THE FIELD $\mathbb{Q}_p$ AND HOW IT IS DIFFERENT FROM $\mathbb{R}$

KENT SLINKER

Besides the fields $\mathbb{R}$ and $\mathbb{Q}$, there are many fields in Mathematics – other fields students are probably familiar with are the finite fields $\mathbb{Z}/p\mathbb{Z}$ for a particular prime number p and the field $\mathbb{C}$ of complex numbers. In what follows, we will examine how elements in $\mathbb{Q}_p$ are represented, and explore how distance between elements of $\mathbb{Q}_p$ is different from distances in $\mathbb{Q}$ by introducing the p-adic absolute value.

The easiest way to see how elements of a p-adic field $\mathbb{Q}_p$ are different is perhaps to see what the natural numbers look like in $\mathbb{Q}_p$ for a specific prime p. To make things easy, let's take as our prime $p = 5$, and recall what additive notation means in base 10. The number 24356 really is short-hand for:

$$2(10^4) + 4(10^3) + 3(10^2) + 5(10^1) + 6(10^0)$$

In other words, natural numbers in base 10 can be represented in the following way:

$$\sum_{i=0}^{\infty} a_i b^i$$

Where $b = 10$ and the a_i are taken from the list $(0, 1, 2, ..., 9)$ and all but a finite number of the a_i are 0. A natural number is represented p-adically in a similar way, with the important differences that the base b is always a prime p, the a_i are taken from the list $(0, 1, 2, ..., p-1)$, and the requirement that all but a finite number of the a_i be zero is dropped. Hence, in $\mathbb{Q}_5$ the base-10 number 24356 would look like ...001234411, or:

$$\ldots + 0(5^8) + 0(5^7) + 1(5^6) + 2(5^5) + 3(5^4) + 4(5^3) + 4(5^2) + 1(5^1) + 1(5^0)$$

By convention, we drop the leading zeros and just write, 1234411, or 1234411_5 if we need to specify that we are in $\mathbb{Q}_5$.

Addition, subtraction, multiplication are all carried out in $\mathbb{Q}_p$ exactly as they are done in the case with base 10, with the usual attention to how carries are to be treated in the particular base (e.g. in $\mathbb{Q}_5$ ...00123 + ...00123 = ...00301). To see how dropping the requirement that all but a finite number of the a_i be zero affects things, we will take an example of division. In particular, given that $\mathbb{Q}_p$ is a field, each element has a multiplicative inverse, in particular, we want to know what is the multiplicative inverse of 2 in $\mathbb{Q}_5$? In other words, what element of $\mathbb{Q}_5$ solves the equation $2x = 1$? Observe that

$$\begin{array}{r} \ldots 2222222222223 \\ +\underline{\ldots 2222222222223} \\ \ldots 0000000000001 \end{array}$$

So in $\mathbb{Q}_5$, the inverse of 2 is the infinite sequence $\ldots 22223$, or what amounts to saying the same thing, $\frac{1}{2} = \ldots 22223$ in $\mathbb{Q}_5$.

We have seen how natural numbers can be represented in $\mathbb{Q}_p$, but what about ratios of natural numbers? This is accomplished the following way, given $\frac{a}{b}$ where $a, b \in \mathbb{N}$ express $\frac{a}{b}$ in $\mathbb{Q}_p$ as, $p^{(\alpha-\beta)}\left(\frac{a_1}{b_1}\right)$ where α is the multiplicity of p in the numerator, and β is the multiplicity of p in the denominator, and p is not a factor of a_1 or b_1. For example in $\mathbb{Q}_5$ we would represent $\frac{36}{60}$ as $5^{(0-1)}\left(\frac{36}{12}\right)$. To make things complete, we need the expression for -1, which surprisingly is expressed as the infinite series:

$$-1 = \sum_{i=0}^{\infty}(p-1)p^i = \ldots p^3(p-1) + p^2(p-1) + p(p-1) + (p-1)$$

To avoid circularity in our definitions, the term $(p-1)$ is to be understood as the last digit in our list of a_i, namely $(0, 1, 2, ..., p-1)$. To see how this works, consider the above expression in $\mathbb{Q}_5$:

$$-1 = \sum_{i=0}^{\infty}(5-1)p^i = \ldots 4(5^3) + 4(5^2) + 4(5) + 4$$

Just as in the case above, where we discovered that $\frac{1}{2} = \ldots 22223$ in $\mathbb{Q}_5$, by adding 1 to $\ldots 44444$ in $\mathbb{Q}_5$ we obtain 0, hence $\ldots 44444$ is the additive inverse of 1 in $\mathbb{Q}_5$.

What follows from the above is that any element in $\mathbb{Q}$ has an expression in $\mathbb{Q}_p$, in other words there is an inclusion map from $\mathbb{Q}$ to $\mathbb{Q}_p$. This leads to the question as to whether all algebraic expressions have a solution in $\mathbb{Q}_p$? In $\mathbb{Q}$, the answer is clearly no, as $x^2 - 2 = 0$ has no solution in $\mathbb{Q}$. The same is true of $\mathbb{Q}_p$, for example the equation $x^2 - 2 = 0$ has no solution in $\mathbb{Q}_5$, but just like $\mathbb{Q}$, there is a completion of $\mathbb{Q}_p$ such that every algebraic equation has a solution and every Cauchy sequence converges. The proof of that completion requires knowledge of ring theory and is well beyond what might be done in a presentation of this type, but within grasp is the first step toward that proof which takes us to the fascinating world of non-Archimedean absolute values.

In general, an absolute value on any field $\mathbb{K}$ is a map from $\mathbb{K}$ to the non-negative real numbers such that the following three axioms hold:

(1) $|x| = 0$ if and only if $x = 0$
(2) $|xy| = |x|\,|y|$ for all $x, y \in \mathbb{K}$
(3) $|x + y| \leq |x| + |y|$

These are the properties of the absolute value that we all are familiar with, but if the absolute value on $\mathbb{K}$ has the additional property:

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

We say that the absolute value is non-Archimedean. Clearly our familiar absolute value on $\mathbb{R}$ does not obey property 4, to see this, just let x and y be any positive numbers. However we can define a non-Archimedean absolute value on $\mathbb{R}$ by the following:

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

This is called the trivial non-Archimedean absolute value, and is not of much interest, although for those who are familiar with finite fields might wish to prove that the only non-Archimedean absolute value on a finite field is the trivial one.

Let us define the p-adic absolute value and prove that it is non-Archimedean and consider a few interesting examples.

First, we should recall the Fundamental Theorem of Arithmetic which states if $x \in \mathbb{Z} \setminus \{0\}$, then x has a unique representation in the form:

$$x = \prod_{i=1}^{\infty} (-1)^n p_i^{\alpha_i}$$

Where $n \in \{0, 1\}$, and the p_i are distinct primes, and all but a finite number of the α_i are zero. With this in mind, let $n \in \mathbb{Z} \setminus \{0\}$ and define $v_p(n)$ as follows:

Definition 1. Let $v_p(x)$ be the unique non-negative number such that:

$$x = p^{v_p(x)} x'$$

Where p does not divide x'.

By using the fact that $p^\alpha p^\beta = p^{\alpha+\beta}$, it is easy to see that $v_p(ab) = v_p(a) + v_p(b)$ and $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.

In other words, the value of $v_p(x)$ represents the multiplicity of the prime p found in the rational number x. Here are some examples for various values of p:

x	$v_3(x)$	$v_7(x)$	$v_{13}(x)$
3	1	0	0
$\frac{1}{9} = \frac{1}{3^2}$	-2	0	0
$\frac{9}{21} = \frac{3}{7}$	1	-1	0
$49 = 7^2$	0	2	0
$371293 = 13^5$	0	0	5
$\frac{11025}{2197} = \frac{3^2 5^2 7^2}{13^3}$	2	2	-3

We now define the p-adic absolute value and prove that it is an example of an non-Archimedean absolute value.

Definition 2. For any $x \in \mathbb{Q} \setminus \{0\}$, fix a prime p. The **p-adic absolute value** of x, symbolized as $|x|_p$, is given to be 0 iff $x = 0$, otherwise we have:

$$|x|_p = p^{-v_p(x)}$$

Here are some examples:

x	$\lvert x\rvert_3$	$\lvert x\rvert_7$	$\lvert x\rvert_{13}$
3	$\frac{1}{3}$	1	1
$\frac{1}{9} = \frac{1}{3^2}$	9	1	1
$\frac{9}{21} = \frac{3}{7}$	$\frac{1}{3}$	7	1
$49 = 7^2$	1	$\frac{1}{49}$	1
$371293 = 13^5$	1	1	$\frac{1}{13^5}$
$\frac{11025}{2197} = \frac{3^2 5^2 7^2}{13^3}$	$\frac{1}{9}$	$\frac{1}{49}$	13^3

Now we need to prove that the p-adic absolute value is really a non-Archimedean absolute value. In other words, we need to show that the following properties hold:

(1) $|x| = 0$ if and only if $x = 0$
(2) $|xy| = |x|\,|y|$ for all $x, y \in \mathbb{K}$
(3) $|x + y| \leq |x| + |y|$
(4) $|x + y| \leq \max\{|x|, |y|\}$

To simplify our proof, we will first establish the following lemma:

Lemma. *For $x, y \in \mathbb{Z} \setminus \{0\}$, $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$*

We will divide our proof into 3 cases.

Proof. Case 1. Exactly one of x and y is a multiple of p.
Without loss of generality, assume x is a multiple of p. Then $x = kp^a$ for some integers k, α, where $\alpha \geq 1$ and p does not divide k. However $x + y = kp^a + y$ is not a multiple of p (otherwise we would have $kp^a + y = mp$ for some integer m, which implies $y = p(m - kp^{\alpha-1})$ contradicting our assumption that y is not a multiple of p). So $v_p(x + y) = 0 \geq \min\{\alpha, 0\} = \min\{v_p(x), v_p(y)\}$.

Case 2. x and y are both multiples of p.
Since x and y are both multiples of p, we have $x = kp^a$ and $y = mp^\beta$ for some integers k and m where p does not divide k or m. Without loss of generality, suppose $\alpha \leq \beta$, then $x + y = p^\alpha(k + mp^{\beta-\alpha})$, so $v_p(x + y) = v_p(p^\alpha(k + mp^{\beta-\alpha})) = \alpha \geq \min\{\alpha, \beta\} = \min\{v_p(x), v_p(y)\}$.

Case 3a. Suppose neither x or y are multiples of p, but $x + y$ is a multiple of p.

Suppose $x+y=kp^\alpha$, then $v_p(x+y)=v_p(kp^\alpha)=\alpha\geq\min\{0,0\}=\min\{v_p(x),v_p(y)\}$.

Case 3b. Suppose neither x or y are multiples of p, and $x+y$ is not a multiple of p.
We have $v_p(x+y)=0\geq\min\{0,0\}=\min\{v_p(x),v_p(y)\}$.

□

We are now ready to prove that $|x|_p$ is a non-Archimedean absolute value.

Proof. Let $x=\frac{a}{b}$, $y=\frac{c}{d}$ be two rational numbers. Property 1 follows from the definition of $|x|_p$. To prove property 2, observe:

$$\begin{aligned}|xy|_p &= \left|\left(\tfrac{a}{b}\right)\left(\tfrac{c}{d}\right)\right|_p\\ &= p^{-(v_p(ac)-v_p(bd))}\\ &= p^{-(v_p(a)+v_p(c)-v_p(b)-v_p(d))}\\ &= p^{-(v_p(a)-v_p(b)+v_p(c)-v_p(d))}\\ &= p^{-(v_p(a)-v_p(b))}p^{-(v_p(c)-v_p(d))}\\ &= \left|\tfrac{a}{b}\right|_p\left|\tfrac{c}{d}\right|_p\\ &= |x|_p\,|y|_p\end{aligned}$$

Since $|x+y|\leq\max\{|x|,|y|\}\leq|x|+|y|$, property 4 implies property 3, so we need only to show that property 4 holds.

We will use the property that if $a\geq\min(c,d)$ then $-a\leq\max(-c,-d)$.

Observe $\left|\frac{a}{b}+\frac{c}{d}\right|_p=\left|\frac{ad+cb}{bd}\right|_p=p^{-(v_p(ad+bc)-v_p(bd))}=p^{-(v_p(ad+bc)-v_p(b)-v_p(d))}$

By our previous lemma

$$v_p(ad+bc)\geq\min\{v_p(ad),v_p(bc)\}$$

so

$$\begin{aligned}-v_p(ad+bc)&\leq\max\{-v_p(ad),-v_p(bc)\}\\ &=\max\{-v_p(a)-v_p(d),-v_p(b)-v_p(c)\}\end{aligned}$$

Hence $\max\{-v_p(a)-v_p(d),-v_p(b)-v_p(c)\}+(v_p(b)+v_p(d))$ is either

$$\begin{aligned}&-v_p(a)+v_p(d)\quad\text{or}\\ &-v_p(c)+v_p(d)\end{aligned}$$

Therefore:

$$\begin{aligned}
\left|\tfrac{a}{b}+\tfrac{c}{d}\right|_p &= \left|\tfrac{ad+cb}{bd}\right|_p \\
&= p^{-(v_p(ad+bc)-v_p(bd))} \\
&= p^{-(v_p(ad+bc)-v_p(b)-v_p(d))} \\
&= p^{(-v_p(ad+bc)+v_p(b)+v_p(d))} \\
&\leq \max\left\{\left|\tfrac{a}{b}\right|_p, \left|\tfrac{c}{d}\right|_p\right\}
\end{aligned}$$

□

References

Gouvêa, Fernando. *p-adic Numbers, An Introduction.* Springer, 1997.

Madore, David A. "*A First Introduction to P-adic Numbers.*" Mathematics (old Page). David Madore, 7 Dec. 2000. Web. 28 Oct. 2012. <http://www.madore.org/~david/math/>