p-adic Complex Numbers

Christopher Eur

December 2, 2013

1 Introduction

Our usual $\mathbb{C}$ is constructed in the following way: completion of $\mathbb{Q}$ with respect to the usual norm $|\ |$ gives us $\mathbb{R}$, and taking the algebraic closure of $\mathbb{R}$ gives us $\mathbb{C} = \mathbb{R}[i]$, which happens to be complete with respect to the extended norm. The p-adic case is a bit more complicated; we impose a different norm $|\ |_p$ on $\mathbb{Q}$, and by completing $\mathbb{Q}$ with such norm we have $\mathbb{Q}_p$. Unlike $\mathbb{R}$ we need to adjoin infinitely many elements to make $\overline{\mathbb{Q}_p}$, the algebraic closure of $\mathbb{Q}_p$. However, $\overline{\mathbb{Q}_p}$ is not complete, and its completion Ω is algebraically closed and complete.

In this presentation we will discuss upto the algebraic closure of $\mathbb{Q}_p$.

2 p-adic Valuation

Definition 2.1. Let F be a field. A **field norm / absolute value** on F is a map $\|\ \| : F \to \mathbb{R}$ satisfying: (1) $\|x\| = 0 \Leftrightarrow x = 0$, (2) $\|xy\| = \|x\|\|y\|$, and (3) $\|x + y\| \leq \|x\| + \|y\|$.

Lemma 2.2. Let $\|\ \|$ be a **non-Archimedean** norm: i.e. $\|x + y\| \leq \max(\|x\|, \|y\|)$. Then,

1. $\|x\| < \|y\| \Rightarrow \|x + y\| = \|y\|$. (That is, every triangle is isosceles).
2. Let $\{x_i\}$ be a Cauchy sequence. Then the sequence $\|x_i\|$ either converges to 0 or stabilizes to a nonzero value (there exists $N > 0$ such that $\|x_i\| = \|x_{i+1}\|$ for all $i \geq N$).
3. A sequence $\{a_k\}_{k\in\mathbb{N}}$ converges to 0 if and only if the series $\sum_{k=1}^{\infty} a_k$ converges.

Definition 2.3. Fix a prime $p \in \mathbb{N}$. Let $z \in \mathbb{Z}$, define $\mathbf{ord}_p(z) =$ maximum i such that $p^i | z$. We can extend this to $\mathrm{ord_p} : \mathbb{Q}^* \to \mathbb{Z}$ where $\mathrm{ord_p}(\frac{m}{n}) = \mathrm{ord_p}(m) - \mathrm{ord_p}(n)$.

Proposition 2.4. $\mathrm{ord_p} : \mathbb{Q}^* \to \mathbb{Z}$ *is a discrete valuation on* $\mathbb{Q}$.

Definition 2.5. Define $|\ |_p : \mathbb{Q} \to \mathbb{R}$ as follows:

$$|x|_p = \begin{cases} p^{-\mathrm{ord_p}(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

Proposition 2.6. $|\ |_p$ is a field norm on $\mathbb{Q}$ with the non-Archimedean property

3 p-adic Field $\mathbb{Q}_p$

We complete $\mathbb{Q}$ with respect to $|\ |_p$ in the standard way:

Definition 3.1. Define

$$\mathbb{Q}_p = \{(a_i) \in \prod_{i=1}^{\infty} \mathbb{Q} : (a_i) \text{ is Cauchy}\}/\sim$$

where the equivalence relation $\sim$ is given by $(a_i) \sim (a_i') \Leftrightarrow |a_i - a_i'|_p \to 0$. The embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is given by the constant sequence: $q \in \mathbb{Q} \mapsto (q, q, \ldots) \in \mathbb{Q}_p$. Denote $\{0\}$ by 0.

Lemma 3.2. Let $a \in \mathbb{Q}_p$, and Let $\{a_i\}$ represent a. Define $|a|_p := \lim_{i\to\infty} |a_i|_p$. Then $|\ |_p$ is a well-defined map $\mathbb{Q}_p \to \mathbb{R}$.

Proof) The limit always exists by **Lemma 2.2**. If $\{b_i\}$ represents a too, then $\forall i \in \mathbb{N}$, $|b_i|_p \leq \max(|a_i|_p, |b_i - a_i|_p)$, so take i large enough then apply **Lemma 2.2**.

Theorem 3.3. $\mathbb{Q}_p$ is a field which is complete with the norm $|\ |_p$.

Proof) Define $+, \cdot, ^{-1}$ using representatives, use the above **Lemma 3.2** and **Lemma 2.2** to show that $|\ |_p$ is a norm, and completeness follows by diagonalizing.

The following theorem provide a concrete way to think about numbers in $\mathbb{Q}_p$.

Theorem 3.4. Every $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$ has a unique representative $\{a_i\}$ such that $\forall i = 0, 1, 2, \ldots$

1. $0 \leq a_i < p^{i+1}, \quad a_i \in \mathbb{Z}$
2. $a_i \equiv a_{i+1} \pmod{p^{i+1}}$

Proof) Uniqueness: If $\{a_i'\}$ another such representative and $a_k \neq a_k'$ at some k, then $a_k \not\equiv a_k' \pmod{p^{k+1}}$, which implies $a_i \equiv a_k \not\equiv a_k' \equiv a_i' \pmod{p^{k+1}}$ for all $i > k$. So $|a_i - a_i'|_p > p^{-(k+1)}$ for all $i > k$. Contradiction.

Existence: Let $\{b_i\}_{i\in\mathbb{Z}_{\geq 0}}$ be any sequence that represents a. Passing through a subsequence assume $|b_m - b_n|_p \leq p^{i+1}$ whenever $m, n \geq i$. Noting that $\forall i, |b_i|_p \leq 1$, we are done by the following lemma:

Lemma 3.5. If $x \in \mathbb{Q}$ with $|x|_p \leq 1$, then for any $i \in \mathbb{Z}_{\geq 0}$ there exists integer $a_i \in \{0, 1, \ldots, p^{i+1} - 1\}$ such that $|a_i - x| \leq p^{-(i+1)}$.

Proof) Let $x = \frac{a}{b}$ in lowest terms, then $|x|_p \leq 1$ implies that $p \not| b$ and so there exists integers m, n such that $mb + np^{i+1} = 1$. Letting $a_i = am$ we have our desired result.

Remark: Theorem 3.4 implies that the integers a_i's are of the form:

$$a_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_i p^i$$

Hence, for any $a \in \mathbb{Q}_p$ with $|a|_p \leq 1$, we may write a as a p-adic expansion:

$$a = b_0 + b_1 p + b_2 p^2 + \cdots$$

as a short-hand for the sequence of the partial sums. Furthermore, if $|a|_p > 1$, then $|ap^m| \leq 1$ for some $m \in \mathbb{N}$ so, by p-adically expanding ap^m and then dividing by p^m,

$$a = \frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \cdots + b_0 + b_1 p + b_2 p^2 + \cdots$$

In fact, we can take the above shorthand to actually mean equality by **Lemma 2.2.** since the series converges.

Definition 3.6. Define p-adic integers, denoted $\mathbb{Z}_p$, to be $\{a \in \mathbb{Q}_p : |a|_p \leq 1\}$. Equivalently, $\mathbb{Z}_p$ is the set of numbers in $\mathbb{Q}_p$ whose p-adic expansion involves no negative powers of p.

Example 3.7.

1. If $n \in \mathbb{N}$, p-adic expansion of n looks like p-ary expansion written backwards: $11 = 1011_2$ (binary), $11 = 1101_2$ (2-adic).
2. p-adic expansion of $-\frac{1}{p-1}$ is $1111\cdots$
3. We can do addition, subtraction, multiplication, long division just as we do in the decimals, except "carrying," "borrowing," etc. now goes from left to right instead of right to left.
4. $\mathbb{Q}_p$ is not algebraically closed. For example, $\mathbb{Q}_5$ does not have a square root of 7; $|7|_5 = 1$ so $|\sqrt{7}|_5 = 1$, but no $a_0 \in \mathbb{Z}$ satisfies $a_0^2 \equiv 2 \pmod 5$.

4 $\overline{\mathbb{Q}_p}$: Algebraic Closure of $\mathbb{Q}_p$

Before we take the algebraic closure of $\mathbb{Q}_p$, we need discuss whether we can extend the norm on $\mathbb{Q}_p$ to $\overline{\mathbb{Q}_p}$ in the first place. In other words, let $K \supset F$ be a field extension, where F has field norm $\| \ \|_F$; is there a field norm $\| \ \|_K$ on K whose restriction to F is $\| \ \|_F$?

Assume that all extensions $K \supset F$ are finite extensions for this section.

Lemma 4.1. $\mathbb{Z}_p$ is compact in $\mathbb{Q}_p$, and hence, $\mathbb{Q}_p$ is locally compact field.

Proof) We prove sequential compactness since we are in metric space. Let a sequence $\{a_i\}$ in $\mathbb{Z}_p$ be given. Each has a unique p-adic expansion with no negative powers of p. Now, since the first digit is among $0, \ldots, p-1$, we can extract a subsequence $\{b_i\}$ of $\{a_i\}$ all sharing the same first digit. Then extract a subsequence $\{c_i\}$ of $\{b_i\}$ all sharing the same first and second digit. And so on. Diagonalizing, we have our desired sequence that converges in $\mathbb{Z}_p$.

Since $\mathbb{Z}_p$ is compact, its translates $x + \mathbb{Z}_p := \{y : |y - x|_p \leq 1\}$ are compact, and hence, every closed ball of radius 1 is compact. So, $\mathbb{Q}_p$ is locally compact.

Theorem 4.2. If V is a finite dimensional vector space over a locally compact field F, then all norms on V are equivalent. I.e. $\exists c_1, c_2 \in \mathbb{R}$ such that $\forall x \in V, \|x\|_2 \leq c_1\|x\|_1$ and $\|x\|_1 \leq c_2\|x\|_2$.

Corollary 4.3. Let $K \supset F$ be a field extension. Then there is at most one field norm $\| \ \|_K$ of K which extends $\| \ \|_F$ on F.

Combining **Lemma 4.1.** and **Corollary 4.3**, we have that if $K \supset \mathbb{Q}_p$ is a finite extension, the norm $| \ |_p$ extends uniquely to K (if it exists). We now show that norm extension in fact exists for any finite extension of $\mathbb{Q}_p$.

Definition 4.4. Let $K = F(\alpha)$ be a finite extension of a field F where α is a root of the monic irreducible polynomial $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,\ a_i \in F$. Define **norm of α from K to F**, denoted $\mathbb{N}_{K/F}(\alpha)$ in the following three equivalent ways:

1. Consider K as n-dimensional vector space over F, multiplication by α as a F-linear map on K with the matrix A_α. $\mathbb{N}_{K/F}(\alpha) := \det(A_\alpha)$
2. $\mathbb{N}_{K/F}(\alpha) := (-1)^n a_n$
3. $\mathbb{N}_{K/F}(\alpha) := \prod_{i=1}^n \alpha_i$ where α_i's are the n roots of $f(x)$ in $\overline{F}$, $\alpha_1 = \alpha$.

More generally, if $K \supset F$ is a finite extension, $\beta \in K$, then $\mathbb{N}_{K/F}(\beta) := \det(A_\beta) = (\mathbb{N}_{F(\beta)/F}(\beta))^{[K:F(\beta)]}$

Proof) $1 \Leftrightarrow 2$: choose $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ as the basis of K over F. $2 \Leftrightarrow 3$: $f(x) = \prod_{i=1}^n (x - \alpha_i)$.
If $\beta \in K$, $[F(\beta)\colon F] = r, [K\colon F(\beta)] = s$, $(k_1, \ldots, k_s)$ is basis for K over $F(\beta)$, then
$(k_1, k_1\beta, \ldots, k_1\beta^{m-1}, k_2, \ldots, k_2\beta^{m-1}, \ldots, k_s\beta^{m-1})$ is a basis for K over F. So, the matrix A_β of multiplication by β on K consists of $[K : F(\beta)]$ diagonal blocks of A'_β where A'_β is matrix of multiplication by β in $F(\beta)$.

Remark: Using this notion, we can derive what the norm $\| \ \|$ on $K \supset \mathbb{Q}_p$ has to be if it extends the norm $| \ |_p$ on $\mathbb{Q}_p$.

Let K be Galois extension of $\mathbb{Q}_p$ containing α. Let α' be any conjugate of α (satisfies same irreducible polynomial), and let $\sigma \in \mathrm{Gal}(K/F)$ such that $\sigma(\alpha) = \alpha'$. Suppose there exists norm $\| \ \|$ on K that extends $| \ |_p$. Then, $\| \ \|' : K \to \mathbb{R}$ defined by $\|x\|' = \|\sigma(x)\|$ is clearly a norm on K that extends $| \ |_p$ as well. Hence, $\| \ \| = \| \ \|'$, which implies that $\|\alpha\| = \|\alpha'\|$. Hence, the α and its conjugates all have the same norm.

Now, noting that $\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$, we have

$$\begin{aligned} |\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p &= \|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\| \\ &= \| \prod_{\text{conjugates } \alpha' \text{ of } \alpha} \alpha' \| \\ &= \prod \|\alpha'\| \\ &= \|\alpha\|^{[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]} \end{aligned}$$

So we have $\|\alpha\| = |\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|_p^{1/n}$ where $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}]$. In more concrete terms, to find the (extended) p-adic norm of $\alpha \in K \supset \mathbb{Q}_p$, look at the monic irreducible polynomial satisfied by α. If it has degree n and constant term a_n, then p-adic norm of α is nth root of $|a_n|_p$.

Moreover, if K is *any* finite extension of $\mathbb{Q}_p$ containing α, we have

$$\|\alpha\| = \left|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]} = \left|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)\right|_p^{1/[K:\,\mathbb{Q}_p]}$$

since $\mathbb{N}_{K/\mathbb{Q}_p}(\alpha) = (\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha))^{[K:\mathbb{Q}_p(\alpha)]}$ and $[K : \mathbb{Q}_p(\alpha)][\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [K : \mathbb{Q}_p]$.

Theorem 4.5. Let $K \supset \mathbb{Q}_p$ be a finite extension. Then there exists a (unique) field norm on K which extends the norm $|\ |_p$ on $\mathbb{Q}_p$. In fact, the norm is given by:

$$\|\alpha\| = \left|\mathbb{N}_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)\right|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}$$

Proof) (0) $\forall a \in \mathbb{Q}_p$, $\|a\| = |a|_p$ is obvious, and this also implies that (1) $\|\alpha\| = 0 \Leftrightarrow \alpha = 0$. (2) $\|\alpha\beta\| = \|\alpha\|\|\beta\|$ follows from the fact that $\mathbb{N}_{K/\mathbb{Q}_p}(\alpha), \mathbb{N}_{K/\mathbb{Q}_p}(\beta)$ are determinants of $A_\alpha, A_\beta \in \mathrm{Hom}_{\mathbb{Q}_p}(K, K)$, and multiplication commutes with determinants. (3) For $\|\alpha + \beta\| \leq \max(\|\alpha\|, \|\beta\|)$, we prove the following equivalent notion:

Claim: If $\gamma \in K$ with $\|\gamma\| \leq 1$, then $\|1 + \gamma\| \leq 1$.

Since $\mathbb{Q}_p(\gamma) = \mathbb{Q}_p(1 + \gamma)$, the only two values we are concerned with are

$$\|\gamma\| = \left|\mathbb{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(\gamma)\right|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]} \text{ and } \|1 + \gamma\| = \left|\mathbb{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(1 + \gamma)\right|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]}$$

So WLOG assume $K = \mathbb{Q}_p(\gamma)$. Let $n := [K : \mathbb{Q}_p(\gamma)]$ and so $(1, \gamma, \gamma^2, \ldots, \gamma^{n-1})$ is the basis of K over $\mathbb{Q}_p$. For any $n \times n$ matrix $A = \{a_{ij}\}$ with entries in $\mathbb{Q}_p$, define $|A| := \max_{i,j} |a_{ij}|_p$.

Let A_γ be the matrix for multiplication by γ on K (and $I + A_\gamma$ is thus the matrix for multiplication by $1 + \gamma$). Noting that $|\det A|_p \leq (\max_{i,j} |a_{ij}|_p)^n = |A|^n$, for any $N \in \mathbb{N}$, we have:

$$\|1 + \gamma\|^N = |\det(I + A_\gamma)^N|_p^{1/n} \leq |(I + A_\gamma)^N| \leq \max_{0 \leq i \leq N} \left| \binom{N}{i} A_\gamma^i \right| \leq \max_{0 \leq i \leq N} |A_\gamma^i|$$

With respect to the sup-norm, closed unit ball of a vector space over locally compact field is compact, and using this we can prove that sequence $\{|A_\gamma^i|\}_{i \in \mathbb{N}}$ is bounded by some $M > 0$, and hence $\|1 + \gamma\| \leq \sqrt[N]{M}$ for all N, so $\|1 + \gamma\| \leq 1$ as desired.

Remark: Thus, since algebraic closure of $\mathbb{Q}_p$, denoted $\overline{\mathbb{Q}_p}$, is union of such finite extensions, the norm $|\ |_p$ on $\mathbb{Q}_p$ extends (uniquely) to a field norm on $\overline{\mathbb{Q}_p}$, given exactly as the formula given in the theorem above.