Some facts about p-adic numbers

Seewoo Lee

February 15, 2022

Abstract

In this note, we introduce some simple and nontrivial facts about p-adic numbers. Most of the results here can be generalized to any complete DVRs or Henselian fields. You may need to know some basic notion of local fields such as unramified and totally ramified extensions, Newton polygon, Hensel's lemma, etc. See [7] for such definitions.

1 The only automorphism is the identity.

Theorem 1. *Let $f : \mathbb{Q}_p \to \mathbb{Q}_p$ be a field automorphism. The $f = \mathrm{id}$.*

Proof. This proof is adapted from Jyrki Lahtonen's answer on MSE [4]. Note that this is true for $p = \infty$, where $\mathbb{Q}_p = \mathbb{R}$. We will prove that case first, which gives an intuition for the proof of non-archimedean case. Assume that $\varphi : \mathbb{R} \to \mathbb{R}$ is a field automorphism. So $\varphi|_{\mathbb{Q}} = \mathrm{id}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, it is enough to show that φ is continuous. For any $a \in \mathbb{R}$, we have $\varphi(a^2) = \varphi(a)^2 \geq 0$. This implies that $\varphi(\mathbb{R}_{\geq 0}) \subseteq \mathbb{R}_{\geq 0}$. Now if $a \leq b$, we have

$$\varphi(b) - \varphi(a) = \varphi(b-a) = \varphi((b-a)^{1/2})^2 \geq 0$$

so $\varphi(a) \leq \varphi(b)$, i.e. φ is an increasing function. Now, let $a \in \mathbb{R}$ be given. Choose sequences of rational numbers $\{r_n\}$ and $\{s_n\}$ such that $r_n \leq a \leq s_n$ and r_n (resp. s_n) increases (resp. decreases), and both converges to a. Then

$$r_n = \varphi(r_n) \leq \varphi(a) \leq \varphi(s_n) = s_n,$$

and taking the limit $n \to \infty$ gives $\varphi(a) = a$.

For non-archimedean case, we will also use square as we did for $\mathbb{R}$. First, assume $p > 2$ and let $\varphi : \mathbb{Q}_p \to \mathbb{Q}_p$ be a field automorphism. Assume that we proved φ fixes $\mathbb{Z}_p$, i.e. $\varphi(\mathbb{Z}_p) = \mathbb{Z}_p$. Then $\varphi^{-1}(p^k\mathbb{Z}_p) = p^k\mathbb{Z}_p$ for any $k \geq 0$, which implies that φ is continuous (since $p^k\mathbb{Z}_p$ form a basis of the topology at 0), and so $\varphi|_{\mathbb{Z}_p} = \mathrm{id}$ from the fact that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

To prove that $\varphi(\mathbb{Z}_p) = \mathbb{Z}_p$, we will use the following lemma.

Lemma 1. *Let $x \in \mathbb{Q}_p$. $1 + px^2$ is square in $\mathbb{Q}_p$ if and only if $x \in \mathbb{Z}_p$.*

Proof. If $x \notin \mathbb{Z}_p$, then $x = p^{-m}u$ for some $u \in \mathbb{Z}_p^\times$ and $m \geq 1$, so that $v(1 + px^2) = v(1 + p^{-2m+1}u^2) = -2m + 1$, which is odd. If $x \in \mathbb{Z}_p$, then we can use Hansel's lemma: the polynomial $f(t) = t^2 - (1 + px^2)$ splits mod p, so it has a solution in $\mathbb{Q}_p$ (which is also in $\mathbb{Z}_p$ by considering the valuation). Here we need $p > 2$ to apply Hansel's lemma. □

By the lemma, we have

$$x \in \mathbb{Z}_p \Leftrightarrow 1 + px^2 = y^2 \Leftrightarrow 1 + p\varphi(x)^2 = \varphi(y)^2 \Leftrightarrow \varphi(x) \in \mathbb{Z}_p$$

so $\varphi(\mathbb{Z}_p) = \mathbb{Z}_p$.

For $p = 2$, we need a slight modification. We can use the following variation.

Lemma 2. *Let $x \in \mathbb{Q}_2$. $1 + 8x^2$ is square in $\mathbb{Q}_2$ if and only if $x \in \mathbb{Z}_2$.*

Proof. Assume that $x \notin \mathbb{Z}_2$, so that $x = 2^{-m}u$ with $m \geq 1$ and $u \in \mathbb{Z}_2^\times$. If $m = 1$, then $2x \equiv 1 \pmod 2$ and $1 + 8x^2 \equiv 3 \pmod 4$, which can't be a square mod 4. If $m \geq 2$, then $v(1 + 8x^2) = v(1 + 2^{-2m+3}u^2) = -2m + 3$ is odd, so is not square again. If $x \in \mathbb{Z}_2$, let $f(t) = t^2 - (1 + 8x^2)$ and let $a = 1$. Since $f(a) = -8x^2$ and $f'(a) = 2$, $|f(a)|_2 < |f'(a)|_2^2$, Hensel's lemma shows that there exists $b \in \mathbb{Q}_2$ such that $f(b) = b^2 - (1+8x^2) = 0$ and $|b - a|_2 < |f'(a)|_2 = \frac{1}{2}$. □

As before, this shows $\varphi(\mathbb{Z}_2) = \mathbb{Z}_2$ and continuity of φ. □

2 They are different for distinct p's.

Theorem 2. *$\mathbb{Q}_p \simeq \mathbb{Q}_q$ if and only if $p = q$.*

Proof. Again, such isomorphism should fix $\mathbb{Q}$. We will show that there exists $a \in \mathbb{Z}$ such that $\sqrt{a}$ exists in $\mathbb{Q}_q$ but not in $\mathbb{Q}_p$, which gives a contradiction. This follows from the following lemma:

Lemma 3. *There exists $m \in \mathbb{Z}$ such that $p \nmid m$ and $\left(\frac{mp}{q}\right) = 1$.*

Proof. Assume that $q > 2$. If $\left(\frac{p}{q}\right) = 1$, then we can choose $m = 1$. If $\left(\frac{p}{q}\right) = -1$, choose $m' \in \mathbb{Z}$ with $\left(\frac{m'}{q}\right) = -1$ (such m' exists since $q > 2$). Then at least one of m' and $m' + q$ is not a multiple of p. Let m be such one. Then

$$\left(\frac{mp}{q}\right) = \left(\frac{m}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{m'}{q}\right)\left(\frac{p}{q}\right) = (-1)(-1) = 1.$$

□

Now consider $f(x) = x^2 - mp$. This doesn't have a solution in $\mathbb{Q}_p$: if $\alpha \in \mathbb{Q}_p$ satisfies $\alpha^2 = mp$, then $v(\alpha) = \frac{1}{2}v(mp) = \frac{1}{2}$, which is not an integer. However, the equation has a solution in $\mathbb{Q}_q$ by Hensel's lemma.

As before, this is also true when $q = \infty$, so that $\mathbb{Q}_q = \mathbb{R}$. If $p > 3$, then $\mathbb{Q}_p$ has $(p-1)$-many distinct solution of $x^{p-1} - 1 = 0$ (by Hensel's lemma), but $\mathbb{R}$ has only two solutions. For $p = 2$, $\mathbb{Q}_2$ has $\sqrt{-7}$ (by Hensel's lemma), but $\mathbb{R}$ doesn't. For $p = 3$, $\mathbb{Q}_3$ has $\sqrt{-2}$, but $\mathbb{R}$ doesn't. □

3 Correlation between Algebraic and Analytic Properties

As we know, we can define $\mathbb{Q}_p$ in both algebraic and analytic way. For algebraic definition, we define $\mathbb{Z}_p$ as an inverse limit

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

and $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$. For analytic definition, we define $\mathbb{Q}_p$ as a completion of $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$. The following theorems gives some interesting relations between algebraic and analytic properties. Recall that we define

$$|f| := \max_{0\le i\le n}\{|a_i|\}$$

for a polynomial $f(x) = a_nx^n + \cdots + a_1x + a_0 \in K[x]$. If α is a zero of $f(x)$, we have

$$|\alpha| \le \max\left\{1, \sum_{i=0}^{n-1}\left|\frac{a_i}{a_n}\right|\right\}.$$

Indeed, there's nothing to prove for $|\alpha|\le 1$, and if $|\alpha|>1$, we have

$$|\alpha|^n = \left|\frac{a_{n-1}}{a_n}\alpha^{n-1} + \cdots + \frac{a_0}{a_n}\right| \le \max_{0\le i\le n-1}\left\{\left|\frac{a_i}{a_n}\alpha^i\right|\right\} \le |\alpha|^{n-1}\sum_{i=0}^{n-1}\left|\frac{a_i}{a_n}\right|$$

which proves the inequality.

Theorem 3. *In a Henselian field the zeros of a polynomial are continuous functions on its coefficients. More precisely, let $f(x)\in K[x]$ be a polynomial of degree n with n distinct zeros $\alpha_1,\ldots,\alpha_n$. If the polynomial $g(x)$ of degree n has all coefficients sufficiently close to those of $f(x)$, then it has n roots $\beta_1,\ldots,\beta_n$ which approximate the $\alpha_1,\ldots,\alpha_n$ to any given precision.*

Proof. Let $f(x) = a_nx^n + \cdots + a_n = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ and $\epsilon > 0$. Choose $\delta > 0$ so that

$$\delta \le \min\left\{\frac{|a_n|}{2}, \frac{|a_n|\epsilon^n}{\sum_{i=0}^n M^i}, \frac{|a_n|\epsilon^n}{2\sum_{i=0}^n N^i}\right\}$$

where

$$M = \sum_{i=0}^{n-1}\left(1 + 2\frac{|a_i|}{|a_n|}\right), \qquad N = \max\left\{1, \sum_{i=0}^{n-1}\left|\frac{a_i}{a_n}\right|\right\}.$$

Suppose that $g(x)\in K[x]$ satisfies $|f-g|<\delta$, and let β be any root of g. Then $|a_n| \le |a_n - b_n| + |b_n| < \delta + |b_n| \le \frac{\delta}{2} + |b_n|$ gives $\frac{|b_i|}{|b_n|} \le 2\cdot\frac{|a_i-b_i|+|a_i|}{|b_n|} \le \frac{2\delta}{|a_n|} + 2\frac{|a_i|}{|a_n|} \le 1 + 2\frac{|a_i|}{|a_n|}$. So we get $|\beta|\le M$. Thus

$$|f(\beta)| = |f(\beta) - g(\beta)| \le \sum_{i=0}^n |a_i - b_i||\beta|^i < \delta\sum_{i=0}^n M^i < |a_n|\epsilon^n.$$

Therefore $|a_n| \prod_{i=1}^n |\beta - \alpha_i| < |a_n|\epsilon^n \Leftrightarrow \prod_{i=1}^n |\beta - \alpha_i| < \epsilon^n$, hence one of the factors $|\beta - \alpha_i|$ must be smaller than ϵ. This shows that β is within ϵ of a root of f. Conversely, we can prove that for any zero α of $f(x)$, there exists a zero of $g(x)$ very close to α by the same argument (using $|\alpha| \leq N$ and $\frac{|a_n|}{2} \leq |b_n|$). □

Lemma 4 (Krasner)**.** *Let K be an Henselian field, $\alpha \in \overline{K}$ be separable over K and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be its conjugates over K. If $\beta \in \overline{K}$ and*

$$|\alpha - \beta| < |\alpha - \alpha_i|, \qquad i = 2, \ldots, n,$$

then $K(\alpha) \subseteq K(\beta)$.

Proof. Assume that $\alpha \notin K(\beta)$. Then $K(\alpha, \beta)/K(\beta)$ is a field extension of degree > 1, and it is separable since α is separable over K. So we have an field embedding $\sigma : K(\alpha, \beta) \hookrightarrow \overline{K}$ such that $\sigma|_{K(\beta)} = \mathrm{id}$, but $\sigma(\alpha) \neq \alpha$. Then $\sigma(\alpha) = \alpha_i$ for some $2 \leq i \leq n$, and since the valuation is invariant under the field automorphism (by the uniqueness extension property of Henselian field)

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\beta - \alpha_i|.$$

However, this implies

$$|\alpha - \alpha_i| \leq \max\{|\alpha - \beta|, |\beta - \alpha_i|\} = |\beta - \alpha_i|,$$

which contradicts to the assumption. □

The following corollary shows that how analysis can govern algebra in p-adic (or more generally, in Henselian) fields.

Corollary 1. *Let $f(x) \in K[x]$ be an irreducible polynomial over a Henselian field K which is separable, and let $\alpha \in \overline{K}$ be a zero of $f(x)$. Then there exists $\delta > 0$ such that for all $g(x) \in K[x]$ with $|f - g| < \delta$, there exists a zero $\beta \in \overline{K}$ of $g(x)$ such that $K(\alpha) = K(\beta)$. In particular, $g(x)$ is also irreducible.*

Proof. By Theorem 3, there exists $\delta > 0$ such that a polynomial any $g(x) \in K[x]$ with $|f - g| < \delta$ satisfies

$$|\alpha_i - \beta_i| < \min\{|\alpha_i - \beta_j|, |\alpha_j - \beta_i|\}$$

for all $1 \leq i \neq j \leq$, where $\beta_1, \ldots, \beta_n \in \overline{K}$ are zeros of $g(x)$. By Lemma 4, we have $K(\alpha_i) = K(\beta_i)$. □

Using these, we can prove that the algebraic closure of $\mathbb{Q}_p$ is not complete, but its completion is algebraically closed.

Theorem 4. *For any p, the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ is not complete under the p-adic metric extended to $\overline{\mathbb{Q}_p}$. However, its completion $\mathbb{C}_p := \widehat{\overline{\mathbb{Q}_p}}$ is algebraically closed.*

Proof. For the first statement, let's consider the sequence

$$a_n = \sum_{k=1}^{n} p^{n+\frac{1}{n}}$$

in $\overline{\mathbb{Q}_p}$. It is clear that $a_n \in \overline{\mathbb{Q}_p}$, and also the sequence $\{a_n\}_{n\geq 1}$ is a Cauchy sequence since $|s_n - s_{n-1}| = |p^{n+1/n}| \leq p^{-(n+1/n)}$ converges to 0. However, the limit does not exist in $\overline{\mathbb{Q}_p}$. Indeed, let β be any element in $\overline{\mathbb{Q}_p}$ which has degree m over $\mathbb{Q}_p$. If we consider the Newton polygon of the minimal polynomial $f(x)$ of β, valuation of each zeros should be a form of $\frac{a}{b}$ for some $1 \leq b \leq m$. In other words, denominators of the valuations are bounded by $m!$. However, it is not hard to check that $v(a_n) = \frac{a}{b}$ for $b = \text{lcm}\{1, 2, \dots, n\}$, which tends to infinity as n grows. Thus $\lim_{n\to\infty} a_n$ does not exist in $\overline{\mathbb{Q}_p}$.

We will use the above lemmas to prove the second statement. Let α be a zero of some monic polynomial $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{C}_p[x]$. We want to show that $\alpha \in \mathbb{C}_p$. By the Corollary, we can find $g(x) \in \overline{\mathbb{Q}_p}[x]$ such that $|f - g|$ is sufficiently small so $\mathbb{C}_p(\alpha) = \mathbb{C}_p(\beta)$ for some zero $\beta \in \overline{\mathbb{Q}_p}$ of $g(x)$. This proves $\alpha \in \mathbb{C}_p$. □

In fact, the above theorem is true for any field which is complete with respect to some non-trivial non-archimedean absolute value $|\cdot|$. See [1] for the proof.

4 Extensions of $\mathbb{Q}_p$

There are some interesting things happen for extensions of $\mathbb{Q}_p$. First, there are only *finitely many* extensions of $\mathbb{Q}_p$ with a given degree.

Theorem 5. *For any $n \geq 1$, there are only finitely many extensions $K/\mathbb{Q}_p$ with $[K : \mathbb{Q}_p] = n$. In particular, there exists a unique unramified extension of $\mathbb{Q}_p$ of given degree, which is cyclic.*

Proof. For unramified extension of given degree, it is not hard to show that $K_d = \mathbb{Q}_p(\zeta_{p^d-1})$ is a degree d unramified extension of $\mathbb{Q}_p$. (For example, see [7].) To show the uniqueness of unramified extensions, it is enough to show that there is a 1-1 correspondence between finite unramified extensions of $\mathbb{Q}_p$ and finite extensions of the residue field $\mathbb{F}_p$. In fact, if K_1, K_2 are two unramified extensions of same degree n, then both have a residue field $\mathbb{F}_{p^n}$. The compositum $L = K_1K_2$ is also unramified with a residue field $\mathbb{F}_{p^n}$, so

$$[K_1K_2 : \mathbb{Q}_p] = n = [K_1 : \mathbb{Q}_p]$$

which gives $K_1 = K_2$.

Now, we will show that there are finitely many totally ramified extensions of a given degree. First, we can show that every totally ramified extension is a form of $\mathbb{Q}_p(\alpha)$ for some α which is a zero of an Eisenstein polynomial (polynomial whose Newton polygon has only one segment with a slope $1/n = 1/\deg f$). If

$K = \mathbb{Q}_p(\alpha)$ for some zero α of an Eisenstein polynomial, then $v(\alpha) = 1/n$ by the theory of Newton polygon. So $K/\mathbb{Q}_p$ is totally ramified. Conversely, if $K/\mathbb{Q}_p$ is totally ramified, there exist $\alpha \in K$ such that $v(\alpha) = 1/n$. By the following simple lemma, $1, \alpha, \ldots, \alpha^{n-1}$ are all $\mathbb{Q}_p$-linearly independent:

Lemma 5. *If $b_1 + \cdots + b_m = 0$ for $b_1, \ldots, b_m \in K$, then the minimum of $v(b_i)$ is obtained by at least two i's.*

Proof. If not, we may assume that $v(b_1) < v(b_i)$ for all $2 \leq i \leq m$. Then $v(a_1) = v(-a_1) = v(a_2 + \cdots + a_m) \geq \min\{v(a_2), \ldots, v(a_m)\} > v(a_1)$, a contradiction. □

Note that all $1, \alpha, \ldots, \alpha^{n-1}$ have different valuations. So $\deg(\alpha) \geq n$ and $K = \mathbb{Q}_p(\alpha)$. Now let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Q}_p[x]$ be a minimal polynomial of α. By the lemma again, we should have $v(a_1), \ldots, v(a_{n-1}) \geq 0$ and $v(a_0) = 1$, which means that $f(x)$ is an Eisenstein polynomial.

Now we can prove our claim. For each $(a_0, \ldots, a_{n-1}) \in p\mathbb{Z}_p^\times \times p\mathbb{Z}_p \times \cdots \times p\mathbb{Z}_p$, we have an Eisenstein polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. By Krasner's lemma (Lemma 4), each $(a_0, \ldots, a_{n-1})$ has a neighborhood which defines a same splitting field over $\mathbb{Q}_p$. Since $p\mathbb{Z}_p^\times \times p\mathbb{Z}_p \times \cdots p\mathbb{Z}_p$ is compact, it can covered by finitely many such open subsets, which means that we only need finitely many Eisenstein polynomials to cover all the totally ramified extensions. Combining these two results about unramified and totally ramified extensions, we get the theorem. □

We can even find all the quadratic extensions of $\mathbb{Q}_p$.

Theorem 6. *Let $p > 2$ be an odd prime. Then there are exactly three nonisomorphic quadratic extensions of $\mathbb{Q}_p$,*

$$\mathbb{Q}_p(\sqrt{p}), \mathbb{Q}_p(\sqrt{u}), \mathbb{Q}_p(\sqrt{pu}),$$

where $u \in \mathbb{Z}$ is a non-quadratic residue mod p. Also, there are 7 quadratic extensions of $\mathbb{Q}_2$,

$$\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{\pm 2}), \mathbb{Q}_2(\sqrt{\pm 5}), \mathbb{Q}_2(\sqrt{\pm 10}).$$

Proof. Every quadratic extension has a form of $\mathbb{Q}_p(\sqrt{D})$ for some $D \in \mathbb{Q}_p - \mathbb{Q}_p^2$, and $\mathbb{Q}_p(\sqrt{D}) = \mathbb{Q}_p(\sqrt{D'})$ if and only if $D/D' \in \mathbb{Q}_p^2$. So we can reduce the problem to find representatives of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.

First, let $p > 2$. It is not hard to show that p, u, pu are all not in $\mathbb{Q}_p^2$ and their image in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ are all different. Now let $a \in \mathbb{Q}_p - \mathbb{Q}_p^2$. By multiplying suitable power of p^2, we can assume that $a \in \mathbb{Z}_p$ with $0 \leq v_p(a) \leq 1$. If $v_p(a) = 0$ and $a = a_0 + a_1 p + \cdots$, then $a \in \mathbb{Q}_p^2$ if and only if a_0 is a quadratic residue mod p by Hensel's lemma. When a_0 is not a quadratic residue, then $u^{-1}a \pmod{p}$ is a quadratic residue and so $u^{-1}a \in \mathbb{Q}_p^2$. This means that $\sqrt{a} \in \mathbb{Q}_p(\sqrt{u})$. Similarly, we can prove that $a \in \mathbb{Q}_p(\sqrt{p})$ or $\mathbb{Q}_p(\sqrt{pu})$ when $v_p(a) = 1$.

For $p = 2$, a situation is more technical. First, we can show that they are all degree 2 extensions. If -1 is square in $\mathbb{Q}_2$, then it is also square in $\mathbb{Z}_2$ since it has valuation 0, and this is impossible since there's no solution of $x^2 + 1 = 0$ mod 4. Similarly, 5 and -5 are not squares because of mod 4 or 8. ± 2 and ± 10 are not squares since their valuations are 1, which is odd.

To show that they are all, it is enough to show that all $D \in \mathbb{Z}$ with $D \equiv 1 \pmod 8$ are square in $\mathbb{Z}_2$. This follows from (strong) Hensel's lemma - if we put $f(x) = x^2 - D$, then $|f(1)|_2 \le 2^{-3} < 2^{-2} = |f'(1)|_2^2$, so there exists $a \in \mathbb{Z}_2$ such that $f(a) = a^2 - D = 0$ (with $|a-1|_2 < |f'(1)|_2 = 2^{-2}$. Then we can proceed as we did above. □

This theorem tells us that extensions of $\mathbb{Q}_p$ are much simpler than extensions of global fields, such as $\mathbb{Q}$. How about Galois groups? As we know, Abel proved that there's no general formula to solve quintic equation. More precisely, there exists a degree 5 polynomial over $\mathbb{Q}$ whose roots can't be represented as radicals. However, for $\mathbb{Q}_p$, we can prove that *every* finite Galois extension of $\mathbb{Q}_p$ are solvable. Before we prove it, we define higher ramification groups, which give a filtration of normal subgroups of the Galois group.

Definition 1. *Let $K/\mathbb{Q}_p$ be a finite Galois extension and let $G = \mathrm{Gal}(K/\mathbb{Q}_p)$ be a Galois group. . Let v_K be a normalized valuation on K which extends the p-adic valuation on $\mathbb{Q}_p$. For each $s \ge -1$, we define the higher ramification groups as*

$$G_s = G_s(K/\mathbb{Q}_p) := \{\sigma \in G : v_K(\sigma(a) - a) \ge s + 1 \,\forall a \in \mathcal{O}_K\}$$

It is easy to check that

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{s_0} = \{1\}$$

is a filtration of G which are all normal subgroups and $G_s = \{1\}$ for sufficiently large s.

Proposition 1. *Let π_K be a uniformizer of K. For any $s \ge 0$, we have a well-defined homomorphism*

$$G_s/G_{s+1} \to U_K^{(s)}/U_K^{(s+1)}, \qquad \sigma \mapsto \frac{\sigma(\pi_K)}{\pi_K}$$

is an injective homomorphism which is independent of the choice of π_K. Here $U_K^{(0)} = \mathcal{O}_K^\times$ and $U_K^{(s)} = 1 + \pi_K^s \mathcal{O}_K$ for $s \ge 1$.

Proof. The most tricky part is injectivity. We will only prove injectivity for $s = 0$, and $s \ge 1$ case is similar. (You can find the proof for $s \ge 1$ in [2].) Assume that $\sigma \in G_s$ is in the kernel of the map, so that $\sigma(\pi_K) \equiv \pi_K \pmod{\pi_K^{s+1}}$. Let K' be a maximal unramified subextension of K. Then the residue field k' is same as k because $k/\mathbb{F}_p$ is separable. This means that we have a surjective map $\mathcal{O}_{K'} \twoheadrightarrow k$, so that any $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv c_0 + c_1\pi_K \pmod{\pi_K^2}$ for some $c_0, c_1 \in \mathcal{O}_{K'}$. Then

$$\sigma(\alpha) \equiv \sigma(c_0) + \sigma(c_1)\sigma(\pi_K) \equiv c_0 + c_1\pi_K \equiv \alpha \pmod{\pi_K^2}$$

since $K' = K^{G_0}$. This proves $\sigma \in G_1$. □

Corollary 2. *Any finite Galois extension of $\mathbb{Q}_p$ are solvable.*

Proof. The quotient $U_K^{(s)}/U_K^{(s+1)}$ is clearly an abelian group for any $s \geq 0$. In fact, it is not hard to show that

$$U_K^{(s)}/U_K^{(s+1)} \simeq \begin{cases} k^\times & s = 0 \\ k & s \geq 1 \end{cases}$$

where k is the residue field of K. By the previous proposition, every quotient G_s/G_{s+1} is abelian, and the above filtration proves that G is a solvable group. □

In general, it is hard to find generators of a ring of integer of a number field. It is known that there are some number fields which has a ring of integer that is not monogenic, i.e. not of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. For example, Dedekind found that a cubic field $K/\mathbb{Q}$ generated by a root of the polynomial $x^3 - x^2 - 2x - 8$ is not monogenic. Also, $\mathbb{Q}(\sqrt{7}, \sqrt{10})$ is another example - see Chapter 2, Exercise 30 of [5]. However, for local fields, we can show that every ring of integers are monogenic.

Theorem 7. *Every ring of integer of finite extension K of $\mathbb{Q}_p$ is monogenic, i.e. $\mathcal{O}_K = \mathbb{Z}_p[\alpha]$ for some $\alpha \in \mathcal{O}_K$.*

Proof. Let k be a residue field of K, which is a finite extension of $\mathbb{F}_p$. Then there exists $\alpha \in \mathbb{F}_p$ s.t. $k = \mathbb{F}_p(\bar{\alpha})$. Now let $\bar{f}(x) \in \mathbb{F}_p[x]$ be a minimal polynomial of $\bar{\alpha}$ and let $f(x) = \mathcal{O}_K[x]$ be a lift.

Lemma 6. *There exists a lift $\alpha \in \mathcal{O}_K$ of $\bar{\alpha}$ such that $\pi = f(\alpha)$ is a uniformizer of K.*

Proof. Let v_K be a normalized valuation on K. From $\bar{f}(\bar{\alpha}) = 0$, we have $v_K(f(\alpha)) \geq 0$ for any lift α. If $v_K(\alpha) = 1$, then we are done. So let's assume $v_K(\alpha) \geq 2$. Then $\alpha + \pi_K$ will work: indeed, by Taylor's formula we have

$$f(\alpha + \pi_K) = f(\alpha) + f'(\alpha)\pi_K + b\pi_K^2, \quad b \in \mathcal{O}_K$$

and we get $v_L(f(\alpha + \pi_K)) = 1$ since $f'(\alpha) \in \mathcal{O}_K^\times$, because $\bar{f}'(\bar{\alpha}) \neq 0$. □

From this, one can prove that

$$\alpha^j \pi^i, \quad 0 \leq i \leq e - 1, 0 \leq j \leq f - 1$$

form an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}_p$. Hence $\mathcal{O}_K = \mathbb{Z}_p[\alpha]$. □

5 Monsky's theorem

At last, we introduce some amazing application of p-adic numbers, which seems to be nothing to do with p-adic numbers.

Theorem 8 (Monsky)**.** *If we dissect a square into n triangles with all the same areas, then n is even.*

Proof. This proof requires Axiom of Choice. By using Zorn's lemma, we can prove that any two different extensions of a same field which are algebraically closed and have the same cardinality are isomorphic as a field. This implies that there is a field isomorphism $i_p : \mathbb{C} \to \mathbb{C}_p$, and we can extend the p-adic valuation to $\mathbb{C}$ by $|x|_p := |i_p(x)|_p$.

Now we can color points on a real plane $\mathbb{R}^2$ equipped with a 2-adic norm via $\mathbb{R} \hookrightarrow \mathbb{C} \xrightarrow{i_2} \mathbb{C}_2$. Color a point (x, y) red if $|x|_2 < 1, |y|_2 < 1$, color it blue if $|x|_2 \leq |y|_2$ and $|y|_2 \geq 1$, and color it green if $|x|_2 > |y|_2$ and $|x|_2 \geq 1$. Then each edge can only contain at most two colors. By Sperner's lemma, we can find a complete triangle where all the vertices have different colors. Let $(x_r, y_r), (x_b, y_b), (x_g, y_g)$ be the coordinates of the complete triangle with red, blue, and green colors. The area A of the triangle is the absolute value of

$$\frac{(x_g - x_r)(y_b - y_r) - (x_b - x_r)(y_g - y_r)}{2}.$$

By definition of the coloring, we have

$$\begin{gathered} |(x_b - x_r)(y_g - y_r)|_2 = |x_b y_g|_2 \geq 1, \\ |x_b|_2 \geq \max\{|y_b|_2, |y_r|_2\}, \\ |y_g|_2 > \max\{|x_g|_2, |x_r|_2\} \end{gathered}$$

and so we have

$$|A| = |1/2||x_b||y_g| \geq 2.$$

By the way, the area is $A = 1/n$, so we get $|n| \leq 1/2$ and n is even. □

References

[1] Brian Conrad, *Completion of Algebraic Closure*, http://virtualmath1.stanford.edu/~conrad/248APage/handouts/algclosurecomp.pdf, Online note.

[2] Brian Conrad, *Higher ramification groups*, http://math.stanford.edu/~conrad/676Page/handouts/ramgroup.pdf, Online note.

[3] Keith Conrad, *Which number fields are monogenic? and related questions*, https://mathoverflow.net/questions/21267/which-number-fields-are-monogenic-and-related-questions, Answer to a question on Mathematics Overflow.

[4] Jyrki Lahtonen, answer to the question *An automorphism of the p-adic numbers*, `https://math.stackexchange.com/questions/449424/an-automorphism-of-the-field-of-p-adic-numbers`, Mathematics StackExchange.

[5] Daniel A. Marcus, *Number fields*, Vol. 8. New York: Springer, 1977.

[6] James Milne, *Algebraic Number Theory*, Online note.

[7] Jürgen Neukirch, Algebraic number theory. Vol. 322. Springer Science & Business Media, 2013.