Mini-course notes: p-adics

Jackie Lang

July 22, 2010

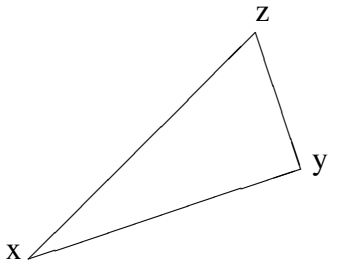
I would like to thank Dr. T.A. Fisher. These notes are based on some of his lectures given in 2009 at the University of Cambridge for the Local Fields Part III course.

This first goal of this talk is to extract some properties of distance. Just as we extract a reduced inventory for $\mathbb{Z}$ during the number theory class, we would like a short list of simple properties of distance that capture the essence of the idea from which we can prove many other facts.

What is distance? For any points x, y, z in our space (which we will later specify to be $\mathbb{Q}$ - the rational numbers) let $d(x, y)$ denote the distance between x and y. We would like d to satisfy the following properties:

1. $d(x, y) \geq 0$
2. $d(x, y) = 0 \iff x = y$
3. $d(x, z) \leq d(x, y) + d(y, z)$

The last condition is sometime called the *triangle inequality* because it captures the relationship between the lengths of the three sides of any triangle.



Distance functions are closely related to absolute values. In particular, if we have an absolute value on our space, we can get a distance function by defining $d(x, y) = |x - y|$ for any x, y in the space. We can rephrase the properties of distance using absolute values:

1. $|x| \geq 0$

2. $|x| = 0 \iff x = 0$

3. (Triangle Inequality) $|x + y| \leq |x| + |y|$

4. $|xy| = |x||y|$

Note that the last property of absolute values does not correspond to any of the properties of distance. It simply says that an absolute value should respect the multiplication on the space. We will let these four properties be our definition of absolute value for this talk. (That is, an *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}$ satisfying the above properties.)

Example 1. We can consider the usual absolute value on $\mathbb{Q}$, $\mathbb{Z}$ (the integers), $\mathbb{R}$ (the real numbers), $\mathbb{Z}[i]$ (the Gaussian integers), or $\mathbb{C}$ (the complex numbers). In these cases, the absolute value represents the Euclidean distance from zero (or the origin). It is standard notation to denote this ordinary Euclidean absolute value by $|\cdot|_\infty$, and we will adopt this convention for the remainder of these notes.

Example 2. Define $|\cdot|_t$ by

$$|x|_t = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

This is called the *trivial absolute value*. It is easy to check that $|\cdot|_t$ satisfies the four properties of an absolute value listed above.

Before we proceed to a theorem classifying absolute values on $\mathbb{Q}$, let us make some simple observations that can be deduced from the properties of an absolute value given above. Let $|\cdot|$ be any absolute value on a field K.

1. |1| = 1

   Proof. Since $|\cdot|$ is multiplicative, $|1| = |1^2| = |1|^2$ so by cancellation $1 = |1|$. □

2. $|a| = |-a|$ for all $a \in K$.

   Proof. Using the multiplicativity of $|\cdot|$ we have

   $$|a|^2 = |a^2| = |(-a)^2| = |-a|^2,$$

   so $|a| = \pm|-a|$. Since absolute values are always non-negative, it follows that $|a| = |-a|$ for all a. □

Table 1: Some Computations

p	$v_p(3/2)$	$\lvert 3/2\rvert_p$	$v_p(25/15)$	$\lvert 25/15\rvert_p$	$v_p(512)$	$\lvert 512\rvert_p$
2	-1	2	0	1	9	$1/512$
3	1	$1/3$	-1	3	0	1
5	0	1	1	$1/5$	0	1
47	0	1	0	1	0	1

For the remainder of this talk we will be concerned with absolute values defined on $\mathbb{Q}$.

Example 3. Fix a rational prime p. Take $x \in \mathbb{Q} \setminus \{0\}$, and use unique prime factorization to write $x = p^r \cdot \frac{u}{v}$ with $u, v, r \in \mathbb{Z}$ and $p \nmid uv$. Define the *valuation of x at p* to be $v_p(x) = r$. The *(normalized) p-adic absolute value* is

$$|x|_p = \begin{cases} \left(\frac{1}{p}\right)^{v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

See the above table for some examples of how the valuation and absolute value are computed for specific primes.

Is $|\cdot|_p$ an absolute value? Properties 1 and 2 are easy to check. Property 4 follows from the fact that $v_p(xy) = v_p(x) + v_p(y)$. For Property 3, write $x = p^{r_1} \cdot \frac{u_1}{v_1}$ and $y = p^{r_2} \cdot \frac{u_2}{v_2}$ with $u_i, v_i, r_i \in \mathbb{Z}$ and $p \nmid u_i v_i$. Then $v_p(x) = r_1$, $v_p(y) = r_2$, and $v_p(x+y) \geq \min\{r_1, r_2\}$. Thus

$$\begin{aligned} |x+y|_p = \left(\frac{1}{p}\right)^{v_p(x+y)} &\leq \left(\frac{1}{p}\right)^{\min\{r_1,r_2\}} = \max\left\{\left(\frac{1}{p}\right)^{r_1}, \left(\frac{1}{p}\right)^{r_2}\right\} \\ &= \max\left\{\left(\frac{1}{p}\right)^{v_p(x)}, \left(\frac{1}{p}\right)^{v_p(y)}\right\} = \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p, \end{aligned}$$

as desired.

Note that $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ for all $x, y \in \mathbb{Q}$. This property of an absolute value is called the *strong triangle inequality*. Any absolute value satisfying this property is called a *non-Archimedean absolute value*. Any absolute value that is not non-Archimedean is called *Archimedean*.

The following lemma was only stated as a fact in the talk due to time constraints, but we include a proof here.

Lemma 1. *An absolute value $|\cdot|$ on $\mathbb{Q}$ is non-Archimedean if and only if the set $\{|n| : n \in \mathbb{Z}\}$ has an upper bound.*

Proof. ($\Rightarrow$) Assume that $|\cdot|$ is a non-Archimedean absolute value on $\mathbb{Q}$. Since $|-n| = n$ we may assume without loss of generality that $n > 0$. Then $|n| = |\sum_{i=1}^{n} 1| \leq \max\{|1|\} = 1$. Hence $\{|n| : n \in \mathbb{Z}\}$ is bounded above by 1, as desired.

($\Leftarrow$) Suppose $|\cdot|$ is an absolute value on $\mathbb{Q}$ such that for some $B > 0$ we have $|n| \leq B$ for all $n \in \mathbb{Z}$. Let $x, y \in \mathbb{Q}$. Using the binomial theorem we have $(x+y)^m = \sum_{i=0}^{m} \binom{m}{i} x^{m-i} y^i$. Taking the absolute value of both sides yields

$$\begin{aligned} |x+y|^m &= \left| \sum_{i=0}^{m} \binom{m}{i} x^{m-i} y^i \right| \leq \sum_{i=0}^{m} \left| \binom{m}{i} \right| |x|^{m-i} |y|^i \\ &\leq \sum_{i=1}^{m} B \max\{|x|, |y|\}^m = (m+1) B \max\{|x|, |y|\}^m. \end{aligned}$$

Taking m-th roots of both sides yields

$$|x+y| \leq ((m+1)B)^{1/m} \max\{|x|, |y|\}$$

for all $m \in \mathbb{N}$. Using logarithms and L'Hopital's Rule (a theorem from calculus) one can check that $\lim_{m\to\infty}((m+1)B)^{1/m} = 1$. This implies that we must have $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in \mathbb{Q}$, so $|\cdot|$ is a non-Archimedean absolute value, as claimed. □

Definition 1. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on $\mathbb{Q}$ are said to be *equivalent*, denoted $|\cdot|_1 \sim |\cdot|_2$, if there is some $c > 0$ such that $|x|_1 = |x|_2^c$ for all $x \in \mathbb{Q}$.

Theorem 2 (Ostrowski)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p.*

Proof. Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$.

Case 1: $|\cdot|$ is Archimedean.

By Lemma 1 there is some $b \in \mathbb{Z}$ such that $|b| > 1$. Let $a \in \mathbb{Z}$ and write b^n in base a:

$$b^n = c_m a^m + c_{m-1} a^{m-1} + \cdots + c_1 a + c_0,$$

with $0 \leq c_i < a$. Let $B = \max\{c_0, \ldots, c_m\}$. Note that

$$n \log_a b = \log_a(b^n) = \log_a(c_m a^m + \cdots + c_0) \geq \log_a(a^m) = m.$$

Using these bounds we find that for any $n \in \mathbb{N}$

$$\begin{aligned} |b|^n &= |c_m a^m + \cdots + c_0| \leq |c_m||a|^m + \cdots + |c_0| \leq B|a|^m + \cdots + B \\ &= B(|a|^m + \cdots + 1) \leq B(m+1) \max\{|a|^m, 1\} \\ &\leq B(1 + n \log_a b) \max\{|a|^{n \log_a b}, 1\}. \end{aligned}$$

Thus for any $n \in \mathbb{N}$ we have

$$|b| \leq \sqrt[n]{B(1+n\log_a b)}\max\{|a|^{\log_a b}, 1\}.$$

Noting that $\lim_{n\to\infty}\sqrt[n]{B(1+n\log_a b)} = 1$ (a fact that requires a bit of analysis to prove) we find that $|b| \leq |a|^{\log_a b}$. Since $|b| > 1$ it follows that $1 < |a|$.

Now, the only difference between a and b in the above construction was that we knew that $1 < |b|$. As we now know that $1 < |a|$, it follows by symmetry that $|a| \leq |b|^{\log_b a}$. Taking logs of both $|a| \leq |b|^{\log_b a}$ and $|b| \leq |a|^{\log_a b}$ gives $\ln|b| \leq (\log_a b)\ln|a|$ and $\ln|a| \leq (\log_b a)\ln|b|$. Combining these yields

$$\ln|b| \leq \log_a b \log_b a \ln|b| = \ln|b|,$$

so in fact we must have $\ln|b| = (\log_a b)\ln|a| = \frac{\ln b}{\ln a}\ln|a|$. So we can define the constant

$$c = \frac{\ln|b|}{\ln b} = \frac{\ln|a|}{\ln a},$$

which we have just shown is independent of the integer a or b. Then for all $a \in \mathbb{N}$ we have $c\ln a = \ln|a|$ which implies that

$$|a|_\infty{}^c = a^c = |a|.$$

By the multiplicativity of $|\cdot|$ and the fact that $|-a| = |a|$ it follows that $|x|_\infty{}^c = |x|$ for all $x \in \mathbb{Q}$. Thus, $|\cdot|_\infty \sim |\cdot|$ as desired.

Case 2: $|\cdot|$ is non-Archimedean.

Note that for any $n \in \mathbb{Z}$ we have

$$|n| = |1+\cdots+1| \leq \max\{|1|,\ldots,|1|\} = |1| = 1.$$

Since $|\cdot|$ is non-trivial there is some $a \in \mathbb{Z}$ such that $|a| < 1$. Using unique prime factorization in $\mathbb{Z}$ we can write $a = p_1{}^{e_1}\cdots p_r{}^{e_r}$ where the p_i are distinct primes. Then

$$|a| = |p_1|^{e_1}\cdots|p_r|^{e_r}.$$

Since $|a| < 1$ there must be some i such that $|p_i| < 1$. Without loss of generality, say $i = 1$ and write $p = p_1$.

Suppose for contradiction that there is another prime q distinct from p such that $|q| < 1$. Choose $A, B \in \mathbb{Z}$ such that $|p|^A < 1/2$ and $|q|^B < 1/2$. As $(p,q) = 1$ we can use linear Diophantine equations to find $r, s \in \mathbb{Z}$ such that

$$rp^A + sq^B = 1.$$

Then

$$\begin{aligned} 1 = |1| = |rp^A + sq^B| &\leq \max\{|r||p|^A, |s||q|^B\} \\ &< \max\{|r|/2, |s|/2\} = 1/2 \max\{|r|, |s|\} \leq 1/2, \end{aligned}$$

which is a contradiction. Hence there exactly one prime (namely p) with $0 < |p| < 1$. So $|q| = 1$ for all primes $q \neq p$. Then

$$|a| = |p_1|^{e_1} \cdots |p_r|^{e_r} = |p_1|^{e_1} = |p|_p{}^{e_1 c} = |a|_p{}^c,$$

where $c = \ln |p| + \ln p$. Thus $|\cdot| \sim |\cdot|_p$, and this completes the proof. □

The following topics were not covered in the minicourse for time reasons, but it gives some insight into why p-adic absolute values are interesting. This mini-course is an introduction to the beautiful and useful theory of p-adic numbers - an important part of modern number theory. The following account is not meant to be precise or anywhere near complete, but it gives a brief account of the broader context of this talk.

Definition 2. A sequence $x_1, x_2, \ldots, x_n, \ldots$ of elements in $\mathbb{Q}$ is *Cauchy with respect to an absolute value* $|\cdot|$ if after some term N the terms are as close as desired (relative to $|\cdot|$).

Example 4. $1, 1/2, 1/4, 1/8, \ldots$ is Cauchy with respect to $|\cdot|_\infty$.
$1, i, -1, -i, 1, i, -1, -i, 1, \ldots$ is not Cauchy with respect to $|\cdot|_\infty$.
$1, p, p^2, p^3, p^4, \cdots$ is Cauchy with respect to $|\cdot|_p$, for any fixed prime p.

Definition 3. The *completion of* $\mathbb{Q}$ with respect to an absolute value $|\cdot|$ is the set of limit points of all points Cauchy sequences in $\mathbb{Q}$.

Example 5. $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$. For a fixed prime p, we let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

It turns out that equivalent absolute values give rise to the same completion, so Ostrowski's Theorem implies that $\mathbb{R}$ and $\mathbb{Q}_p$ for primes p are the only possible completions of $\mathbb{Q}$. Furthermore, these are all distinct completions.

A major question in number theory is the problem of how to find rational solutions to polynomial equations. These questions are easier to answer over complete fields like $\mathbb{R}$ and $\mathbb{Q}_p$. As $\mathbb{Q}$ is a subset of any completion of $\mathbb{Q}$ (just identify $a \in \mathbb{Q}$ with the constant Cauchy sequence $a, a, a, \ldots$), we can try to understand $\mathbb{Q}$ by understanding all completions of $\mathbb{Q}$. This philosophy of approaching a problem one prime at a time is known as the *Local Global* or *Hasse Principle*. Much of classical and modern number theory has shown that this is a great philosophy!