p-adic "geometry"

Notes by Aaryan Sukhadia, based off K.Sound's lectures.

SUMaC 2025 Research Projects

Contents

1 Introduction to / Refresher on Rings and Fields 2
2 Ostrowski's Theorem 5
3 $\mathbb{Q}_p$ and its topological properties 10
4 The p-adic integers 13
5 Geometry of $\mathbb{Q}_p$ 15

Section 1

Introduction to / Refresher on Rings and Fields

§1.1 Rings

Think about our old friend $\mathbb{Z}$, the integers. What can we do with integers? We can add and subtract them, and multiply them. We want to generalize this idea to a more broad structure that can apply to other mathematical objects, the same way we do for groups.

DEFINITION 1.1. A (commutative) **ring** R is a set equipped with two operations $+$ and $\cdot$ (addition and multiplication) such that:

1. $+$ and $\cdot$ are both commutative and associative.
2. Multiplication distributes over addition, i.e $r \cdot (s+t) = (r \cdot s) + (r \cdot t)$, for all $r, st \in R$.
3. There is a unique element $0 \in R$ that is an additive identity, i.e $0 + r = r, \ \forall r \in R$.
4. Every element $r \in R$ has a unique additive inverse $-r$ such that $r + (-r) = 0$.
5. There is a unique element $1 \in R$ that is a multiplicative identity (i.e $1 \cdot r = r, \ \forall r \in R$).

REMARK. There are some people who will say that it is not necessary that a ring have a multiplicative identity. We will ignore these people. It is also not necessary that all rings be commutative (i.e their multiplication can be non-commutative) – take the ring of invertible matrices, for example – but for our purposes it suffices to purely focus on commutative rings.

EXAMPLE 1.2 (Various Rings).
1. The integers $\mathbb{Z}$ form a ring. So do the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the complex numbers $\mathbb{C}$. (Note each example is a **subring** of the next)
2. The set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ form a ring.
3. The set integers modulo n, for any n, form a ring

EXAMPLE 1.3 (Various non-rings).
1. The naturals $\mathbb{N}$ don't form a ring (why? which of the rules break?)
2. The set of all functions $f : \mathbb{R} \to \mathbb{R}$ such that $f(1) = 1$ don't form a ring (why?)

Exercises

1. Show that in any ring we have $0 \cdot r = 0$ for any $r \in R$ (Note this isn't part of the definition of 0!!)

2. Show that in any ring we must have $(-1)\cdot(-1) = 1$ (work with the definition of -1 as the additive inverse of the multiplicative identity).

3. If $rs = 0$ for $r, s \neq 0$, then both r and s are called **zero-divisors**. Give an example of a ring with zero-divisors.

§1.2 Ideals

DEFINITION 1.4. An **ideal** I of a ring R is a subset such that:

- $0 \in I$
- For any $a, b \in I$, we have $a + b \in I$ (i.e I is additively closed)
- For any $a \in I, r \in R$, we have $ar \in I$ (i.e I is *totally* mutiplicatively closed, not just under multiplication by elements of I)

Notationally we often write $I \trianglelefteq R$ to indicate it is an ideal.

REMARK. By now in the Program 2 course you will have learned about normal subgroups. In particular, you have learnt that the kernel of every group homomorphism is a normal subgroup, and conversely every normal subgroup is the kernel of a group homomorphism. Ideals are exactly the extension of normal subgroups to rings (which is why they have similar notation!)

EXAMPLE 1.5 (Ideals).
- R itself is an ideal of R for any ring.
- The set $\{0\}$ is an ideal of R, for any ring.
- The set of multiples of n, for any $n \in \mathbb{Z}$, is an ideal of $\mathbb{Z}$. (We often use (n) to denote this ideal)

DEFINITION 1.6. An ideal is said to be **prime** if, for any $a, b \in R$ such that $ab \in I$, either $a \in I$ or $b \in I$

QUESTION. Does the definition of a prime ideal look familiar? Where might you have seen something similar before? Do exercise 2 of this chapter to make this idea rigorous.

§1.3 Exercises

1. Show that any ideal of $\mathbb{Z}$ is of the form (n) (i.e the set of all multiples of n).

2. Show that any prime ideal of $\mathbb{Z}$ must be of the form (p) for p prime or 0.
3. Suppose A is a subring of B, and let $\mathfrak{P} \trianglelefteq B$ be a prime ideal of B. Show that $\mathfrak{p} := \mathfrak{P} \cap A$ is a prime ideal of A.
4. Is the ideal (0) always a prime ideal for any ring? Why or why not?

§1.4 Fields

We've seen a ring generalizes the idea of having the operations of addition, subtraction and multiplication on a set. There's one more basic arithmetic operation we learn in elementary school that's missing here, and that's the gap that a field will fill in.

Definition 1.7. A **field** F is a ring such that every non-zero element $x \in F$ has a unique multiplicative inverse, i.e $\exists x^{-1}$ such that $x \cdot x^{-1} = 1$.

For example, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all fields, but $\mathbb{Z}$ is not.

§1.5 Exercises

1. Show that any finite ring with no zero-divisors is a field.
2. Show the only ideals of a field F are F itself and (0).

Section 2

Ostrowski's Theorem

Definition 2.1. A function $\alpha : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is called an **absolute value** if it satisfies the following 3 conditions:

1. (Non-degeneracy) We have $\alpha(x) = 0$ if and only if $x = 0$.
2. (Multiplicativity) For all $x, y \in \mathbb{Q}$ we have $\alpha(xy) = \alpha(x) \cdot \alpha(y)$.
3. (Triangle inequality) For all $x, y \in \mathbb{Q}$ we have $\alpha(x + y) \leq \alpha(x) + \alpha(y)$.

Exercise 2.A. Show any absolute value α satisfies

(a) $\alpha(1) = \alpha(-1) = 1$.

(b) $\alpha(n) \leq n$, for any positive integer n.

Example 2.2. The **trivial** absolute value is given by $x \mapsto 1$ for all $x \neq 0$.

Example 2.3. The standard absolute value on $\mathbb{Q}$, given by

$$|\cdot|(x) = \begin{cases} x, & x \geq 0 \\ -x, & x < 0 \end{cases}$$

is an absolute value function.

Exercise 2.B. Show that if α is an absolute value, then

$$\alpha^r : x \mapsto \alpha(x)^r$$

is also an absolute value for any $r \in [0, 1]$.

Essentially an absolute value gives us a notion to describe how "far away from 0" a rational number is. Numbers with a large absolute value are far away from 0, and those with a small absolute value are close to 0. We can make this precise in the following way.

Definition 2.4. For any absolute value function α on $\mathbb{Q}$, the **induced metric** on $\mathbb{Q}$ is given by

$$d(x,y) := \alpha(x-y)(= \alpha(y-x)).$$

Exercise 2.C. Show that the above definition is a valid metric (i.e satisfies the 3 relevant axioms) for any absolute value.

Sanity Check. What metric does the trivial absolute value induce? What topology is this on $\mathbb{Q}$?

Definition 2.5. The **real numbers** $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the metric induced by the standard absolute value.

Remark. There are other ways to define the real numbers, but this is perhaps in some sense the cleanest and the most intuitive: you take the rational numbers and "fill in the gaps", and the standard absolute value tells you exactly where the gaps are.

Example 2.6. Let p be a prime. For any $n \in \mathbb{Z} \setminus \{0\}$, we may write $n = p^a b$ such that $p \nmid b$. Then we may define $|n|_p := p^{-a}$ for any nonzero integer, and then define the p-**adic absolute value** as

$$|m/n|_p := \begin{cases} 0, & m = 0 \\ |m|_p / |n|_p, & m \neq 0 \end{cases}$$

for any $m/n \in \mathbb{Q}$.

Exercise 2.D. Prove that the function given in Example 2.6 is well-defined (i.e that the $a = |n|_p$ is well-defined and that the output of $x \in \mathbb{Q}$ is independent of choice of representation as m/n). Prove it is an absolute value. What are the numbers that are "far away from 0" with this absolute value, and what are the numbers "close to 0"?

Exercise 2.E. Show that the p-adic absolute value satisfies the following stronger version of the triangle inequality:

$$|x+y|_p \leq \max(|x|_p, |y|_p).$$

Definition 2.7. An absolute value satisfying the stronger triangle inequality outlined in 2.E is called **ultrametric**.

Exercise 2.F. If we ran the construction in Example 2.6 with a composite number instead of a prime p, would we get a well-defined absolute value? Why or why not?

In order to classify the absolute values in a more geometrically motivated way, we will want to distinguish them by the topologies that they induce on $\mathbb{Q}$.

Definition 2.8. We say two absolute values α, β on $\mathbb{Q}$ are **equivalent** if the metric induced by them on $\mathbb{Q}$ induces the same topology on $\mathbb{Q}$. A **valuation** on $\mathbb{Q}$ is an equivalence class of absolute values

Sanity Check. Check that this does indeed form an equivalence relation (i.e satisfies reflexivity, symmetry and transitivity).

Exercise 2.G. For any absolute value α and $r \in \mathbb{R} \setminus \{0\}$, show that α^r (defined in Exercise 2.B) is equivalent to α.

So we've seen a number of absolute values on $\mathbb{Q}$ now, some of them equivalent to one another. Our main result is that we have actually seen all of them.

Theorem 2.9 (Ostrowski). Any valulation on $\mathbb{Q}$ is represented by one of the following:

1. The trivial absolute value
2. The standard absolute value in Example 2.3.
3. The p-adic absolute value in Example 2.6, for some prime p.

Remark. This theorem tells us that the *only* possible notion of (nontrivial) distance on $\mathbb{Q}$ is either given by our standard geometric intuition as a subset of $\mathbb{R}$ (by Exercise 1.C) or some algebraic information corresponding to a prime number.

Proof outline. For any non-trivial absolute value α, the casework follows into one of two cases.

1. There exists at least one $n \in \mathbb{N}$ such that $\alpha(n) < 1$.
2. We have $\alpha(n) \geq 1$ for all $n \in \mathbb{N}$.

We will see that Case 1 corresponds to some power of the p-adic absolute value on $\mathbb{Q}$ for some prime p,, and that Case 2 corresponds to some power of the standard absolute value. You will cover the first case in Exercise 2.H and the second in Exercise 2.I. □

Exercise 2.H. Suppose we have some positive integer n with $\alpha(n) < 1$.

(a) Show there must exist some prime p with $\alpha(p) < 1$.

(b) For any integer b, show that there is a (unique) representation of b in "base p", i.e we can write

$$b = b_0 + b_1 p + \dots b_k p^k,$$

where each b_i is an integer in $[0, p-1]$.

(c) Applying the triangle inequality to the above (and using Exercise 2.A) , show that we must have

$$\alpha(b) \leq (k+1)(p-1) < \left(\frac{\log(b)}{\log(p)} + 1\right)(p-1).$$

(d) If we replace b with b^n, check that we get

$$\alpha(b)^n \leq \left(n\frac{\log(b)}{\log(p)} + 1\right)(p-1).$$

Deduce $\alpha(b) \leq 1$ (Hint: take the limit as $n \to \infty$).

(e) Let a be any integer coprime to p Show that, for any integer exponent n, we must have

$$1 \leq \alpha(a)^n + \alpha(p)^n$$

(Hint: use Bezout's identity and part (d)). By taking the limit as $n \to \infty$, deduce $\alpha(a) = 1$.

(f) Combine parts (b) and (e) to deduce α must be some power of the p-adic absolute value.

This completes Case 1: you have that if *any* natural number has absolute value less than one, then the only possible absolute value it can be must be a p-adic one.

Exercise 2.I. Suppose we have $\alpha(n) \geq 1$ for all positive integers. Let m, n be any positive integers ≥ 2.

(a) Following a similar process as in parts (c) and (d) of the previous Exercise, show that we have

$$\alpha(m) \leq \left(\frac{\log(m)}{\log(n)} + 1\right)(m-1)\alpha(n)^{\log(m)/\log(n)}.$$

(b) By a similar argument as in part (e) of the previous exercise, show we must have:

$$\alpha(m) \leq \alpha(n)^{\log(m)/\log(n)}.$$

(c) By swapping m and n, deduce we must have the equality

$$\alpha(m)^{1/\log(m)} = \alpha(n)^{1/\log(n)}.$$

Deduce for all n that $\alpha(n) = n^r$, for some $r \in \mathbb{R}$. Hence α is either trivial (if $r = 0$) or else equivalent to the standard absolute value on $\mathbb{Q}$, by 2.G.

This completes the second case. You've now classified all valuations on $\mathbb{Q}$!

Section 3

$\mathbb{Q}_p$ and its topological properties

Recall that if we have a metric space X with metric d then the **completion** of X (with respect to d) is the smallest complete metric space (X', d') containing X such that d' restricted to X is d. In Theorem 2.9, we saw that any non-trivial absolute value on $\mathbb{Q}$ that isn't (equivalent to) the stanadrd one must be (equivalent to) a p-adic absolute value for some prime p. We know the completion of $\mathbb{Q}$ with respect to the standard absolute value gives us the real numbers, so this motivates the following definition.

Definition 3.1. For p a prime number, the **p-adic field** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$.

Remark. There are no other completions of $\mathbb{Q}$ other than $\mathbb{R}$ or $\mathbb{Q}_p$ for p prime, since completing with respect to two different equivalent metrics gives the same completion.

In the proof of Theorem 2.9, we split it into two cases: one where the image of $\mathbb{Z}$ was bounded by 1 by the absolute value and one where it wasnt. This motivates the following definition.

Definition 3.2. An absolute value on an arbitrary field F is called **non-Archimedean** if the image of $\mathbb{Z} \to F$ is bounded, and **Archimedean** otherwise.

Remark. Speaking of *the* image of $\mathbb{Z}$ in F in the above definition makes sense, since for any ring R (which includes all fields!), there is a unique ring homomorphism $\mathbb{Z} \to \mathbb{R}$, since 0 has to map to 0, 1 has to map to 1, and $\mathbb{Z}$ is generated additively by 1.

Exercise 3.A (non-Archimdean = Ultrametric). Show that any absolute value $|\cdot|$ on any field F is non-Archimedean if and only if it is ultrametric (i.e we can use these terms interchangeably) via the following steps.

(a) Suppose $|\cdot|$ is ultrametric. Then, using the fact that the image of $\mathbb{Z}$ in F is generated by 1, show that the absolute value of the image of any $n \in \mathbb{Z}$ must be bounded.

(b) Suppose that $|\cdot|$ is non-Archimedean. Then use the binomial theorem, and by bounding the binomial coefficent by some global constant C, and thereby show that

$$|x+y|^n \leq (n+1)C \max(|x|, |y|)^n$$

for all $n \geq 1$. By taking the n-th root of both sides and the taking the limit as $n \to \infty$, show the ultrametric triangle inequality holds.

Thus, we may call $\mathbb{Q}_p$ a **non-Archimedean** field, since we've seen the p-adic absolute value is ultrametric.

Exercise 3.B (Closed balls are open). This exercise takes you through one of the core weird properties of $\mathbb{Q}_p$.

(a) Show for any non-Archimedean absolute value $|\cdot|$ on any field F that if $|x| \neq |y|$ then in fact
$$|x+y| = \max(|x|, |y|).$$
[**Hint:** Consider $y = (y+x) - x$.]

(b) Show that if $r > 0$ then and we have $a, a' \in F$ such that $|a - a'| \leq r$ then for any x we have $|x - a| \leq r$ if and only if $|x - a'| \leq r$.

(c) Define the closed ball of radius r centered at a in $\mathbb{Q}_p$ by
$$\overline{B_r(a)} := \left\{ x \in \mathbb{Q}_p : |x - a|_p \leq r \right\}.$$
As in any metric space, this is a closed set. Show *every* point in the ball is its center, i.e. $\overline{B_r(b)} = \overline{B_r(a)}$ for every $b \in \overline{B_r(a)}$.

(d) Deduce every closed ball in $\mathbb{Q}_p$ is open.

To understand more about the weirdness of this topology, we'll refresh a familiar concept in a bit more rigor.

Definition 3.3. A topological space X is **connected** if it *cannot* be written as the disjoint union of two open sets. A subset $A \subseteq X$ is said to be connected if it is connected in the subspace topology. X is said to be **path-connected** if for any $x, y \in X$ there exists a continuous function $f : [0,1] \to X$ (with the domain being given its standard Euclidean topology) such that $f(0) = x$ and $f(1) = y$.

Exercise 3.C (Path-Connected implies Connected). Let X be a path connected space. Show that X must also be connected. [**Hint**: Suppose $X = U \sqcup V$ a disjoint union of open sets, and consider a path between $x \in U$ and $y \in V$. By considering $f^{-1}(U)$ and $f^{-1}(V)$, derive a contradiction.]

Example 3.4. We know $\mathbb{R}$ is path-connected, so it is also connected. The same argument holds for any nice enough space, e.g S^n, $\mathbb{C}$, etc.

In most scenarios any connected set you work with will also be path-connected (there's only weird edge cases where you have spaces that connected but not path-connected. See the **topologist's sine curve** and **the deleted comb** if you're curious for examples.

DEFINITION 3.5. The **connected component** of a point $x \in X$ is the largest connected set that x is contained in. We say X is **totally disconnected** if the only connected components are singleton sets.

Intuitively, to be totally disconnected is to be as far away from being a connected space as topologically possible.

EXERCISE 3.D ($\mathbb{Q}_p$ is totally disconnected). Let C be a connected set containing a point $x_0 \in \mathbb{Q}_p$. Assume for the sake of contradiction $C \neq \{x_0\}$. Using this, express C has the disjoint union of the intersection of C with a closed (hence open, by 3.B!) ball and its complement. Deduce C cannot be connected, leading to a contradiction, and thus $\mathbb{Q}_p$ must be totally disconnected.

The above exercise shows a striking difference between completing $\mathbb{Q}$ with respect to its standard absolute value and any other. With one, you get a connected space $\mathbb{R}$, and completing with respect to any other you get a space as far away from being connected as possible!

Section 4

The p-adic integers

Definition 4.1. The **p-adic integers** $\mathbb{Z}_p$ is defined as the unit ball centered at 0 in $\mathbb{Q}_p$, i.e

$$\mathbb{Z}_p := \left\{ x \in \mathbb{Q}_p : |x|_p \leq 1 \right\}.$$

Warning. Some places use $\mathbb{Z}_p$ to mean $\mathbb{Z}/p\mathbb{Z}$. These are NOT the same thing, and one should ideally never use the former to refer to the latter. PROMYS and Ross Mathcamps unfortunately have not changed their ways.

Exercise 4.A. Show that $\mathbb{Z}_p$ is a ring. Show that $\mathbb{Z} \subseteq \mathbb{Z}_p$. Show that

$$\mathfrak{m}_p := \left\{ x \in \mathbb{Q}_p : |x|_p < 1 \right\}$$

is a maximal ideal of this ring.

Proposition 4.2. The canonical injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ is dense. In other words, for every $x \in \mathbb{Z}_p$ and $n \geq 1$ there exists some $z_n \in \mathbb{Z}$ such that $z_n \in [0, p^n - 1]$ and

$$|x - z_n|_p \leq p^{-n}.$$

The integer z_n with these properties is uniquely defined.

Proof. We have seen that any metric space is dense in its completion, so $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Thus for any $x \in \mathbb{Q}_p$ and any positive integer n we can find some rational $a/b \in \mathbb{Q}$ (let's say a, b are coprime) such that

$$|a/b - x|_p \leq p^{-n} (< 1).$$

However, the ultrametric triangle inequality in fact tells us we have

$$|a/b|_p \leq \max(|x|_p, |a/b - x|_p) \leq 1.$$

Examining the definition of the p-adic absolute value, we deduce $p \nmid b$. Thus there exists a (unique!) inverse of b modulo p^n, which we denote b'. In other words, we have

$$\begin{aligned} 1/b \equiv b' \mod p^n &\implies a/b \equiv ab' \mod p^n \\ &\implies |a/b - ab'|_p \leq p^{-n}. \end{aligned}$$

Using part (b) of Exercise 3.B, we deduce

$$\left| x - ab' \right|_p \leq p^{-n}.$$

Picking the unique integer $z_n \in [0, p^n - 1]$ such that $ab' \equiv z_n \mod p^n$, we get our desired properties. □

Exercise 4.B (Elements of $\mathbb{Q}_p$ as power series). Proposition 4.2 gives us, for every $x \in \mathbb{Z}_p$ a uniquely defined sequence of integers $\{z_n\}_{n\geq 1}$ such that $\left| x - z_n \right|_p \leq p^{-n}$.

(a) Check that $z_n \equiv z_{n+1} \mod p^n$ for all n.

(b) By writing each z_n in "base p" expansion, deduce that

$$x = b_0 + b_1 p + b_2 p^2 + \cdots,$$

for some integers $b_i \in [0, p-1]$. In particular, the RHS is a convergent sequence.

(c) Show that any element of $\mathbb{Q}_p$ can be written as $p^m x$ for some $m \in \mathbb{Z}$ and $x \in \mathbb{Z}_p$, and conclude that every element of $\mathbb{Q}_p$ has a (unique!) power series expansion of the form

$$x = \sum_{k \geq n} b_k p^k,$$

for some $n \in \mathbb{Z}$.

‘

Exercise 4.C ($\mathbb{Z}_p$ is compact). (a) Using the previous exercise, show that $\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z} / p^n \mathbb{Z}$.

(b) Deduce that every open cover of $\mathbb{Z}_p$ has a finite subcover. [**Hint:** It suffices to show that, for open balls of arbitrary small radius $\epsilon > 0$, that a finite number of them can cover $\mathbb{Z}_p$].
Remark. The property of a subset of a metric space being able to be covered by a finite number of arbitrarily small open balls is called being **totally bounded**. It is a (non-obvious) fact that in a complete metric space being totally bounded is equivalent to being compact).

(c) Conclude $\mathbb{Q}_p$ is **locally compact**, i.e every point has an open neighborhood whose closure is compact.

Section 5

Geometry of $\mathbb{Q}_p$

Exercise 5.A (Equidistant points). (a) Find a set of p points in $\mathbb{Q}_p$ all equidistant from one another.

(b) Show that no more than p distinct points in $\mathbb{Q}_p$ can be equidistant from one another. [**Hint:** Argue via contradiction. Use the (unique!) power-series expansions of elements of $\mathbb{Q}_p$].

Exercise 5.B. To show all the following properties, use the ultrametric triangle inequality.

(a) Prove that no 3 points in $\mathbb{Q}_p$ are collinear (i.e lie on the same line). Hint: Note that points x, y, z are collinear iff $d(x,z) = d(x,y) + d(y,z)$ (assuming y is "between" x and z)

(b) Prove all triangles in $\mathbb{Q}_p$ are isoceles i.e given any 3 points (which you have shown must be non-collinear!), there must be at least two of the distances between them that are the same.

(c) Prove there are no right-triangles in $\mathbb{Q}_p$ (i.e you can't pick 3 points such that the distances between them sastisfy the Pythagorean theorem)

Visualizing p-adics is really hard, since (as we've seen), they have super messed up geometric properties. Check out this website for a cool animation that takes a crack at it, however. Rotation corresponds to addition and scaling corresponds to multiplication.