Valued Fields and Hensel's Lemma

Isaac Martin

Last compiled July 10, 2022

1 Absolute Values

The reader familiar with metric topologies will be aware of the various norms often considered on the finite dimensional vector space $\mathbb{R}$. Beyond the typical Euclidean norm, we often consider the norm $\|\cdot\|_1$, the sup norm $\|\cdot\|_\infty$, etc. All of these norms, when restricted to $\mathbb{R}$, recover the typical absolute value on $\mathbb{R}$. This begs the question, what are the different absolute values we can place on $\mathbb{R}$ or on other fields K?

Definition 1.1. Let K be a field. An *absolute value* on K is a function $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ such that

(i) $|x| = 0 \iff x = 0$

(ii) $|xy| = |x| \cdot |y|$

(iii) $|x + y| \leq |x| + |y|$ (triangle inequality).

We refer to the pair $(K, |\cdot|)$ as a *valued field*.

Exercise 1.2 (Quick)**.** Show that if $(K, |\cdot|)$ is a valued field then $|1| = 1$ and $|-1| = 1$.

An absolute value $|\cdot|$ on K generates a topology K.

Definition 1.3. Let $(K, |\cdot|)$ be a valued field. The *open/closed ball of radius $r \in \mathbb{R}$ centered at $x \in K$* are

$$B(x, r) = \{y \in K \mid |x - y| < r\}, \quad \text{and}$$
$$\overline{B}(x, r) = \{y \in K \mid |x - y| \leq r\},$$

respectively. The collection of all such open balls generate a topology on K, which we call the metric topology. It is precisely the metric topology on K under the metric $d(x, y) = |x - y|$.

The discussion above begs the question,

Question 1.1. Given a field K, how many distinct absolute values are there on K?

Note that two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are said to be *equivalent* if they generate the same topology on the field.

Absolute values fall into one of two categories: Archimedean and non-Archimedean. An absolute value $|\cdot|$ on a field K is said to be *Archimedean* if it satisfies the Archimedean property: for all $x, y \in K$ there exists an integer $n \in \mathbb{Z}$ such that $|nx| > |y|$. A field is said to be *non-Archimedean* if it does not satisfy this property. However, despite the name, non-Archimedean absolute values are more often defined in the following way:

Definition 1.4. An absolute value $|\cdot|$ on a field K is said to be *non-Archimedean* if it satisfies the following stronger version of the triangle inequality:

(iv) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.

This is quite strange for a myriad of reasons. For one, open and closed balls have no center.

Proposition 1.5. Suppose $x, y \in K$ and $r \in \mathbb{R}$. If $y \in B(x,r)$ then $B(y,r) = B(x,r)$.

Proof: Suppose $z \in B(x,r)$. Then

$$|y - z| = |y - x + x - z| \leq \max\{|y-x|, |x-z|\} < r$$

since both y and z are in $B(x,r)$. Hence $B(x,r) \subseteq B(y,r)$. The reverse inclusion follows identically by swapping the roles of x and y. □

For another, open balls are closed sets and closed balls are open sets.

Proposition 1.6. Suppose that $(K, |\cdot|)$ is a non-Archimedean field, $x \in K$ and $r \in \mathbb{R}$. Then $B(x,r)$ is a closed set and $\overline{B}(x,r)$ is an open set (i.e. both are clopen).

Proof: We first show that $B(x,r)$ is closed by showing its complement is open. Let $y \notin B(x,r)$ so that $|x-y| \geq r$. We claim that $B(y,r) \cap B(x,r) = \emptyset$. If this intersection were not trivial, then there would be some $z \in B(y,r) \cap B(x,r)$ satisfying $|x-z| < r$ and $|y-z| < r$. But then

$$|x-y| = |x-z+z-y| \leq \max\{|x-z|, |x-y|\} < r,$$

and hence $y \in B(x,r)$, which is not the case. Hence $B(y,r) \cap B(x,r) = \emptyset$ and so y has an open set entirely contained in the complement of $B(x,r)$. Since y was chosen to arbitrarily, the complement of $B(x,r)$ is open.

We now show that $\overline{B}(x,r)$ is open. Choose $y \in \overline{B}(x,r)$ and pick an arbitrary open neighborhood U of y. As the open balls form a basis for the topology on K, we may find a $B(y,s) \subseteq U$, and may assume $0 < s < r$. For any $z \in B(y,s)$ we get

$$|x-z| = |x-y+y-z| \leq \max\{|x-y|, |y-z|\} = r,$$

and so $z \in \overline{B}(x,r)$. This means $B(y,s) \subseteq \overline{B}(x,r)$, and as above we conclude that $\overline{B}(x,r)$ is open. □

Quite weird indeed. The reader may be wondering at this point whether non-Archimedean absolute values exist at all. To stave off these concerns, let's consider an example.

Example 1.7. Consider $\mathbb{Q}$ and fix a prime integer p. For any $\frac{a}{b}$, we may find a unique $n \in \mathbb{Z}$ such that $\frac{a}{b} = p^n \frac{x}{y}$ for some integers $x, y \in \mathbb{Z}$ such that $p \not| x$ and $p \not| y$. Define the *p-adic absolute value* $|\cdot|_p : \mathbb{Q} \longrightarrow \mathbb{R}_{\geq 0}$ by

$$\left|\frac{a}{b}\right|_p = \begin{cases} 0 & \text{if } \frac{a}{b} = 0 \\ p^{-n} & \text{otherwise} \end{cases}.$$

We claim that $|\cdot|_p$ is a non-Archimedean absolute value on $\mathbb{Q}$. Indeed, one may quickly check that $|x| = 0$ if and only if $x = 0$ and $|xy|_p = |x|_p \cdot |y|_p$. For the ultrametric inequality, suppose $x = p^n \frac{a}{b}$ and $y = p^m \frac{c}{d}$ are rational numbers and p does not divide a, b, c or d. Suppose without loss of generality that $n < m$, so that $|x|_p = p^{-n} \geq p^{-m} = |y|_p$. Then

$$x + y = p^n \left(\frac{a}{b} + p^{m-n}\frac{c}{d}\right) = p^n \left(\frac{ad + p^{m-n}bc}{bd}\right).$$

Since bd is coprime to p, any additional factors of p must come from the numerator. That is, if $x+y = p^{\ell}\frac{a'}{b'}$ with a' and b' coprime to p, it must be the case that $n \leq \ell$. Hence $|x+y|_p = p^{-\ell} \leq p^{-n} = \max\{|x|_p, |y|_p\}$.

Hence $|\cdot|_p$ satisfies the ultrametric property and is therefore a non-Archimedean absolute value.

Let's include one more example so as not to be accused of cherry picking.

Example 1.8. Let K be a field. The *power series ring* over K is defined to be

$$K[\![t]\!] = \left\{ \sum_{n=0}^{\infty} a_n t^n \;\middle|\; a_n \in K \right\}.$$

It's field of fractions is the field of *formal Laurent series* over K, given by

$$K(\!(t)\!) = \left\{ \sum_{n=N}^{\infty} a_n t^n \;\middle|\; a_n \in K, N \in \mathbb{Z} \right\}$$

so that a power series is only allowed to contain finitely many terms $a_n t^n$ with $n < 0$.

The *t-adic* absolute value $|\cdot|_t$ on $K(\!(t)\!)$ is defined

$$\left| \sum_{n\in N}^{\infty} a_n t^n \right|_t = \frac{1}{N}$$

where a_N is the first nonzero coefficient. It is left to the reader to check that this is a non-Archimedean absolute value.

The following theorem provides a characterize of non-Archimedean absolute values. It boils down to showing that an absolute value satisfies the ultrametric inequality if and only if it doesn't satisfy the Archimedean property.

Theorem 1.9. *Let $(K, |\cdot|)$ be a valued field. The absolute value $|\cdot|$ is non-Archimedean if and only if $\{|n| \mid n \in \mathbb{Z}\}$ is bounded in $\mathbb{R}$.*

Proof: To do. □

Finally, to conclude this introductory section, we list the first lemma that appears in the proof of Hensel's lemma. This condition is used throughout the literature frequently without comment, so it is worth familiarizing yourself with it.

Lemma 1.10 (Case of Equality)**.** Let $(K, |\cdot|)$ be a non-Archimedean absolute value. Then whenever $|x| \neq |y|$ we have $|x+y| = \max\{|x|, |y|\}$.

Proof: Without loss of generality assume that $|x| < |y|$. Then

$$|y| = |x - x + y| = \max\{|-x|, |x+y|\} = |x+y| \leq \max\{|x|, |y|\} = |y|.$$

Note that $\max\{|-x|, |x+y|\} = |x+y|$ as otherwise $|y| \leq |x|$. □

2 Valuations

This section will be made more comprehensive in the future. For now, we simply write down some definitions.

Definition 2.1. Let K be a field. A *valuation* on K is a map $v : K^\times \longrightarrow \mathbb{R}$ satisfying the following properties:

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x + y) \geq \min\{v(x), v(y)\}$.

The first thing to note about valuations is their connection to absolute values. In particular, valuations yield absolute values and vice versa.

Proposition 2.2. Let K be a field and fix some $\alpha \in \mathbb{R}$ so that $0 < \alpha < 1$.

- If $|\cdot| : K \longrightarrow \mathbb{R}_{0\leq}$ is an absolute value on K then $v : K^\times \longrightarrow \mathbb{R}$ defined $v(x) = \log_\alpha(|x|)$ is a valuation.
- If $v : K^\times \longrightarrow \mathbb{R}$ is a valuation on K, then $|\cdot| : K \longrightarrow \mathbb{R}_{0\leq}$ defined $|x| = \alpha^{v(x)}$ is an absolute value on K.

□

However, despite the connection to absolute values, we typically think of valuations on fields as an algebraic construct rather than an analytic one. The following illustrates this point.

Proposition 2.3. Let K be a field and $v : K^\times \longrightarrow \mathbb{R}$ a valuation. The *valuation ring* of K is the set $\mathcal{O}_K = \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$.

There is also a special kind of valuation, which we will see corresponds to non-Archimedean absolute values.

Definition 2.4. Let $v : K^\times \longrightarrow \mathbb{R}$ be a valuation. We say that v is a *discrete valuation* if there exists some real number $a \in \mathbb{R}$ such that $a \cdot v(K^\times) = \mathbb{Z}$. In this case, we redefine v to include this scaling by a, i.e. $v(x) = a \cdot v'(x)$ where v' is the original valuation, and write $v : K^\times \longrightarrow \mathbb{Z}$.

The valuation ring of a discrete valuation is quite special. It is called a *discrete valuation ring*, and it has some exceptionally nice properties. In particular, it is local:

Proposition 2.5. Suppose K is a field and $v : K^\times \longrightarrow \mathbb{Z}$ is a discrete valuation. Then $\mathcal{O}_K$ is a local ring with unique maximal ideal $\mathfrak{m} = \{x \in K^\times \mid v(x) \geq 1\} \cup \{0\}$.

We have a case of equality for valuations too.

Proposition 2.6. Suppose $v : K^\times \longrightarrow \mathbb{Z}$ is a discrete valuation and $x, y \in K^\times$ satisfy $v(x) \neq v(y)$. Then $v(x + y) = \min(v(x), v(y))$. □

Proposition 2.7. Let $(K, |\cdot|)$ be a complete valued field and let $\pi \in \mathcal{O}_K$ with $|\pi| < 1$. Let $A \subseteq \mathcal{O}_K$ be a set of coset representatives for the residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$. Show that any $x \in K$ can be written uniquely as a power series $x = \sum_{i=n}^{\infty} a_i\pi^i$ with $a_i \in A$, $n \in \mathbb{Z}$ and that any such power series converges to an element of $\mathcal{O}_K$.

> *Proof:* In essence, we are arguing that we have an isomorphism $K \cong k(\!(t)\!)$. I claim it suffices to prove that for every $x \in \mathcal{O}_K$ we can uniquely write $x = \sum_{i=0}^{\infty} a_i\pi^i$ for some $a_i \in A$ and that every such power series

converges to a unique element in $\mathcal{O}_K$. We then get an isomorphism $\mathcal{O}_K \cong k[\![t]\!]$ by reducing a_i and sending $t \mapsto \pi$. Taking $\mathrm{Frac}(-)$ on both sides yields the desired result for K.

Let $\sum_{i=0}^{\infty} a_i \pi^i$ be a power series as above. Note that $|a_i| \leq 1$ since $a_i \in A \subseteq \mathcal{O}_K$. For any nonnegative integers n, m with $m > n$, we have

$$\begin{aligned}
\left| \sum_{i=0}^{m} a_i \pi^i \ - \ \sum_{i=0}^{n} a_i \pi^i \right| &= \left| a_m \pi^m + \cdots + a_{n+1} \pi^{n+1} \right| \\
&\leq \left| \pi^m + ... + \pi^{n+1} \right| \\
&\leq \max\{|a_m \pi^m|, ..., |a_{n+1} \pi^{n+1}|\} \\
&\leq \max\{|\pi|^m, ..., |\pi|^{n+1}\} \qquad (|a_i| \leq 1) \\
&= |\pi|^{n+1}.
\end{aligned}$$

Because $|\pi| < 1$, $|\pi|^{n+1} \longrightarrow 0$ as $n \longrightarrow \infty$. Hence the sequence $\left(\sum_{i=0}^{n} a_i \pi^i \right)_{n=0}^{\infty}$ is Cauchy and $\sum_{i=0}^{\infty} a_i \pi^i$ converges to some element of K by completeness. We have that

$$\left| \sum_{i=0}^{n} a_i \pi^i \right| \leq \max\{|a_0|, ..., |a_n \pi^n|\} \leq 1$$

for each nonnegative integer n, since $a_i| \leq 1$ and $|\pi| < 1$ implies $|a_i \pi^i| = |a_i||\pi|^i \leq 1$ for each nonnegative integer i. Limits preserve nonstrict inequalities, so

$$\left| \sum_{i=0}^{\infty} a_i \pi^i \right| \leq 1,$$

meaning the sum necessarily converges to an element of $\mathcal{O}_K$.

We now prove that any $x \in \mathcal{O}_K$ can be written uniquely as a power series $x = \sum_{i=0}^{\infty} a_i \pi^i$ with $a_i \in A$. Define $a_0 \equiv x \ (\mod \pi)$. Suppose that we have chosen $a_0, ..., a_{n-1} \in A$ such that

$$x \equiv \sum_{i=0}^{n-1} a_i \pi^i \ (\mod \pi^n).$$

This means there exists some $c_n \in \mathcal{O}_K$ such that $x - \sum_{i=0}^{n-1} a_i \pi^i = c_n \pi^n$; choose $a_n \in A$ such that $a_n \equiv c_n \ (\mod \pi)$. There is therefore some d such that $d\pi = c_n - a$. Multiplying both sides by π^n yields $d\pi^{n+1} = c_n \pi^n - a\pi^n$, hence $c_n \pi^n \equiv a_n \pi^n \ (\mod \pi^{n+1})$. Then

$$x - \sum_{i=0}^{n} a_i \pi^i \equiv x - \left(\sum_{i=0}^{n-1} a_i \pi^i \right) \ - \ a_n \pi^n \equiv x - \left(\sum_{i=0}^{n-1} a_i \pi^i \right) \ - \ c_n \pi^n \equiv 0 \ (\mod \pi^{n+1}).$$

We thus have that for $n \in \mathbb{N}$, $x - \sum_{i=0}^{n} a_i \pi^i = c_n \pi^{n+1}$ for some $c_n \in \mathcal{O}_K$, hence

$$\left| x - \sum_{i=0}^{n} a_i \pi^{i+1} \right| = \left| c_{n+1} \pi^{n+1} \right| \leq \left| \pi^{n+1} \right| = |\pi|^{n+1} \longrightarrow 0,$$

and therefore $x = \sum_{i=0}^{\infty} a_i \pi^i$ in $\mathcal{O}_K$. Uniqueness of this summation follows from the fact that the set A contains exactly one representative for each equivalence class in $\mathcal{O}_K / \pi \mathcal{O}_K$, and we are done. $\square$

Let's write down some integers and fractions in the case that $K = \mathbb{Q}_p$.

Example 2.8. Set $p = 5$, $x = 40$ and let $A = \{0, ..., p-1\}$ be the set of coset representatives for $\mathbb{F}_5$. We can calculate the coefficients a_i by considering $x \mod p^i$ for various powers i.

If $40 = a_0 5^0 + a_1 5^1 + a_{25}^2 ...$ then $40 \equiv a_0 \mod 5 \implies a_0 = 0$. Similarly,

$$40 \equiv a_1 5^1 \mod 5^2 \implies 15 \equiv a_1 5^1 \implies a_1 = 3$$

and

$$40 \equiv a_1 5^1 + a_2 5^2 \mod 5^3 \implies a_2 = 1.$$

Example 2.9. Now lets try a fraction. Set $p = 5$ again, $x = \frac{9}{40}$ and let $A = \{0, ..., 4\}$ as before.

Step 1: Factor out as many 5's as possible.

$$\frac{9}{40} = 5^{-1}\frac{9}{8}.$$

Step 2: Since the denominator of $\frac{9}{8}$ contains no 5's in its prime factorization, $\frac{9}{8}$ is an element of $\mathbb{Z}_{(5)} \subseteq \mathbb{Z}_5$ and hence can be written as a power series $\sum_{i=0}^{\infty} a_i 5^i$. Calculate the coefficient a_i inductively by looking modulo 5^{i+1}.

For a_0:

$$\frac{9}{8} \equiv a_0 \mod 5 \implies 4 \equiv 8 \cdot a_0 \mod 5 \implies a_0 = 3,$$

For a_1:

$$\begin{aligned} \frac{9}{8} \equiv a_0 + a_1 5 \mod 25 &\implies \frac{9}{8} - 3 \equiv a_1 5 \mod 25 \\ &\implies 9 \cdot (-3) - 3 \equiv -30 \equiv 20 \equiv a_1 5 \mod 25 \\ &\implies a_1 = 4, \end{aligned}$$

Etc. Notice that this involves computing $\frac{9}{8}$ modulo 5^i for each $i \in \mathbb{N}$.

Step 3: Multiply in the 5's from step 1.

$$\frac{9}{40} = 5^{-1}\left(3 + 4 \cdot 5^1 + ...\right) = 3 \cdot 5^{-1} + 4 \cdot 5^0 + ...$$

and we are done.

3 Hensel's Lemma

Theorem 3.1 (Hensel's Lemma)**.** *Let $(K, |\cdot|)$ be a non-Archimedean complete valued field with valuation ring $\mathcal{O}_K \subseteq K$ and fix $f \in \mathcal{O}_K[y]$. If $a \in \mathcal{O}_K$ satisfies $|f(a)| < |f'(a)^2|$ then there exists a unique $x \in \mathcal{O}_K$ such that $|x - a| < |f'(a)|$ and $f(x) = 0$.*

Here's the idea behind the proof. Letting π be a uniformizer for K with respect to the valuation v, construct a sequence $\{x_n\} \subseteq \mathcal{O}_K$ such that $x_n \equiv a \mod \pi$ and $f(x_n) \equiv 0 \mod \pi^n$. This way, as $n \longrightarrow \infty$, we converge on an element $x \in \mathcal{O}_K$ such that $f(x) = 0$ and still have $x \equiv a \mod \pi$. The latter condition helps with uniqueness, as $x \equiv a \mod \pi$ means that x is "close" to a in the absolute value corresponding to π. We construct this sequence recursively as follows:

- set $x_0 = a$
- set $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$.

This is precisely Newton's method. To ensure this sequence actually converges, we need the following two lemmas.

Lemma 3.2. Let $v : K^\times \longrightarrow \mathbb{R}$ be a valuation on a field K. If $x, y \in K^\times$ and $v(x) \neq v(y)$, then $v(x+y) = \min\{v(x), v(y)\}$.

Lemma 3.3. Let R be any ring, and consider $f(x) \in R[x]$. If y is another indeterminant, then there exist $f_0, ..., f_d \in R[x]$ where $d = \deg f$ such that

$$f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + ... + f_d(x)y^d.$$

Furthermore, $f_0 x(x) = f(x)$ and $f_1(x) = f'(x)$.

Proof: Proof here □

We are now ready to prove Hensel's lemma.

Proof: (Hensel's Lemma) Proof goes here woo. □

When identifying/counting roots of a polynomial, we often use the following corollary instead. It immediately follows from Hensel's lemma in the case that $v(f'(a)) = 0$.

Corollary 3.4. Let $(K, |\cdot|)$ be a non-Archimedean complete valued field with valuation ring $\mathcal{O}_K \subseteq K$ and fix $f \in \mathcal{O}_K[y]$. If $a \in \mathcal{O}_K$ is a simple root of $\overline{f} \in \mathcal{O}_K/\mathfrak{m}$, then there exists a unique $x \in \mathcal{O}_K$ such that $x \equiv a \mod \mathfrak{m}$ and $f(x) = 0$.

Let's look at some examples.

Example 3.5. Show that the equation $x^3 - 3x + 4 = 0$ has a unique solution in $\mathbb{Z}_7$, but has no solutions in $\mathbb{Z}_5$ or in $\mathbb{Z}_3$. How many are there in $\mathbb{Z}_2$?

Proof: Let $f(x) = x^3 - 3x + 4$ denote the polynomial of interest in $\mathbb{Z}_p[x]$. First consider $p = 7$ and $\overline{f} \in \mathbb{F}_7$. We see here that we have a factorization $\overline{f} = (x-4)(x^2 + 4x - 1)$. If $x^2 + 4x - 1$ were reducible, then it would necessarily factor into linear factors and therefore have a root in $\mathbb{F}_7$, but via exhaustion we see that no such root exists. This means $x = 4$ is a simple root of $\overline{f}$, and by a Corollary to Hensel's lemma, there must exist a unique solution $a \in \mathbb{Z}_7[x]$ to the equation $f(x) = 0$ where $a \equiv 4 \pmod 7$.

Now consider $p = 3$ $\overline{f} \in \mathbb{F}_3[x]$. Here, $\overline{f}(x) = x^3 + 1$. If f had a root $a \in \mathbb{Z}_3$, then $\overline{f}(\overline{a}) = 0$ in $\mathbb{F}_3$. However, one can easily check $\overline{f}(x) = x^3 + 1$ has no roots in $\mathbb{F}_3$, and hence has no roots in $\mathbb{Z}_3$.

Similarly, for $p = 5$, the polynomial $\overline{f}(x) = x^3 + 2 - 1 \in \mathbb{F}_5$ has no roots, and therefore f has no roots in

$\mathbb{Z}_5$.

Now let $p = 2$. The polynomial $\overline{f}(x) = x^3 - 3x + 4 = x^3 + x = x(x^2 + 1) = x(x + 1)^2$ in $\mathbb{F}_2[x]$. Because $x = 0$ is a simple root in $\mathbb{F}_2$, Hensel's lemma tells us that f has a simple root $a \in \mathbb{Z}_2[x]$ such that $a \in (2) \in \mathbb{Z}_2$. However, it does not tell us whether the double root appearing modulo 2 lifts to a root (or possibly two roots) in $\mathbb{Z}_2$. If this roots lifted to $\mathbb{Z}_2$ then it would necessarily also lift to $\mathbb{Z}_2/(4)$, however, $\overline{f}(x) \equiv x(x^2 - 3) \pmod{2^2}$. Via exhaustion, we check that $x^2 - 3$ has no root in $\mathbb{Z}_2/(4)$, and hence the double root in $\mathbb{F}_2$ does not lift to a root in $\mathbb{Z}_2$. We conclude that $f(x) = x^3 - 3x + 4$ has only one root in $\mathbb{Z}_2$. $\square$