p-adic Groups

Guo Haoyang

March 2025

Contents

1 Construction of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

1.1 Completion of $\mathbb{Q}$

1.2 Extending the absolute value

2 Algebraic properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

2.1 Properties of $\mathbb{Z}_p$

First, $\mathbb{Z}_p$ is a local ring and $\mathbb{Z}_p$ is compact. Hence, the results on local rings are applicable to detect the precise structure of $\mathbb{Z}_p$. It has unique maximal ideal and then can be decomposed into its collection of units $\mathbb{Z}_p^\times$ and maximal ideals $\mathfrak{m}$. At the same time, $\mathbb{Z}_p$ is also a (discrete) valuation ring. By virtue of the language of valuation, the detailed structure of $\mathbb{Z}_p^\times$ and $\mathfrak{m}$ is explicit.

Theorem 2.1: Exact sequence of $\mathbb{Z}_p$

The sequence

$$\{0\} \longrightarrow \mathbb{Z}_p \xrightarrow{[p^m]} \mathbb{Z}_p \longrightarrow \mathbb{Z} \longrightarrow \{0\}$$

where $[p^m] : x \mapsto p^m \cdot x$ and , is a short exact sequence.

This theorem gives the structure of $\mathbb{Z}_p/p^m\mathbb{Z}_p$.

Corollary 2.1: Ring Type of $\mathbb{Z}_p$

Every ideal of $\mathbb{Z}_p$ is of the form $\langle p^n \rangle$ for some $n \geq 0$. Hence, $\mathbb{Z}_p$ is a principal ideal domain and a local ring.

Proof: Take an arbitrary ideal $I \neq \{0\} \trianglelefteq \mathbb{Z}_p$. Let $m := \inf\{v_p(a) : a \in I\}$. Since $I \neq \{0\}$, then $m < \infty$. So, $\forall a \in I$, $a = p^m u \in p^m\mathbb{Z}_p$. Hence, $I \subseteq \langle p^m \rangle$. Now take an arbitrary element $b \in \langle p^m \rangle$, $b = p^m u$ with $u \in \mathbb{Z}_p^\times$. Hence, $u^{-1} \in Z_p$ and $p^m = u^{-1} b \in I$ since I is an ideal. Then, $\langle p^m \rangle \subseteq I$. □

Remark $\mathbb{Z}_p$ is a local ring hence a PID hence a UFD. This would be useful in 2.1

2.2 Properties of $\mathbb{Q}_p$

2.3 Hensel's lemma

'Hensel's lemma' is probably the most important algebraic property of the p-adic numbers ([Gou20]). It basically says that if some information is given in modulo some power of p, i.e. p^k or $\mathbb{Z}/p^k\mathbb{Z}$, then then we know the limit case of that information $\mathbb{Z}_p$. In the meanwhile, modulo congruences are approximations: $a \equiv b \pmod{p^k}$ is equivalent to $|a-b|_p \leq p^{-k}$. From the perspective of approximation, the Hensel's lemma says that if we know the approximation of an element within any precision, say for any k, a_k approximates α within p^{-k}, then we know the information of α.

Theorem 2.2: Hensel's lemma: For simple roots

Let $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}_p[x]$. If $\exists$ a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ with

$$f(\alpha_1) \equiv 0 \bmod p \quad f'(\alpha_1) \not\equiv 0 \bmod p$$

where $f'(x)$ is the formal derivative of $f(x)$. Then, $\exists! \alpha \in \mathbb{Z}_p$, such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_1 \bmod p$.

Remark The condition $f(\alpha_1) \equiv 0$ but $f'(\alpha_1) \not\equiv 0$ means that α_1 is a simple root.
This theorem predicts that there is a unique root α within a certain distance of an approximate root α_1.
Proof: □
In fact, the Hensel's lemma could be applied under a looser condition. In the next theorem, we introduce a general version of Hensel's lemma. The generality comes from the fact that it allows the multiple roots, i.e. roots $\alpha_1 \in \mathbb{Z}_p$ such that $f(\alpha_1) \equiv 0$ and $f'(\alpha_1) \equiv 0$. This is implied in the condition $|f(\alpha_1)|_p < |f'(\alpha_1)|_p^2$. Why?
Since $f'(\alpha_1) \in \mathbb{Z}_p$, we have $|f'(\alpha_1)|_p \leq 1$.

When $|f'(\alpha_1)|_p = 1$, $|f(\alpha_1)|_p < 1$. So, we get the condition in theorem 2.2:

$$|f(\alpha_1)|_p < 1 \Leftrightarrow f(\alpha_1) \equiv 0 \bmod p \qquad |f'(\alpha_1)|_p = 1 \Leftrightarrow f'(\alpha_1) \not\equiv 0 \bmod p$$

When $|f'(\alpha_1)|_p < 1$, $|f(\alpha_1)|_p < 1$. We obtain:

$$|f(\alpha_1)|_p < 1 \Leftrightarrow f(\alpha_1) \equiv 0 \bmod p \qquad |f'(\alpha_1)|_p < 1 \Leftrightarrow f'(\alpha_1) \equiv 0 \bmod p$$

which is not contained in the condition of theorem 2.2 and is equivalent to saying α_1 is not a simple root.

Theorem 2.3: A strong version of Hensel's lemma: For multiple roots

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}_p[x]$. If $\exists$ a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ with

$$|f(\alpha_1)|_p < |f'(\alpha_1)|_p^2$$

where $f'(x)$ is the formal derivative of $f(x)$. Then, $\exists! \alpha \in \mathbb{Z}_p$, such that $f(\alpha) = 0$ and $|\alpha - \alpha_1|_p < |f'(\alpha_1)|_p$. Moreover,
(1) $|\alpha - \alpha_1|_p = \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p < |f'(\alpha_1)|_p$
(2) $|f'(\alpha)|_p = |f'(\alpha_1)|_p$

Remark The reason why the inequality is less than $|f'(\alpha_1)|_p^2$ instead of being linear is from the proof 1: it ensures that the ???

Proof: (**Proof 1: Newton's method**)
Let $\{\alpha_n\}$ be the sequence recursively defined by Newton's method: $\alpha_{n+1} := \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$. Claim: This sequence is a Cauchy sequence with the limit α. Let $c = \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p$. Since $f'(\alpha_1) \in \mathbb{Z}_p$, $|f'(\alpha_1)|_p \leq 1$ and $c < |f'(\alpha_1)|_p \leq 1$.
To do this, there are three properties that $\{\alpha_n\}_n$ has: $\forall n$,
(i) $|\alpha_n|_p \leq 1$
(ii) $|f'(\alpha_n)|_p = |f'(\alpha_1)|_p$
(iii) $|f(\alpha_n)|_p \leq |f'(\alpha_1)|_p^2 c^{2^n}$
Base case: These three are obviously applicable to $n = 1$.
Suppose this is true for all n, then consider $n + 1$:
(i°) Since $|\alpha_{n+1}|_p = |\alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}|_p \leq \max\left\{|\alpha_n|_p, \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p\right\}$. It suffices to show $\left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p \leq 1$. Notice that

$$\left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p \overset{\text{(ii)}}{=} \left|\frac{f(\alpha_n)}{f'(\alpha_1)}\right|_p \overset{\text{(iii)}}{\leq} |f'(\alpha_1)|_p c^{2^n} < 1$$

(ii°) We need the lemma:

Lemma 2.1 (Lipschitz property in $\mathbb{Z}_p$) *Let $F(x) \in \mathbb{Z}_p[x]$. Then, $\forall \alpha, \beta \in Z_p$, $|F(\alpha) - F(\beta)|_p < |\alpha - \beta|_p$.*

Let $F(x) = \sum_{i=0}^{n} a_i x^i$ $F(x) - F(y) = \sum_{i=1}^{n} a_i(x^i - y^i) = (x-y)G(x,y)$ with $G(x,y) \in \mathbb{Z}_p[x,y]$. Since $G(\alpha,\beta) \in \mathbb{Z}_p$, $|G(\alpha,\beta)|_p \leq 1$. Then,

$$|F(x) - F(y)|_p = |x-y|_p |G(x,y)|_p \leq |x-y|_p$$

Let $F := f'$, then

$$|f'(\alpha_{n+1}) - f'(\alpha_n)|_p \leq |\alpha_{n+1} - \alpha_n|_p = \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p = \left|\frac{f(\alpha_n)}{f'(\alpha_1)}\right|_p \overset{\text{(iii)}}{<} |f'(\alpha_1)|_p = |f'(\alpha_n)|_p \tag{1}$$

By the strong triangle inequality in $\mathbb{Z}_p$, 1 implies $|f'(\alpha_{n+1})|_p = |f'(\alpha_n)|_p$. So, $|f'(\alpha_{n+1}|_p = |f'(\alpha_1)|_p$.
(iii°) Use the expansion, we have

$$f(\alpha_{n+1}) = f\left(\alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}\right) \overset{\dagger}{=} f(\alpha_n) + f'(\alpha)\left(-\frac{f(\alpha_n)}{f'(\alpha_n)}\right) + z\left(\frac{f(\alpha_n)}{f'(\alpha_n)}\right)^2 = z\left(\frac{f(\alpha_n)}{f'(\alpha_n)}\right)^2$$

where $z \in \mathbb{Z}_p$. So, $|f(\alpha_{n+1})|_p \leq \left|\dfrac{f(\alpha_n)}{f'(\alpha_n)}\right|_p^2 \overset{\text{(ii)}}{=} \left|\dfrac{f(\alpha_n)}{f'(\alpha_1)}\right|_p^2 \overset{\text{hypothesis}}{\leq} \dfrac{(|f'(\alpha_1)|_p^2 c^{2^n})^2}{|f'(\alpha_1)|_p^2} = |f'(\alpha_1)|_p^2 c^{2^{n+1}}$

Existence: Now, use this sequence $\{\alpha_n\}$. We are going to show that this sequence admits a limit having the listed properties:

$\{\alpha_n\}$ is a Cauchy sequence. Since $|\alpha_{n+1} - \alpha_n|_p = \left|\frac{f(\alpha_n)}{f'(\alpha_n)}\right|_p \leq |f'(\alpha_1)|_p c^{2^n}$ and $c < 1$.

The existence of α comes from two parts: • The completeness of $\mathbb{Q}_p$. • Take the limit of (i), we have $|\alpha|_p \leq 1$, i.e. $\alpha \in \mathbb{Z}_p$

Take the limit of (ii) and (iii), (ii) implies (2): $|f'(\alpha)|_p = |f'(\alpha_1)|_p$. (iii) implies that $|f(\alpha)|_p = 0 \Leftrightarrow f(\alpha) = 0$

For $|\alpha - \alpha_1|_p = \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p$, we use the induction and take it to the limit case. The base case $n = 1$ is immediate. Suppose this works for every n, then for $n+1$, $|\alpha_{n+1} - \alpha_1|_p = \max\{|\alpha_{n+1} - \alpha_n|_p, |\alpha_n - \alpha|_p \overset{\text{hypothesis}}{=} \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p\}$. Also, from above-mentioned argument, $|\alpha_{n+1} - \alpha_n|_p < \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p$. So, $|\alpha_{n+1} - \alpha_1|_p = \left|\frac{f(\alpha_1)}{f'(\alpha_1)}\right|_p$. Take the limit, we get (1).

Uniqueness: We have already shown the existence of such an α satisfying all properties listed. It remains to do the uniqueness part. Suppose there is another root $\beta \in \mathbb{Z}_p$ satisfies all the properties, i.e. $f(\beta) = 0$, $|\beta - \alpha_1|_p < |f'(\alpha_1)|_p$ and $|f'(\beta)|_p = |f'(\alpha_1)|_p$. Then, write $\beta = \alpha + h$ with $h \in \mathbb{Z}_p$. If $h = 0$, done. If $h \neq 0$, then $|h|_p = |\beta - \alpha|_p = \max\{|\beta - \alpha_1|_p, |\alpha - \alpha_1|_p\} < |f'(\alpha_1)|_p$ since both of them by assumption $< |f'(\alpha_1)|_p$.

In the meanwhile, $0 = f(\beta) = f(\alpha + h) = f(\alpha) + f'(\alpha)h + zh^2 = f'(\alpha)h + zh^2$ with $z \in \mathbb{Z}_p$. Since $h \neq 0$, $f'(\alpha) = -zh$. Then, $|f'(\alpha)|_p = |zh|_p \leq |h|_p$, contradiction. So, it is impossible that $h \neq 0$.

(**Proof 2: Contraction mapping**) □

Let $f(x), g(x)$ be two polynomials. $f(x)$ and $g(x)$ are coprime $\bmod p$ is more strict than being coprime in $\mathbb{Z}_p$. Why?

First we can consider this example (Exercise 125 in [Gou20]). The two polynomials $x+1$ and $x+p+1$. They have roots -1 and $-p-1$, respectively. $-1 \neq -p-1$ in $\mathbb{Z}_p$ ($|-1|_p = 1 \neq |-p-1|_p = \frac{1}{p}$). So, they are not coprime in $\mathbb{Z}_p$. But, $-1 \equiv -p-1 \bmod p$. So, they are coprime $\bmod p$. Conversely, being coprime $\bmod p$ implies that being coprime in $\mathbb{Z}_p$.

2.3.1 Roots of unity in $\mathbb{Q}_p$(Application of Hensel's lemma)

Now, we use the notation $\boldsymbol{\mu}_n$ to denote the set of n-th root of unity and $\boldsymbol{\mu}_n^{\text{prim}}$ denotes the set of primitive n-th root of unity.

The first fact is: Every root of unity in $\mathbb{Q}_p$ is a p-adic integer for every p. $\forall n$, let $\zeta \in \boldsymbol{\mu}_n \cap \mathbb{Q}_p$. Then,

$$|\zeta|_p^n = |\zeta^n|_p = 1 \Rightarrow |\zeta|_p = 1 \Leftrightarrow \zeta \in \mathbb{Z}_p$$

This means $\forall p, (\bigcup_n \boldsymbol{\mu}_n) \cap \mathbb{Q}_p \subseteq \mathbb{Z}_p$.

It is incorrect that for all n, every n-th root of unity is a p-adic integer. That's because $|\cdot|_p$ is only defined for $\mathbb{Q}_p$, but some n-th roots of unity are not in $\mathbb{Q}_p$. So, for such a ζ, $|\zeta|_p$ is not well-defined. Hence, we cannot have $|\zeta|_p^n = |\zeta^n|_p$.

The assumption starts from the existence of 'roots of unity in $\mathbb{Q}_p$'. Naturally, let's pay attention to the question: When does an n-th root of unity lie in $\mathbb{Q}_p$? Knowing this question implies the knowledge of which n-th roots of unity are in $\mathbb{Z}_p$.

Theorem 2.4: n-th root of unity in $\mathbb{Q}_p$

Let p be a prime. When p is odd, $\mathbb{Q}_p$ contains only $p-1$-th roots of unity.
When $p = 2$, $\mathbb{Q}_p$ contains

2.3.2 Application: Judging whether a number is square

2.4 Local-Global properties

Lemma 2.1: Local Gauss's lemma: General version

Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with a non-trivial factorization in $\mathbb{Q}_p[x]$:

$$f(x) = g(x)h(x), \quad g(x), h(x) \in \mathbb{Q}_p[x]$$

$(g(x), h(x)$ are non-constant). Then, $\exists$ non-constant polynomial $g_0(x), h_0(x) \in \mathbb{Z}_p[x]$ such that $f(x) = g_0(x)h_0(x)$.

Proof: (1) Preliminary: Let $k(x) = \sum_{0 \le i \le n} a_i x^i \in \mathbb{Q}_p[x]$ be any polynomial. Define

$$w(k(x)) := \min_i v_p(a_i)$$

i.e. $w(k(x))$ is the largest power of p that divides all coefficients a_i.
For $k \in \mathbb{Z}_p$, $w(kf(x)) = v_p(k) + w(f(x))$.
Since $f(x) \in \mathbb{Z}_p[x]$, $w(f(x)) \ge 0$. We are going to divide this into two cases: $w(f(x)) > 0$ and $w(f(x)) = 0$. Then, notice that the > 0 case can be converted into the $= 0$ case.
For $w(f(x)) = 0$, assume that $f(x)$ has a factorization in $\mathbb{Q}_p[x]$: $f(x) = g(x)h(x)$. Then, take $a \in \mathbb{Z}_p$ such that $ag(x) \in \mathbb{Z}_p[x]$ and $bh(x) \in \mathbb{Z}_p[x]$. The existence of a and b comes from !! . Set $f_1(x) := abf(x)$, $g_1(x) := ag(x)$ and $h_1(x) := bh(x)$. Then, $f_1(x) = g_1(x)h_1(x)$.

$$0 = w(f_1(x)) = w(abf(x)) = v_p(ab) + w(f(x)) = v_p(ab) \Rightarrow ab \in \mathbb{Z}_p^\times$$

ab is a unit in $\mathbb{Z}_p$ implies that $(ab)^{-1} \in \mathbb{Z}_p$. Consider $g_0(x) := (ab)^{-1}g_1(x) \in \mathbb{Z}_p[x]$ and $h_0(x) := h_1(x)$. Then, $f(x) = g_0(x)h_0(x)$.
Swipe up to the $w(f(x)) > 0$ case. Claim: If the $w(f(x)) = 0$ case is true for every $f(x) \in \mathbb{Z}_p[x]$, then the factorization for $w(f(x)) > 0$ is true.
Let c be a coefficient of $f(x)$ with smallest valuation. By assumption $f(x) \in \mathbb{Z}_p[x]$, $c \in \mathbb{Z}_p$. Set $\tilde{f}(x) := c^{-1}f(x)$. The valuation of $\tilde{f}(x)$ is

$$w(\tilde{f}(x)) = -v_p(c) + w(f(x)) = -v_p(x) + \min_i v_p(f(x)) = -v_p(x) + v_p(x) = 0$$

Since for each a_i, $v_p(c^{-1}a_i) = v_p(a_i) - v_p(c) \ge 0$, $\tilde{f}(x) \in \mathbb{Z}_p[x]$. By assumption, $f(x)$ has a factorization $f(x) = g(x)h(x)$. So, $\tilde{f}(x) = \tilde{g}(x)h(x)$ with $\tilde{g}(x) := c^{-1}g(x)$ in $\mathbb{Q}_p[x]$. The assumption in the claim tells that $\tilde{f}(x)$ boils down to a factorization in $\mathbb{Z}_p[x]$: $\tilde{f}(x) = \widetilde{g_0}(x)\widetilde{h_0}(x)$. Set $g_0(x) := c\widetilde{g_0}(x)$ and $h_0(x) := \widetilde{h_0}(x)$. We have $f(x) = g_0(x)h_0(x)$, as desired. $\square$
(2) Since $\mathbb{Z}_p$ is a UFD and $\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p)$, then from the (general) Gauss's lemma. This is true. $\square$

Proposition 2.1: Local Gauss's Lemma: Monic version

[Local Gauss's lemma $\Rightarrow$ Global Gauss's lemma]

Proposition 2.2: Eisenstein's theorem for $\mathbb{Q}_p$

2.5 Field extensions of $\mathbb{Q}_p$

2.5.1 Finite field extensions of $\mathbb{Q}_p$

2.5.2 Algebraic closure $\overline{\mathbb{Q}_p}$

Corollary 2.2: Absolute value on $\mathbb{Q}_p$

$\overline{\mathbb{Q}_p}$ has a unique absolute value $|\cdot|_p'$ extending the absolute value $|\cdot|_p$ on $\mathbb{Q}_p$. In particular, $\forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and $\forall \alpha \in \overline{\mathbb{Q}_p}$, $|\sigma(\alpha)|_p' = |\alpha|_p'$

Proof: Since $\overline{\mathbb{Q}_p}/\mathbb{Q}_p$ is an algebraic extension, so the theorem ?? Define an absolute value on $\overline{\mathbb{Q}_p}$ by

$$|\cdot|_p^\sigma : \overline{\mathbb{Q}_p} \to \mathbb{Q} \quad \alpha \mapsto |\sigma(\alpha)|_p'$$

$|\cdot|_p^\sigma$ is an non-Archimedean absolute value since: $\forall x, y \in \overline{\mathbb{Q}_p}$

(1) $|x|_p^\sigma = |\sigma(x)|_p' \geq 0$,
(2) $|xy|_p^\sigma = |\sigma(xy)|_p' = |\sigma(x)|_p'|\sigma(y)|_p' = |x|_p^\sigma|y|_p^\sigma$
(3) $|x+y|_p^\sigma = |\sigma(x)+\sigma(y)|_p' \leq |x|_p^\sigma + |y|_p^\sigma$
(4) $|x+y|_p^\sigma = |\sigma(x)+\sigma(y)|_p' \leq \max\{|x|_p^\sigma, |y|_p^\sigma\}$

By uniqueness of absolute value on $\overline{\mathbb{Q}_p}$, $|\alpha|_p^\sigma = |\alpha|_p' \Rightarrow |\sigma(\alpha)|_p' = |\alpha|_p'$. Uniqueness? □ Here is another divergence between p-adic completion and ∞ completion. The algebraic closure of $\mathbb{R}$, $\mathbb{C}$ is complete. While the algebraic closure of $\mathbb{Q}_p$, $\overline{\mathbb{Q}_p}$ is not complete.

Theorem 2.5: Incompleteness of $\mathbb{Q}_p$

$\overline{\mathbb{Q}_p}$ is not complete.

Proof: □ For a field with absolute value, its algebraically closure might not be complete. So, it can be completed with respect to that

Lemma 2.2: L

t $(K, |\cdot|)$ be an algebraically closed field with a non-Archimedean absolute value. If K' is the completion of K with respect to $|\cdot|$, then K' is algebraically closed.

2.5.3 Classifying all extensions of $\mathbb{Q}_p$

3 Elementary analysis in $\mathbb{Q}_p$

3.1 Sequences and Series

3.2 Differentiation

3.3 Integration

3.4 Functions defined by power series

3.5 Strassman's theorem

3.6 Logarithm and exponential functions

References

[Gou20] Fernando Q. Gouvêa. "Exploring $$\mathbb{Q}_p$$". In: *p-adic Numbers: An Introduction*. Cham: Springer International Publishing, 2020, pp. 73–108. ISBN: 978-3-030-47295-5. DOI: 10.1007/978-3-030-47295-5_4. URL: https://doi.org/10.1007/978-3-030-47295-5_4.