_p] \ge f$$

따라서 $K/\mathbb{Q}_p$는 unramified extension.

Uniqueness. Corollary 6.5.3에 의하여 $\mathbb{O}_K^\times$는 $p^f - 1$ roots of unity를 포함한다. 따라서 smallest field extension of $\mathbb{Q}_p$ which contains the $(p^f - 1)$-st roots of unity is already degree f 임을 보이면 끝난다.
β가 $(p^f - 1)$-st roots of unity라고 하면

$$\mathbb{Q}_p \subset \mathbb{Q}_p(\beta) \subset K$$

또한, β^i는 modulo π로 모두 distinct하기 때문에 (check!) residue field of $\mathbb{Q}_p(\beta)/\mathbb{Q}_p$는 $\Bbbk = \mathbb{F}_{p^f}$를 포함한다. 즉, $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \ge [\Bbbk' : \mathbb{F}_p] \ge f$ 따라서 $K = \mathbb{Q}_p(\beta)$ □

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.