Construction of $\mathbb{C}_p$ and Extension of p-adic Valuations to $\mathbb{C}$

Mike Hamburg

May 24, 2004

1 Introduction

Here we will derive the structure of the p-adic complex numbers, that is, an algebraically closed, topologically complete field containing the p-adic numbers.

2 Valuations

We will begin by defining valuations and proving some of their simple properties.

Definition (Valuation). *A valuation on a field F is a function $|\cdot| : F \to \mathbb{R}$ satisfying three conditions:*

1) $|x| = 0$ *if* $x = 0$*; otherwise* $|x| > 0$.

2) $|xy| = |x||y|$ *for all* $x, y \in F$.

3) There is a constant C *such that if* $|x| \leq 1, |x+1| \leq C$.

Two valuations $|\cdot|_1, |\cdot|_2$ *are called equivalent if there is a constant* c *such that* $|x|_1 = |x|_2^c$ *for all* $x \in F$.

Note some basic properties that this implies: $|1| = |-1| = 1$, $|-x| = |x|$ and $|x^{-1}| = |x|^{-1}$.

An example of a valuation is the absolute value on $\mathbb{R}$, with $C = 2$; we will refer to this valuation as $|\cdot|_\infty$. Such valuations, for which we may choose $C = 2$, satisfy the familiar triangle inequality $|a + b| \leq |a| + |b|$, although we will not prove it here. This means that for any valuation, some sufficiently small positive power of it (an equivalent valuation) will satisfy the triangle inequality.

We we will be concerned here primarily with a special sort of valuation:

Definition. *A valuation is called non-Archimedian if we can choose* $C = 1$ *in the above definition.*

Non-Archimedian valuations such as $|\cdot|_p$ are particularly nice because they satisfy a strong triangle inequality, which is also well-known and which we will not prove:

Lemma 1 (The Strong Triangle Inequality). *If* $|\cdot|$ *is a non-Archimedian valuation on a field* F*, then*

$$|a + b| \leq \max(|a|, |b|)$$

with equality whenever $|a| \neq |b|$*, for all* $a, b \in F$.

We have two obvious but very useful corollaries of the Strong Triangle Inequality:

Corollary. *The set $\mathcal{O}_K$, defined as $\{x \in K : |x| \leq 1\}$, is a ring. This set is called the integers of K.*

Corollary. *Partial sums of a series $\sum_{n=0}^{\infty} a_n$ form a Cauchy sequence if and only if $a_n \to 0$ as $n \to \infty$.*

A well-known fact in number theory is that the only non-Archimedian valuations on $\mathbb{Q}$ up to exponentiation are the trivial valuation $|\cdot|_1$ such that $|x|_1 = 1$ for nonzero x, and the p-adic valuation $|\cdot|_p$ defined by $|p^k x|_p = p^{-k}$ where p divides neither the numerator nor the denominator of x. We will be more or less ignoring the trivial valuation in this paper, and concentrating on p-adic valuations on $\mathbb{Q}$ and their extensions to other fields.

A valuation $|\cdot|$ with $\mathbb{C} \leq 2$ defines a metric and therefore a topology on its field K. We will be interested in the topological properties of various extensions of $\mathbb{Q}$, and we will be considering completions $\mathbb{Q}_{|\cdot|}$ of $\mathbb{Q}$ under $|\cdot|$. In the case that $|\cdot| = |\cdot|_p$ is the p-adic valuation, we will write this completion as $\mathbb{Q}_p$. Here is one such topological property that we will need:

Lemma 2. *$\mathbb{Q}_p$ is locally compact, that is, $\mathcal{O}_{\mathbb{Q}_p}$ is compact.*

Proof. We must show that $\mathcal{O}_{\mathbb{Q}_p}$ is complete and totally bounded. As a closed ball $B_1(0)$, it is clearly complete. Furthermore, we can cover $\mathcal{O}_{\mathbb{Q}_p}$ with finitely many balls of radius p^{-n} for any n because these balls are simply equivalence classes of $\mathcal{O}_{\mathbb{Q}_p}/p^n\mathcal{O}_{\mathbb{Q}_p}$, of which there are only p^n. ▽

We need one more lemma before we can extend valuations:

Lemma 3 (Stein 15.2.10). *A valuation $|\cdot|$ is non-Archimedian if and only if $|n| \leq 1$ for all $n \in \mathbb{Z}$.*

Proof. "Only if" is trivial by induction with the definition of non-Archimedian. For the "if" direction, we must choose an equivalent valuation $|\cdot|_1$ which satisfies the triangle inequality; this preserves the condition, and $|\cdot|_1$ is Archimedian if and only if $|\cdot|$ is. Now pick any $a \in K$ with $|a| \leq 1.$, and expand using the Binomial Theorem:

$$\begin{aligned} |1+a|_1^n &= |(1+a)^n|_1 \\ &= |\sum_{k=0}^{n} \binom{n}{k} a^k|_1 \\ &\leq \sum_{k=0}^{n} |\binom{n}{k}|_1 |a^k|_1 \\ &\leq n+1 \end{aligned}$$

Thus $|1+a|_1 \leq \sqrt[n]{n+1}$ for all positive integers n, and so it is at most 1 as desired. ∎

3 Extension of Valuations

We would like to be able to extend valuations, that is, for some finite extension field L over K and valuation $|\cdot| : K \to \mathbb{R}$, we wish to find another valuation $||\cdot|| : L \to \mathbb{R}$ such that $|x| = ||x||$ for $x \in K$. The next lemma shows that this is possible, at least in the cases that we will need.

Lemma 4 (Stein 19.1.2). *Let $L = \mathbb{Q}_p(r)$ be an extension of $\mathbb{Q}_p$ by the root r of some irreducible polynomial P of degree n. Then there exists a non-Archimedian valuation $||\cdot|| : L \to \mathbb{R}$ which extends $|\cdot|$.*

Proof. We will show that $||x|| = |\mathrm{Norm}_{L/\mathbb{Q}_p} x|^{1/n}$ suffices. This is clearly positive-definite and multiplicative, and by lemma 3, it will be non-Archimedian if it is in fact a valuation. So we need only show that there is some C such that for $||x|| \leq 1, ||x+1|| \leq C$. This is obvious for $x = 0$, so we need only consider nonzero x. This we will do following [3].

Take a basis $\{b_k\}$ of L over $\mathbb{Q}_p$, and us it to define a max-norm $||\cdot||_m$ on L; note that the unit ball under this norm, as the product of finitely many compact spaces, is compact, and so is the unit sphere S as a closed subset of a compact space. Therefore, the max-norm $||\cdot||_m$ attains a (nonzero) minimum m and a maximum M on S.

Now, for some nonzero x with $||x||_m = c$, we have

$$\begin{aligned} \frac{||x||}{||x||_m} &= \frac{||x/c||}{||x/c||_m} \\ &= ||x/c|| \\ &\in [m, M] \end{aligned}$$

since $x/c \in S$. Therefore if $||x|| \leq 1$, then $||x||_m \leq m^{-1}$, so $||x+1||_m \leq m^{-1} + ||1||_m$, and finally $||x+1|| \leq M(m^{-1} + ||1||_m)$. Thus we may take $C = M(m^{-1} + ||1||_m)$. ∎

You will further note that all these extended valuations $||\cdot||$ are compatible. That is, if we have $x \in L, L'$, then the valuation $||\cdot||_p$ extended to L and to L' give the same value for $||x||_p$; this is why we do not subscript $||\cdot||$ additionally with the extension L. Therefore if we let Ω_p be the algebraic closure of $\mathbb{Q}_p$, we can define a valuation $|\cdot|_p$ on Ω_p simply as $|z|_p$ for $z \in \Omega_p$ is the same $||z||_p$ defined on some finite extension $L \ni z$.

4 Construction of $\mathbb{C}_p$

We would like to extend the p-adic field $\mathbb{Q}_p$ to a closed and complete space, to facilitate both algebra and analysis using the p-adics. In the case of the Archimedian $|\cdot|_\infty$ over $\mathbb{Q}$, we need merely find the algebraic closure $\mathbb{C}$ of $\mathbb{R} = \mathbb{Q}_v$; this field is not only algebraically closed, but also complete space under the extension of $|\cdot|_\infty$. For a p-adic valuation $|\cdot|_p$ this turns out not to be the case: Ω_p is not complete.

Definition. *Let $p^{a/b} \in \Omega_p$ denote a root of $x^b - p^a = 0$ for $a, b \in \mathbb{N}$, chosen so that $p^{ab/c} = (p^{a/c})^b$; $p^{a/b}$ will of course have valuation $p^{-a/b} \in \mathbb{R}$.*

Theorem 1. *The series*

$$s := \sum_{n=0}^{\infty} p^{k_n}, \qquad k_n = 3^{n^2}/2^{n^2}$$

does not converge in Ω_p, although the sequence of its partial sums is Cauchy.

Proof. The sequence of partial sums is Cauchy because the summands go to zero. Take any monic polynomial $P \in \mathbb{Q}_p[x]$ of degree m; we will show that $P(s) \neq 0$, specifically, that if we write

$$P(s) = \sum_{k=0} c_k p^{e_k}$$

then there is a k such that $c_k = 1$. Consider the exponents e_k of the terms that can arise when computing such a series for s^m. Let $e(\{n_a\}) = \sum_{a=1}^{m} 3^{n_a^2}/2^{n_a^2}$; this is the form that all the e_k will take. Sort the $\{n_a\}$ in descending order and let $N = \max\{n_a\}$; if precisely n_1 through n_b are equal to N, then this sum becomes

$$e(\{n_a\}_1^m) = 2^{-N^2}\left(3^{N^2} b + \sum_{a=b+1}^{m} 3^{n_a^2} 2^{N^2 - n_a^2}\right)$$

The sum component of this formula is divisible by 2^{2N-1} at least, and $b \leq m$. Therefore if $2N-1 > m$, this term's denominator is divisible by more than $(N-1)^2$ — but at most N^2 — powers of 2, so it is distinct from terms with lesser (and likewise greater) N.

Now consider the term p^{e_k} whose exponent e_k has the associated $N > (m+1)/2$ and $a_n = N$ for all a (that is, $b = m$). Since 3^{N^2} is odd, left-multiplication by it is invertible mod 2^{2N-1}, so since no other term in the expansion of $P(s)$ can have the same N and $b = m$, none can the same valuation as p^{e_k} (even allowing multiplication by powers of p). Therefore no other term in the expansion of $P(s)$ can cancel p^{e_k}, and so $P(s) \neq 0$ as desired.

We would like $\mathbb{C}_p$ to be both topologically complete and algebraically closed, like $\mathbb{C}$. Since Ω_p is not complete, we must complete it, producing $\hat{\Omega}_p$. Fortunately, the resulting space $\mathbb{C}_p := \hat{\Omega}_p$ is closed in addition to being complete.

Theorem 2 (Bruhat Proposition 7.5). *The completion $\hat{\Omega}_p$ of Ω_p is algebraically closed.*

Proof. We must show that any polynomial $f(x) \in \hat{\Omega}[x]$ of any degree n has at least one root in $\hat{\Omega}$. By rescaling the variable x as well as the coefficients of f, we may assume that $f \in \mathcal{O}_{\hat{\Omega}_p}[x]$ and that f is monic.

Write $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. By the definition of $\hat{\Omega}$, there is some Cauchy sequence in $\mathcal{O}_{\Omega_p}$ whose limit is a_k for each k. For each k, take some sufficiently sparse subsequence $\{a_{mk}\}$ of this Cauchy sequence, such that if $l < m$, $|a_{lk} - a_{mk}| < p^{-ln}$, and call $f_m(x) = x^n + a_{m\ n-1}x^{n-1} +$

$\ldots + a_{m1}x + a_{m0}$; notice that by the triangle inequality, $|f_m(x) - f(x)| < p^{-mn}$ for $x \in \mathcal{O}_{\hat{\Omega}_p}$.

Now, since $f_m \in \Omega_p[x]$, a complete field, we can write $f_m = \prod_{k=0}^{n-1}(x - r_{mk})$; since f_m has integer coefficients, the r_{mk} must be integers. Pick some r_{mk} and compute:

$$\begin{aligned} f_{m+1}(r_{mk}) &= f_{m+1}(r_{mk}) - f(r_{mk}) + f(r_{mk}) - 0 \\ &= (f_{m+1}(r_{mk}) - f(r_{mk})) + (f(r_{mk}) - f_m(r_{mk})) \end{aligned}$$

so that $|f_{m+1}(r_{mk})| < p^{-mn}$. Thus

$$\prod_{l=0}^{n-1} |(r_{mk} - r_{m+1\ l})| < p^{-mn}$$

and thus for some l, $|(r_{mk} - r_{m+1\ l})| < p^{-m}$. This gives us a Cauchy sequence of roots r_{mk_m} which converge to some $r \in \hat{\Omega}_p$. Taking the bound we used to construct this sequence, we have $|f_m(r)| < p^{-m}$, and so $f(r) = 0$ and we have succeeded in finding a root of f. ⩔

5 Extension of $|\cdot|_p$ to $\mathbb{C}$

$\mathbb{C}_p$ and $\mathbb{C}$ are intimately related, as is shown by the following theorem:

Theorem 3. *Assuming the Axiom of Choice, there is a field isomorphism $\phi : \mathbb{C} \to \mathbb{C}_p$. Thus we can extend the p-adic valuation to $\mathbb{C}$ by $|z|_p := |\phi(z)|_p$.*

Proof. In fact, there is an isomorphism between any two extensions of a field K if they are algebraically closed and have the same cardinality. Construct two transcendence bases A, B for $\mathbb{C}$ and $\mathbb{C}_p$; these must both be the same size as $\mathbb{R}$, so we can construct a bijection $\psi : A \to B$. Assign isomorphism $\phi_0 : K_0 := \text{span}_{\mathbb{Q}}(A) \to L_0 := \text{span}_{\mathbb{Q}}(B)$ by $\phi_0(a) = \psi(a)$ for $a \in A$, and sums and products of these as sums and corresponding products of their images; ϕ_0 is well-defined because A and B are transcendence bases, so expressions of elements in terms of them are unique up to polynomial identities.

Now, define a partially ordered set S of isomorphisms $\phi_I : K_I \to L_I$, where K_I is a superfield of K_0 and a subfield of $\mathbb{C}$, and L_I is a superfield of L_0 and a subfield of $\mathbb{C}_p$. Define the ordering $\phi_I \sqsupset \phi_J$ if and only if $K_I \supseteq K_J$ and $\phi_I(z) = \phi_J(z)$ for all $z \in K_J$. Clearly $\phi_0 \in S$. For any ascending chain $\{\phi_I\}_I$ in S, the isomorphism $\phi_U : \bigcup K_I \to L_I$ defined by $\phi_U(x) = \phi_I(x), x \in K_I$ is maximal, so by Zorn's lemma there is a maximal isomorphism $\phi_M : K_M \to L_M$ in S.

I claim that $K_M = \mathbb{C}$ and $L_M = \mathbb{C}_p$. For suppose that $\mathbb{C}\backslash K_M$ contained some element x. Since A is a full transcendence basis, this x must be algebraic over K_M, with some minimal polynomial $P(x) = 0$. $\phi_M(P)$ must then be irreducible in L_M by the isomorphism ϕ_M, but have a root $\hat{x}$ in $\mathbb{C}_p$, so we can assign $\phi_N(x) = \hat{x}$, and extend it to the ring $K_M(x)$ and thus find a greater valuation $\phi_X : K_M(x) \to L_M(\hat{x})$, contradicting maximality of ϕ_M.

Similarly, L_M can lack no element z of $\mathbb{C}_p$. Therefore, we have an isomorphism $\phi : \mathbb{C} \to \mathbb{C}_p$ as desired. ▽

6 Application

We will prove a simple theorem using this extension of $|\cdot|_p$ to $\mathbb{C}$. This theorem was presented at Mather House Math Table on October 15, 2002.

Theorem 4 (Loves Me, Loves Me Not). *If we dissect a square into some number n of triangles, all of which have the same area A, then n must be even.*

Proof. Following [2], we begin by coloring the plane based on an extension $|\cdot|$ of the valuation $|\cdot|_2$ to $\mathbb{R}$. Color a point (x, y) red if $|x| < 1, |y| < 1$. Color it blue if $|x| \leq |y|$ and $|y| \geq 1$, and color it green if $|x| > |y|$, and $|x| \geq 1$.

Assume that the square is the unit square with vertices at $(0,0)$, $(1,0)$, $(1,1)$, and $(0,1)$. Call the edges of triangles which are on the boundary of the square border edges. All the border edges with one vertex green and the other blue are on the top right or top left, and since $(0,1)$ is blue and $(1,0)$ green, there must be an odd number of them. Therefore by Sperner's lemma, there is a (possibly degenerate) triangle T inside the square with one red, one green, and one blue vertex; let these vertices have coordinates $(x_r, y_r), (x_g, y_g), (x_b, y_b)$, respectively. The area A of T is then the absolute value of

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

The valuation $|(x_b - x_r)(y_g - y_r)|$ of the right term is $|x_b||y_g| \geq 1$. Note also that $|x_b| \geq \max(|y_b|, |y_r|), |y_g| > \max(|x_g|, |x_r|)$ by the definitions of the colors. Therefore, by the strong triangle inequality, $|A| = |1/2||x_b||y_g| \geq 2$. Since $A = 1/n$, we have $|n| \leq 1/2$, so n is even. ∎

7 Conclusion

Due to the complete and algebraically closed structure of $\mathbb{C}_p$, p-adic analysis — that is, analysis over $\mathbb{C}_p$ — has power comparable to traditional complex analysis. Bruhat, along with many other books, provides a solid if difficult reference for further exploration of this field.

References

[1] Bruhat, F., *Lectures on Some Aspects of p-adic Analysis*, Bombay: Tata Institute of Fundamental Research, 1963.

[2] Fowler, Jim. *Loves Me, Loves Me Not: what you shouldn't do after you dissect a Square into Identical Triangles*. Math Table lecture, 10/15,2002.

[3] Stein, William, *A Brief Introduction to Classical and Adelic Algebraic Number Theory*. Course Notes for Math 129, 2004.