Ostrowski's Theorem and Completions of Fields

Joshua Ruiter

October 15, 2019

Introduction

These notes provide an introduction to absolute values on arbitrary fields, with a focus on absolute values on $\mathbb{Q}$, where Ostrowski's Theorem provides a complete classification. We begin with definitions and examples, discuss the induced metric of an absolute value, then prove Ostrowski's Theorem. We then discuss the completion of a field with respect to an absolute value. Along the way, we see a few somewhat strange properties of nonarchimedean fields.

The main source for these notes is chapter 7 of Milne's notes on algebraic number theory, which can be found at `https://www.jmilne.org/math/CourseNotes/ANT.pdf`. Another source which was useful for the correspondence between absolute values and additive valuations was `https://www2.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf`.

Contents

1 Absolute values

The usual absolute value function $\mathbb{R} \to \mathbb{R}$, has the following properties.

(1) Positivity	$\lvert x\rvert > 0$ except that $\lvert 0\rvert = 0$
(2) Multiplicativity	$\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$
(3) Triangle inequality	$\lvert x+y\rvert \leq \lvert x\rvert + \lvert y\rvert$

We take this as our motivation to define an absolute value on an arbitrary field to be any function satisfying these same properties.

Definition 1.1. An **absolute value** or **multiplicative valuation** on a field K is a function $|\cdot| : K \to \mathbb{R}$ such that for $x, y \in K$ we have

(1) Positivity	$\lvert x\rvert > 0$ except that $\lvert 0\rvert = 0$
(2) Multiplicativity	$\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$
(3) Triangle inequality	$\lvert x+y\rvert \leq \lvert x\rvert + \lvert y\rvert$

The multiplicative property can be expressed as saying $|\cdot|$ restricts to a group homomorphism $K^\times \to (\mathbb{R}_{>0}, \times)$, which tells us that all roots of unity in K are mapped to 1. As a consequence, $|-1| = 1$, so by multiplicativity $|-x| = |x|$.

Definition 1.2. An absolute value $|\cdot| : K \to \mathbb{R}$ is **discrete** if the image of $|K^\times|$ is a discrete subgroup of $(\mathbb{R}_{>0}, \times)$.

Note that the neither the usual absolute value $\mathbb{R} \to \mathbb{R}$ nor its restriction $\mathbb{Q} \to \mathbb{R}$ is discrete, but we will encounter discrete absolute values shortly.

Definition 1.3. If an absolute value $|\cdot| : K \to \mathbb{R}$ satisfies the **nonarchimedean triangle inequality** for all $x, y \in K$,

$$(3') \qquad |x+y| \leq \max(|x|, |y|)$$

then we say the absolute value is **nonarchimedean**. If not, then we say it is **archimedean**.

Remark: Note that with positivity, the nonarchimedean triangle inequality implies the usual triangle inequality.

$$\text{Positivity} \implies |x|, |y| \leq |x| + |y| \implies \max(|x|, |y|) \leq |x| + |y|$$

Examples:

1. The usual absolute value on $\mathbb{R}$ is an archimedean absolute value on $\mathbb{Q}$ or $\mathbb{R}$. We could also think of this as the restriction of the norm on $\mathbb{C}$.

$$|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

2. The **complex norm** $\mathbb{C} \to \mathbb{R}, z \mapsto |z| = \sqrt{z\overline{z}}$ is an archimedean absolute value. We can even think of the standard absolute value $\mathbb{R} \to \mathbb{R}$ as the restriction of this to $\mathbb{R}$.

3. On any field K, we have the **trivial absolute value** which is $|x| = 1$ for $x \neq 0$, and $|0| = 0$. Any other absolute value is called **nontrivial**.

4. Let p be a prime. The **p-adic absolute value** $|\cdot|_p$ on $\mathbb{Q}$ is defined as follows. First, define $|0|_p = 0$. Then note that by the multiplicative property, it suffices to define $|\cdot|_p$ on a (multiplicative) generating set of $\mathbb{Q}^\times$, so it suffices to define it on -1 and primes q. We have to choose $|-1| = 1$, and for primes q, define

$$|q|_p = \begin{cases} 1 & q \neq p \\ p^{-1} & q = p \end{cases}$$

Then by unique factorization, for nonzero $x \in \mathbb{Q}$, we can compute $|x|_p$ as

$$|x|_p = |p^n x'|_p = |p^n|_p |x'|_p = |p|_p^n = p^{-n}$$

where x' is a reduced fraction with numerator and denominator not divisible by p. The fact that this is a nonarchimedean absolute value is not too hard. Positive is obvious, and multiplicativity is by definition. The nonarchimedean triangle inequality is not obvious, but proving it is a relatively short exercise in number theory. See `https://math.stackexchange.com/questions/205886/how-to-prove-the-strong-triangle-inequality` for a proof.

In order to check their understanding of the p-adic absolute value, the reader is encouraged to verify that $\left|\frac{56}{3}\right|_2 = \frac{1}{8}$.

The uninformed reader may be wondering at this point if this has gone off the rails. If this strange-looking p-adic thing is an absolute value on $\mathbb{Q}$, who knows what else there could be? Ostrowski's Theorem later tells us that the situation is not so bad; the possible absolute values on $\mathbb{Q}$ can be fully described.

1.1 Metric induced by an absolute value

Just as the usual absolute value function $\mathbb{R} \to \mathbb{R}$ induces the standard metric topology on $\mathbb{R}$, or as the complex norm induces the standard topology on $\mathbb{C}$, any absolute value gives rise to a metric topology.

Definition 1.4. Let $|\cdot| : K \to \mathbb{R}$ be an absolute value. The **induced metric** on K is $d(x, y) = |x - y|$. This is in fact a metric (exercise for the reader), so $|\cdot|$ induces a metric topology on K.

The standard absolute value $|\cdot|_\infty$ induces the standard topology on $\mathbb{R}$, and when viewed as an absolute value on $\mathbb{Q}$, induces the subspace topology on $\mathbb{Q} \subset \mathbb{R}$. As we shall soon see, the p-adic absolute value induces a topology on $\mathbb{Q}$ that is far different from the subspace topology from $\mathbb{R}$.

Example: Consider the numbers $2^{10} = 1024$ and $2^{11} = 2048$. In the $|\cdot|_\infty$ metric, the distance between them is

$$|2048 - 1024|_\infty = |1024|_\infty = 1024$$

However, in the 2-adic metric, the distance is

$$|2048 - 1024|_2 = |1024|_2 = |2^{10}|_2 = 2^{-10} = \frac{1}{1024} \approx 0.001$$

So $\mathbb{Q}$ with a p-adic metric does not behave like a subspace of $\mathbb{R}$.

Example: Consider the sequence

$$p^0, p^1, p^2, p^3, \ldots$$

With respect to $|\cdot|_p$, the absolute values are

$$p^{-0}, p^{-1}, p^{-2}, p^{-3}, \ldots$$

thus this sequence converges to zero in the p-adic topology. Another interesting sequence is the factorial sequence

$$0!, 1!, 2!, 3!, \ldots$$

which converges to zero in the p-adic topology for any prime p.

If we needed any more convincing at this point, the next proposition tells us that $\mathbb{Q}$ with a p-adic metric behaves very differently than any sort of Euclidean space.

Proposition 1.1 (All triangles are isosceles)**.** *Let K be a field with a nonarchimedean absolute value $|\cdot|$ and induced metric $d(x,y) = |x - y|$. Then every triangle in K is isosceles. That is, for any three distinct points $a, b, c \in K$, at least two of $|a-b|, |a-c|, |b-c|$ are equal.*

It may be confusing to think of three points in $\mathbb{Q}$ composing a triangle, but we need to avoid thinking of $\mathbb{Q}$ as a subset of the real line when dealing with $|\cdot|_p$. As an example, consider the "triangle" $0, 1, 3$. If we take the side lengths in the $|\cdot|_\infty$ distance, we get the following side lengths.

$$|1-0|_\infty = 1 \qquad |3-1|_\infty = 2 \qquad |3-0|_\infty = 3$$

If we take side lengths in the $|\cdot|_3$ distance, we get side lengths as

$$|1-0|_3 = |1|_3 = 1 \qquad |3-1|_3 = |2|_3 = 3^{-0} = 1 \qquad |3-0|_3 = |3|_3 = 3^{-1} = \frac{1}{3}$$

So as the theorem tells us to expect, two of the side lengths are the same.

Proof. First, we consider the case where $c = 0$. Suppose $|a| < |b|$, so side ac is shorter than side bc. By the nonarchimedean triangle inquality, the third side ab has length satisfying

$$|a-b| \leq \max(|a|, |b|) = |b|$$

Using the nonarchimedean triangle inequality again,

$$|b| = |a - (a-b)| \leq \max(|a|, |a-b|)$$

Since $|a| < |b|$, we can't have $|b| \leq |a|$, so $\max(|a|, |a-b|)$ must be $|a-b|$. That is, $|a-b| \leq |b| \leq |a-b|$, so $|a-b| = |b|$. That is, sides bc and ab are the same length, which is what we wanted to prove.

Now consider the general case of three distinct points a, b, c. Notice that $d(a, b)$ is translation invariant, that is, for any $x, y, z \in K$ we have

$$d(x, y) = |x - y| = |(x + z) - (y + z)| = d(x + z, y + z)$$

We translate our triangle a, b, c to the triangle $a-c, b-c, 0$, which by the previous argument has two sides of the same length. Since our distance is translation invariant, the side lengths of triangle a, b, c are the same as the side lengths of the translated triangle, so we're done. $\square$

Remark: The proof actually gives us something stronger than the theorem. The proof tells us that a triangle in a nonarchimedean field has two equal sides, and if the triangle is not equilateral, then the length of one of the equal sides is greater than the length of the third side.

1.2 Equivalence of absolute values

We could consider absolute values to all be different if they are just different as functions $K \to \mathbb{R}$, but it turns out that it's more useful to only consider equivalence classes with respect to the following notion of equivalence. In particular, this notion of equivalence will make the statement of Ostrowski's Theorem much cleaner.

Definition 1.5. Let $|\cdot|_\alpha$ and $|\cdot|_\beta$ be nontrivial absolute values on a field K. They are **equivalent** if $|x|_\alpha = |x|_\beta^a$ for some real number $a > 0$ and for all $x \in K$. (Exercise: Verify that this is an equivalence relation.)

Exercise: Show that as absolute values on $\mathbb{Q}$, $|\cdot|_\infty$ is not equivalent to $|\cdot|_p$ for any p, and $|\cdot|_p$ is equivalent to $|\cdot|_q$ if and only if $p = q$.

The next proposition gives an another characterization of equivalence, but isn't needed to prove Ostrowski's Theorem, so I'll just state it without proof. A proof can be found in Milne's notes on algebraic number theory (see the hyperlink in the introduction).

Proposition 1.2 (Milne, Prop 7.8)**.** *Two nontrivial absolute values on a field K are equivalent if and only if they induce the same metric topology on K.*

Remark: For nontrivial absolute values $|\cdot|_\alpha, |\cdot|_\beta$ on $\mathbb{Q}$, they are equivalent if there exists $a \in \mathbb{R}$, $a > 0$ so that $|n|_\alpha = |n|_\beta^a$ for all $n \in \mathbb{Z}, n > 1$. This is because the equality always holds for zero and -1, and an absolute value on $\mathbb{Q}$ is determined by its values on the (multiplicative) generating set of -1 and positive primes.

1.3 Ostrowski's Theorem

Theorem 1.3 (Ostrowski)**.** *Let $|\cdot|$ be a nontrival absolute value on $\mathbb{Q}$.*

- *If $|\cdot|$ is archimedean, then $|\cdot|$ is equivalent to $|\cdot|_\infty$.*

- *If $|\cdot|$ is nonarchimedean, then it is equivalent to $|\cdot|_p$ for exactly one prime p.*

Outline of proof:

1. Start with an arbitrary absolute value $|\cdot|$ on $\mathbb{Q}$, and show that it is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some p.

2. Consider two separate cases: (1) $\forall n \in \mathbb{Z}_{\geq 1}$, $|n| \leq 1$, and (2) $\exists n \in \mathbb{Z}_{\geq 1}$ such that $|n| > 1$.

3. Show that everything in case (1) is equivalent to $|\cdot|_p$ for some p, and everything in case (2) is equivalent to $|\cdot|_\infty$.

4. Outline of case (1) analysis: find a positive integer n with $|n| < 1$, write it as a product of primes, and conclude that $|p| < 1$ for some prime p using unique prime factorization. Show that for primes $q \neq p$, $|q| = 1$. From here, can compute that

$$|n| = |n|_p^a$$

for $a = -\frac{\log |p|}{\log p}$.

5. Outline of case (2) analysis: Choose m with $|m| > 1$. For an arbitrary positive integer n, expand m in base n as

$$m = a_0 + a_1 n + a_2 n^2 + \ldots + a_r n^r$$

with $0 \leq a_i < n$. Take absolute values, and after a string of inequalities, conclude that

$$|m| \leq |n|^{\frac{\log m}{\log n}}$$

which implies that $|n| > 1$ as well. Raising both sides to the $\frac{1}{\log m}$ power, obtain

$$|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}$$

Now since m, n are both arbitrary, the same argument shows the reverse inequality, so we get this as an equality for all positive integers m, n. After some rearranging, this gives

$$|n| = |n|_\infty^a$$

where $a = \log\left(|n|^{\frac{1}{\log n}}\right)$.

Note: The following proof due to Wikipedia `https://en.wikipedia.org/wiki/Ostrowski%27s_theorem` and Milne `https://www.jmilne.org/math/CourseNotes/ANT.pdf`. The nonarchimedean case in Milne involves more technical language, but there is a simpler proof on Wikipedia, so I went with that. In the archimedean case, Milne and Wikipedia have essentially the same argument.

Proof. We consider two cases, (1) $\forall n \in \mathbb{Z}_{\geq 1}, |n| \leq 1$, and (2) $\exists n \in \mathbb{Z}_{\geq 1}$ such that $|n| > 1$. Recall that to show equivalence, we just have to show equivalence for positive integers. We will show that everything in case (1) is equivalent to some p-adic absolute value, and everything in case (2) is equivalent to the standard absolute value.

(Case 1) Suppose that for all $n \in \mathbb{Z}_{\geq 1}$, $|n| \leq 1$. Since the absolute value is nontrivial, there exists $\frac{a}{b} \in \mathbb{Q}$ with $\left|\frac{a}{b}\right| \neq 1$. Since $|x| = |-x|$, we can assume $a, b \in \mathbb{Z}_{\geq 1}$. By multiplicativity,

$$\left|\frac{a}{b}\right| = \frac{|a|}{|b|} \neq 1 \implies |a| \neq |b|$$

and so we have $|a|, |b| \leq 1$ with $|a| \neq |b|$, so one of them must be strictly less than 1. So choose $n \in \mathbb{Z}_{\geq 1}$ with $|n| < 1$. We write n as a product of primes

$$n = p_0^{k_0} p_1^{k_1} \dots p_m^{k_m}$$

and since $|n| < 1$, it must be the case that $|p| < 1$ for some prime p dividing n. We claim that no other prime q can have absolute value less than 1. Suppose to the contrary that p, q are distinct primes with $|p|, |q| < 1$. Choose N large enough that $|p|^N, |q|^N < \frac{1}{2}$. Since $\gcd(p^N, q^N) = 1$, by the Euclidean algorithm/Bezout's identity there exist $s, t \in \mathbb{Z}$ so that

$$sp^N + tq^N = 1$$

Now we take absolute values, apply the triangle inequality, use the fact that $|p|^N, |q|^N < \frac{1}{2}$, and the fact that $|s|, |t| \leq 1$ by hypothesis, to get

$$1 = |1| = |sp^N + tq^N| \leq |sp^N| + |tq^N| = |s||p|^N + |t||q|^N < \frac{|s| + |t|}{2} \leq 1$$

which says $1 < 1$, a contradiction. Thus there is exactly one prime p so that $|p| < 1$, and for all other primes q, we have $|q| = 1$. Choose $a > 0$ so that $|p| = p^{-a}$. More concretely, set

$$a = -\frac{\log |p|}{\log p}$$

Now for $n \in \mathbb{Z}_{\geq 1}$, write n as $n = p^k n'$ where $\gcd(p, n') = 1$. Then

$$|n| = |p^k n'| = |p|^k |n'| = \left(p^{-a}\right)^k = \left(p^{-k}\right)^a = |n|_p^a$$

Thus $|\cdot|$ is equivalent to the p-adic absolute value.

(Case 2) Now we suppose there is some positive integer with absolute value greater than 1. We'll set this hypothesis aside for the moment, and come back to it. Let $m, n \in \mathbb{Z}_{\geq 2}$. We can write m as

$$m = a_0 + a_1 n + a_2 n^2 + \ldots + a_r n^r = \sum_{i=0}^{r} a_i n^i$$

for some integers a_i satisfying $0 \leq a_i < n$ and $n^r \leq m$. (All we did was write m in base n.) Note that

$$n^r \leq m \iff r \log n \leq \log m \iff r \leq \frac{\log m}{\log n} = \log_n m$$

(by log I mean natural log). Also note

$$|a_i| = |1 + \ldots + 1| \leq a_i|1| = a_i < n$$

Let $N = \max(1, |n|)$. Now we do a long string of estimates. The first comes from the triangle inequality, and the others come from our estimates above.

$$\begin{aligned} |m| &= \left|\sum_{i=0}^{r} a_i n^i\right| \leq \sum_{i=0}^{r} |a_i n^i| = \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} |a_i| N^r \leq \sum_{i=0}^{r} n N^r \\ &= (1+r) n N^r \leq (1 + \log_n m)\, n N^{\log_n m} \end{aligned}$$

Let t be a positive integer, and say we started with m^t and n instead, so we would instead get

$$|m|^t = |m^t| \leq \left(1 + \log_n m^t\right) n N^{\log_n m^t} = (1 + t \log_n m)\, n N^{t \log_n m}$$

Taking tth roots, this becomes

$$|m| \leq (1 + t\log_n m)^{\frac{1}{t}}\, n^{\frac{1}{t}} N^{\log_n m}$$

This inequality holds for all positive integers t, and

$$\lim_{t\to\infty} (1 + t\log_n m)^{\frac{1}{t}}\, n^{\frac{1}{t}} = 1$$

thus

$$|m| \leq \lim_{t\to\infty} (1 + t\log_n m)^{\frac{1}{t}}\, n^{\frac{1}{t}} N^{\log_n m} = N^{\log_n m}$$

Note that $N^{\log_n m} = \max\left(1, |n|^{\log_n m}\right)$. Finally, we go back to our hypothesis. Choose m so that $|m| > 1$, and use our inequality above to get

$$1 < |m| \leq \max\left(1, |n|^{\log_n m}\right) = |n|^{\log_n m} = |n|^{\frac{\log m}{\log n}}$$

We get the penultimate equality because if the max was 1, then we would have $1 < 1$, so this tells us that $|n| > 1$. Since n was arbitrary, we find that $|n| > 1$ for all positive integers n. Raising both sides to the $\frac{1}{\log m}$ power, we get

$$|m|^{\frac{1}{\log m}} \leq |n|^{\frac{1}{\log n}}$$

By symmetry between m and n, the reverse inequality also holds, so we get this equality for arbitrary $m, n \in \mathbb{Z}$, $m, n > 1$.

$$|m|^{\frac{1}{\log m}} = |n|^{\frac{1}{\log n}}$$

Thus there is a constant $c > 0$,

$$c = |n|^{\frac{1}{\log n}} \qquad \forall n \in \mathbb{Z}, n > 1$$

Then

$$|n| = c^{\log n} = e^{(\log c)(\log n)} = n^{\log c} = |n|_\infty^{\log c} \qquad \forall n \in \mathbb{Z}, n > 1$$

Thus $|\cdot|$ is equivalent to the standard absolute value on $\mathbb{Q}$ for positive integer, which makes it equivalent. $\square$

Remark: Ostrowski's Theorem can be generalized to arbitrary number fields (finite field extensions of $\mathbb{Q}$), but this requires more subltety to prove, so we just include it for cultural education here.

Theorem 1.4. *Let $|\cdot|$ be a nontrivial absolute value on a number field K, with ring of integers $\mathcal{O}_K$.*

- *If $|\cdot|$ is archimedean, then it is equivalent to the restriction of the complex norm on $\mathbb{C}$ to K for some embeddign $K \hookrightarrow \mathbb{C}$.*
- *If $|\cdot|$ is nonarchimedean, the it is equivalent to a $\mathfrak{p}$-adic valuation for a nonzero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.*

Proof. `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/ostrowskinumbfield.pdf` □

Remark: In the case $K = \mathbb{Q}$, this is exactly Ostrowski's Theorem, because there is only one embedding $\mathbb{Q} \to \mathbb{C}$, the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, and the nonzero prime ideals of $\mathbb{Z}$ are the principal ideals (p) for prime numbers p.

The generalization says that even for finite extensions of $\mathbb{Q}$, there are still only these two types of absolute values. However, there may be multiple distinct embeddings $K \hookrightarrow \mathbb{C}$, so there can be multiple classes of archimedean absolute values.

2 Completion of a field

One of the basic objects in real analysis is the Cauchy sequence, which in the case of a real sequence, is the same as a convergent sequences. However, the notion of a Cauchy sequence makes sense in any metric space, so we can speak of Cauchy sequences in a field with an absolute value.

Definition 2.1. Let K be a field with a nontrivial absolute value $|\cdot|$. A sequence (a_n) in K is a **Cauchy sequence** if for every $\epsilon > 0$ there exists $N > 0$ such that

$$m, n > N \implies |a_m - a_n| < \epsilon$$

The field K is **complete** if every Cauchy sequence in K has a limit in K. Two Cauchy sequences (a_n) and (b_n) are **equivalent** if

$$\lim_{n\to\infty} |a_n - b_n| = 0$$

Note that this is an equivalence relation.

Examples:

1. The field $\mathbb{Q}$ is not complete with respect to either $|\cdot|_\infty$ or with respect to any p-adic absolute value $|\cdot|_p$.
2. The fields $\mathbb{R}$ and $\mathbb{C}$ are both complete with respect to the usual absolute value $|\cdot|_\infty$.

Theorem 2.1. *Let K be a field with an absolute value $|\cdot|$. There exists a unique (up to isomorphism) field $\widehat{K}$ and an absolute value $|\cdot|$ on $\widehat{K}$ that extends the absolute value on K so that $\widehat{K}$ is complete.*

Furthermore, $\widehat{K}$ is universal in the following sense. If L is a complete valued field, and $\phi : K \to L$ is a homomorphism preserving the absolute value, then ϕ extends uniquely to a morphism $\widehat{\phi} : \widehat{K} \to L$ (that is, the following diagram commutes).

$$\begin{tikzcd}
\widehat{K} \arrow[r, dotted, "\widehat{\phi}"] & L \\
K \arrow[u, "\iota"] \arrow[ur, "\phi"'] &
\end{tikzcd}$$

Proof. We just sketch the proof. Define $\widehat{K}$ to be the space of Cauchy sequences in K, modulo equivalence, with term-by-term addition and multiplication. An element $x \in K$ is identified with the constant sequence $(x, x, x \ldots)$, which lets us think of K as a subfield of $\widehat{K}$. The extension property comes from sending a Cauchy sequence (a_n) to the limit of the sequence $(\phi(a_n))$, which is in L because L is complete, and ϕ preserves Cauchy-ness. Finally, uniqueness of $\widehat{K}$ is an immediate consequence of the universal property. $\square$

Remarks/exercises:

1. The completion of K with respect to two equivalent values gives two isomorphic fields.

2. The completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is $\mathbb{R}$.

3. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is the p-adic numbers, denoted $\mathbb{Q}_p$.

2.1 Series convergence

Here is another really strange property of nonarchimedean fields. Recall that we say a series converges if and only if the sequence of partial sums converges, and when this happens we call that limit the sum of the series. Also recall the first divergence test from Calculus 2:

$$\sum_{n=1}^{\infty} a_n \text{ converges} \implies \lim_{n\to\infty} a_n = 0$$

If only the converse were also true, then we wouldn't need the zoo of divergence tests that we learn in Calc 2, like the root test, the limit comparison test, and the limit ratio test. Well, check this out.

Proposition 2.2 (Milne Exercise 7-2)**.** *Let $|\cdot|$ be a nonarchimedean absolute value on a field K, and suppose that K is complete. A series in K converges if and only if the limit of the terms is zero.*

$$\sum_{n=1}^{\infty} a_n \text{ is convergent} \iff \lim_{n\to\infty} a_n = 0$$

Proof. The forward direction is always true (in any complete field), so we just need to show the backwards direction. Assume $\lim a_n = 0$. Thus for $\epsilon > 0$, there exists $N > 0$ so that $|a_n| < \epsilon$. We want to show that the sequence of partial sums converges. For $s, t > N$ with $s \leq t$, using the nonarchimedean triangle inequality, we get

$$\left|\sum_{n=1}^{s} a_n - \sum_{n=1}^{t} a_n\right| = \left|\sum_{n=s+1}^{t} a_n\right| \leq \max\left\{|a_n| : s+1 \leq n \leq t\right\} < \epsilon$$

Thus the sequence of partial sums is Cauchy, so the series converges. □

3 Additive valuations

In this section we define additive valuations on fields, which turn out to be pretty much the same as nonarchimedean absolute values, just written additively instead of multiplicatively. However, sometimes the additive notation is nicer. In particular, additive valuations have a close relationship with discrete valuations on rings, which are important for commutative algebra.

Definition 3.1. An **additive valuation** or just **valuation** on a field K is a function $v : K \to \mathbb{R} \cup \{\infty\}$ satisfying

$$\begin{aligned} &v(x) = \infty \iff x = 0 \\ &v(xy) = v(x) + v(y) \\ &v(x+y) \geq \min\left(v(x), v(y)\right) \end{aligned}$$

The second property may be rephrased as saying that v restricts to a group homomorphism $K^\times \to (\mathbb{R}, +)$.

Definition 3.2. The **trivial valuation** is $v(x) = 0$ for all $x \neq 0$; any other valuation is called **nontrivial**.

Definition 3.3. A valuation $v : K \to \mathbb{R} \cup \{\infty\}$ is **discrete** if the image is a discrete subgroup of of $\mathbb{R}$, which is to say that the image is of the form $s\mathbb{Z}$ for some $s \in \mathbb{R}$. A discrete valuation is **normalized** if $s = 1$.

Definition 3.4. Two valutaions v_1, v_2 on K are **equivalent** if there exists $s \in \mathbb{R}_{>0}$ so that $v_1 = sv_2$. Thus every discrete valuation is equivalent to a normalized discrete valuation.

The statement of the following theorem is an alternate statement of Theorem 2 of `https://www2.math.ethz.ch/education/bachelor/seminars/fs2008/algebra/Crivelli.pdf`.

Theorem 3.1. *Let K be a field. There is an equivalence-preserving bijection*

$$\begin{aligned} \{\text{nonarchimedean absolute values on } K\} &\longleftrightarrow \{\text{valuations on } K\} \\ |\cdot| &\mapsto \left(v(x) = \begin{cases} -\log|x| & x \neq 0 \\ \infty & x = 0 \end{cases}\right) \\ \left(|x| = \begin{cases} e^{-v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}\right) &\leftarrow\!\shortmid v \end{aligned}$$

Furthermore, discrete absolute values correspond to discrete valuations.

Proof. We just outline what needs to be checked. First, one should check that the image of a nonarchimedean absolute value is an additive valuation, and that the image of a valuation is a nonarchimedean absolute value, but this is immediate from the definitions. The log turns multiplicativity into additivity, and exp reverses this.

Note that the negative signs are not merely convention, but necessary, in translating the nonarchimedean triangle inequality into $v(x+y) \geq \min(v(x), v(y))$. It is also immediate that these maps are inverses. The fact that it preserves equivalence (and discreteness) is also immediate from the definitions. $\square$

Remark: All we're doing is using the group isomorphisms

$$(\mathbb{R}_{>0}, \times) \underset{\exp}{\overset{\log}{\rightleftarrows}} (\mathbb{R}, +)$$

3.1 Discrete valuation rings

In this section we generalize valuations to rings. Discrete valuation rings are important tools in algebraic number theory and algebraic geometry.

Definition 3.5. Let R be a commutative ring with unity. A **discrete valuation** on R is a function $v : R \to \mathbb{Z} \cup \{\infty\}$ satisfying

$$\begin{aligned} &v(x) = \infty \iff x = 0 \\ &v(xy) = v(x) + v(y) \\ &v(x+y) \geq \min(v(x), v(y)) \end{aligned}$$

A ring R that has a discrete valuation is called a **discrete valuation ring**.

Remark: There are many equivalent characterizations of DVRs. For exampe, a DVR can be characterized as a local PID.

Remark: If R is an integral domain, we can form its field of fractions $Q(R)$, and a discrete valuation on R extends uniquely to a valuation on $Q(R)$ by the multiplicative property. Thus we can transfer our classification of absolute values on $\mathbb{Q}$ to a classification of discrete valuations on $\mathbb{Z}$.

Corollary 3.2. *Every nontrivial discrete valuation $v : \mathbb{Z} \to \mathbb{Z} \cup \{\infty\}$ is equal to ord_p for some prime p.*

Proof. A nontrivial discrete valuation on $\mathbb{Z}$ induces a nontrivial, nonarchimedean absolute value on $\mathbb{Q}$, so it must be equivalent to $|\cdot|_p$ for some prime p by Ostrowski's Theorem. The absolute value $|\cdot|_p$ corresponds to

$$v(a) = -\log|a|_p = -\log|p^n a'|_p = -\log p^{-n} = n = \mathrm{ord}_p(a)$$

where $a = p^n a'$ and $\gcd(a', p) = 1$. $\square$

Definition 3.6. Let $|\cdot|$ be a discrete nonarchimedean absolute value on a field K, with corresponding normalized valuation v. Define

$$A = \{x \in K : |x| \leq 1\} = \{x \in K : v(x) \geq 0\}$$
$$U = \{x \in K : |x| = 1\} = \{x \in K : v(x) = 0\}$$
$$\mathfrak{m} = \{x \in K : |x| < 1\} = \{x \in K : v(x) > 1\}$$

Proposition 3.3 (cf Milne Prop 7.6)**.** *Let $A, U, \mathfrak{m}$ be as defined above. A is a subring of K which is a DVR, U is the group of units in A, and $\mathfrak{m}$ is the unique maximal ideal of A.*

Proof. A is closed under multiplication and addition by the properties of an absolute value, so it is a ring. It has discrete valuation v, so it is a DVR, so we know it has a unique nonzero ideal. Clearly $\mathfrak{m}$ is a nonzero ideal, so $\mathfrak{m}$ is the unique nonzero ideal. A unit must live in U, since if a unit u satisfies $|u| > 1$, then the inverse must satisfy $|u^{-1}| < 1$, but the u^{-1} is not in A. On the other hand, U contains all units of A, since if $u \in A$ is a unit with inverse $u^{-1} \in A$, then

$$|u||u^{-1}| = |1| = 1 \qquad 0 \leq |u|, |u^{-1}| \leq 1 \implies |u| = |u^{-1}| = 1$$

□

Example: Let K be an algebraically closed field, and let $K[x]$ be the polynomial ring in one variable. Then $K[x]$ is a UFD, the only irreducible elements are linear polynomials, and the only units are the (nonzero) constant polynomials. For each linear polynomial $\ell(x) = x - a$, define

$$\operatorname{ord}_\ell : K[x] \to \mathbb{Z} \cup \{\infty\} \qquad \operatorname{ord}_\ell(f) = n \qquad \ell^n | f \text{ and } \ell^{n+1} \not| f$$

This is a discrete valuation on $K[x]$. It extends to a discrete valuation on the fraction field $K(x)$, which corresponds to an absolute value on $K(x)$.

$$|\cdot| : K(x) \to \mathbb{R} \qquad \left|\frac{f}{g}\right| = e^{-\operatorname{ord}_\ell\left(\frac{f}{g}\right)}$$

Example: Using the setup of the previous example, take $K = \mathbb{C}$ for concreteness, and $\ell(z) = z - z_0$. Then $\operatorname{ord}_\ell(f)$ is just counting the order of the zero or pole of f at z_0. To get an idea of the resulting topology on $\mathbb{C}(z)$ induced by the absolute value corresponding to ord_ℓ, consider an ϵ-neighborhood of $0 \in \mathbb{C}(z)$, with $0 < \epsilon \ll 1$.

$$B(0, \epsilon) = \left\{\frac{f}{g} : f, g \in \mathbb{C}[z], e^{-\operatorname{ord}_\ell\left(\frac{f}{g}\right)} < \epsilon\right\}$$

Taking logs, the inequality becomes

$$-\operatorname{ord}_\ell\left(\frac{f}{g}\right) < \log \epsilon$$

For $0 < \epsilon \ll 1$, this says that

$$\operatorname{ord}_\ell\left(\frac{f}{g}\right) \gg 0$$

Assuming the fraction $\frac{f}{g}$ is reduced, this says that f is divisible by $(z - z_0)^N$ for $N \gg 0$. So a neighborhood of zero is rational functions which have sufficiently high order of vanishing at z_0.