A first course on p-adic numbers

Contents

Conventions

In these notes we take the following conventions:

- $\mathbf{N}$ denotes the set of non-negative integers.
- $\mathbf{Z}^+$ denotes the set of positive integers.
- The word "ring" means "unital commutative ring".
- Similarly, a "ring homomorphism" is a *unital* ring homomorphism, i.e. $1 \mapsto 1$.
- If A is a ring we write $A^\times$ for the group of units in A, so in particular if k is a field then $k^\times = k \setminus \{0\}$.

1 Week 1

1.1 Norms on fields

Definition 1.1. A *norm* (or *absolute value*) on a field F is a function $|\cdot| : F \longrightarrow \mathbf{R}^{\geqslant 0}$ such that for all $x, y \in F$

(i) $|x| = 0 \iff x = 0$,
(ii) $|xy| = |x|\,|y|$,
(iii) $|x + y| \leqslant |x| + |y|$.

If in place of (iii) we have the stronger condition

(iii)′ $|x + y| \leqslant \max\{|x|, |y|\}$,

then we say the norm is *nonarchimedean*; we call this condition (iii)′ the *nonarchimedean triangle inequality* (sometimes also referred to as the *ultrametric* triangle inequality, but we will not use this phrase).

If $|\cdot|$ is a [nonarchimedean] norm on F then we will refer to the pair $(F, |\cdot|)$ as a *[nonarchimedean] normed field*. We will also often just say phrases like "let F be a normed field", and allow our notation $|\cdot|$ for the norm on F to be understood from context.

Problem 1.2. Show condition (iii) in the definition of a norm implies $\left|\sum_{i=1}^{n} x_i\right| \leqslant \sum_{i=1}^{n} |x_i|$ for any $x_i \in F$. Show a similar result for the nonarchimedean triangle inequality (iii)′.

Remark 1.3. As a first example, notice that $\mathbf{R}$ with its usual absolute value, or $\mathbf{Q}$ with the absolute value from $\mathbf{R}$, are both examples of a field equipped with an absolute value. We will write the absolute value on $\mathbf{R}$ (and its restriction to $\mathbf{Q}$) by $|\cdot|_\infty$, for reasons to be discussed later.

Problem 1.4. For any field F, show the following function $|\cdot| : F \longrightarrow \mathbf{R}^{\geqslant 0}$ is a nonarchimedean norm (we call it the *trivial norm* on F):

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

Problem 1.5. Let $|\cdot|$ be a norm on a field F.

(a) Prove $|1| = 1$ and $|1/x| = 1/|x|$ for $x \in F^\times$.

(b) Prove $|-1| = 1$ and conclude $|-x| = |x|$ for any $x \in F$.
(c) More generally, if $x \in F$ satisfies $x^n = 1$ for some $n \in \mathbf{Z}^+$ then $|x| = 1$.
(d) Conclude if F is a finite field then any absolute value on F must be must be the trivial absolute value. [Hint: think about $F^\times$.]

Problem 1.6. Recall if X is a set then a *metric* (or *distance function*) on X is a function $d : X \times X \longrightarrow \mathbf{R}^{\geqslant 0}$ satisfying, for all $x, y, z \in X$

(i) $d(x, y) = 0 \iff x = y$,
(ii) $d(x, y) = d(y, x)$,
(iii) $d(x, z) \leqslant d(x, y) + d(y, z)$.

A *metric space* is a set equipped with a metric, i.e. a pair (X, d) where d is a metric on X. Show if $(F, |\cdot|)$ is a normed field then the function $d(x, y) := |x - y|$ is a metric. In this way every normed field is naturally a metric space.

Due to this problem we can transfer all definitions of metric spaces, i.e. open balls, open subsets, etc. to the setting of normed fields. We will lay out the explicit definitions here for both arbitrary metric spaces and for normed fields; if you are comfortable with the language of metric spaces this should be nothing new, and if you find the language of metric spaces concerning then you can just focus on the case of normed fields.

Definition 1.7. Let (X, d) denote a metric space.

- For $x_0 \in X$ and $r \in \mathbf{R}^{>0}$, the *open ball of radius r centered at* x_0 is the subset $B_r(x_0) := \{x \in X : d(x, x_0) < r\}$. In addition the *closed ball of radius r centered at* x_0 is the subset $\overline{B}_r(x_0) := \{x \in X : d(x, x_0) \leqslant r\}$.
- In the special case of a normed field $(F, |\cdot|)$, for $a \in F$ the open ball of radius r centered at a is the subset $B_r(a) := \{x \in F : |x - a| < r\}$, and similarly one has the closed ball of radius r centered at a given by $\overline{B}_r(a) = \{x \in F : |x - a| \leqslant r\}$.

Remark 1.8 (For those with background in topology). Beware that despite our notation $B_r(x)$ and $\overline{B}_r(x)$ for open and closed ball respectively, the subset $\overline{B}_r(x)$ is not always equal to the closure of $B_r(x)$ in X.

Definition 1.9. Let (X, d) denote a metric space.

- A subset $U \subseteq X$ is *open* if for every $x \in U$ there exists $r > 0$ such that $B_r(x) \subseteq U$. A subset $A \subseteq X$ is *closed* if its complement $X \setminus A$ is open.

- In the special case of a normed field $(F, |\cdot|)$, a subset $U \subseteq F$ is open if for every $a \in U$ there exists some $r > 0$ such that $B_r(a) \subseteq U$, i.e. $|x - a| < r \implies x \in U$.

Remark 1.10. Be aware: although the words "open" and "closed" would seem to suggest these are disjoint properties, one can in fact have subsets of metric spaces (or normed fields) which are both open and closed (one might use the word "clopen", but we will not). In fact we will see later that such examples always exist when the norm is nonarchimedean.

Notice the notion of open subset of X (resp. open subset of F) is very dependent on the choice of metric d (resp. the choice of norm $|\cdot|$). In other words, changing the metric may change the notion of open subset. Keep this in mind that although we will say phrases like "let U be an open subset of X", this depends on the given metric d on X.

Many things we will deal with in this course could be most nicely phrased in the language of topological spaces, so we will include a set of challenge problems that develop this language; these are not a requirement for understanding the core material, but consider doing them if you plan to take the 190 sequence at some point.

Challenge problem 1.11. Show that if (X, d) is a metric space then the following hold:

(i) the empty set $\emptyset$ and X itself are open subsets of X,
(ii) for any collection of open subsets $U_i \subseteq X$, the union $\bigcup_i U_i$ is open as well,
(iii) for two open subsets $U, V \subseteq X$, the intersection $U \cap V$ is also open.

Often for a metric space X (or a normed field k), conditions we consider only depend on which subsets of X (or of F) are open, rather than the actual metric. Other times it may happen that one wants a notion of "distance" which is not definable by any particular metric. For these reasons one considers topological spaces. Let us make the formal definition (compare with the previous problem):

Challenge definition 1.12. Let X be a set. A *topology* on X is a collection of subsets $\mathscr{T}$ of X (in other words, every element of $\mathscr{T}$ is a subset of X, so $\mathscr{T} \subseteq \mathcal{P}(X)$) satisfying the following conditions:

(i) $\emptyset, X \in \mathscr{T}$,
(ii) for any collection of subsets $U_i \in \mathscr{T}$, the union $\bigcup_i U_i$ is also in $\mathscr{T}$,
(iii) for two subsets $U, V \in \mathscr{T}$, the intersection $U \cap V$ is also in $\mathscr{T}$.

A *topological space* is a pair $(X, \mathscr{T})$ where $\mathscr{T}$ is a topology on X.

Notice by the previous problem, if (X, d) is a metric space then $\mathscr{T} = \{\text{open subsets of } X\}$ defines a topology on the set X. In other words, every metric space is a topological space in a natural way.

In any discussion of topological spaces, it is typical to encounter an abuse of language that many find confusing at first. That is the following: if $(X, \mathscr{T})$ is a topological space, we DEFINE a subset $U \subseteq X$ to be open if and only if $U \in \mathscr{T}$. This does NOT have any relevance to a specific metric, it is just a word to describe the condition $U \in \mathscr{T}$. One often then drops the notation $\mathscr{T}$ and uses phrases like "let X be a topological space and U an open subset of X".

Challenge problem 1.13. Let X be any set.

(i) Show that $\mathscr{T} = \mathcal{P}(X)$ is a topology on the set X. In other words, every subset of X is in $\mathscr{T}$. Put another way (with the language of the paragraph above), we are declaring that every subset of X be open. We call this topology the *discrete topology* on the set X; you should consider it something like a "trivial topology".

(ii) Prove that the discrete topolgy on X is the topology obtained if you start with the "trivial (or discrete) metric" on X:

$$d_{\text{triv}}(x, y) = \begin{cases} 0 & \text{if } x = y, \\ 1 & \text{if } x \neq y. \end{cases}$$

1.2 The p-adic norm

We will now turn our attention towards defining the p-adic norm on $\mathbf{Q}$. As a first step we have the following

Definition 1.14. Define a function $v_p : \mathbf{Z} \longrightarrow \mathbf{Z}$ as follows: given $a \in \mathbf{Z} \setminus \{0\}$, we can uniquely write $a = p^n m$ for $n \in \mathbf{Z}^{\geqslant 0}$ and $m \in \mathbf{Z}$ coprime to p, and we define $v_p(a) = n$; in other words $v_p(a)$ is the unique natural number n such that p^n divides a but p^{n+1} does not divide a. We also write $v_p(0) = \infty$.

We can extend this to a function $v_p : \mathbf{Q} \longrightarrow \mathbf{Z}$ as follows: we still take $v_p(0) = \infty$, and then if $x \in \mathbf{Q}^\times$ we write $x = a/b$ for $a, b \in \mathbf{Z}$, and then take $v_p(x) = v_p(a) - v_p(b)$. [Small exercise: show this is well-defined, i.e. if $a/b = c/d$ then $v_p(a/b) = v_p(c/d)$.

Another way one could describe this is to say that if we have $x \in \mathbf{Q}^\times$ then we write $x = p^n \cdot \frac{a}{b}$ for $a, b \in \mathbf{Z}$ which are coprime to p, then we take $v_p(x) = n$. Convince yourself internally this is the same as the above definition.

We call this function v_p the *p-adic valuation*; we do not yet know what a "valuation" is, we will sort this out in the next few problems.

Problem 1.15. Calculate $v_3(81)$, $v_7(\frac{1}{49})$, $v_2(\frac{14}{24})$ and $v_5(\frac{125}{4})$.

Remark 1.16. You should take this function as a measure of "how divisible by p" a given rational number is. For instance, large powers of p take large positive values under the p-adic valuation, and elements of the form $1/p^n$ take large negative values.

Definition 1.17. A *valuation* on F is a function $v : F \longrightarrow \mathbf{Z} \cup \{\infty\}$ satisfying, for all $x, y \in F$

(i) $v(x) = \infty \iff x = 0$,
(ii) $v(xy) = v(x) + v(y)$,
(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$.

Important problem 1.18. Prove that v_p (as in Definition 1.14) is a valuation on $\mathbf{Q}$.

The following problem shows that valuations lead to nonarchimedean absolute values:

Important problem 1.19. Let $v : F \longrightarrow \mathbf{Z}$ be a valuation on a field F, and fix a real number $0 < \rho < 1$. Prove the following is a nonarchimedean norm on F (with the convention $\rho^\infty = 0$):

$$|x| = \rho^{v(x)}.$$

[Remark: you are allowed to use the fact that the function $\mathbf{R} \longrightarrow \mathbf{R}$ sending $z \mapsto \rho^z$ is a strictly decreasing function.]

Definition 1.20. For the field of rational numbers $\mathbf{Q}$ and a prime number p, we let $|\cdot|_p$ denote the absolute value constructed in the previous problem by taking $v = v_p$ and $\rho = \frac{1}{p}$ (this choice of ρ is not that important, though it has one convenient aspect we will look at later). We call this the *p-adic norm*.

As an example, if we want to compute $|\frac{81}{12}|_3$, we write $\frac{81}{12} = 3^2 \cdot \frac{1}{4}$ and then $|\frac{81}{12}|_3 = 3^{-2} = \frac{1}{9}$.

Problem 1.21. Calculate $|\frac{250}{36}|_p$ for $p = 2, 3, 5$.

2 Week 2

2.1 Nonarchimedean normed fields

In this section we will focus on nonarchimedean normed fields, i.e. fields equipped with a nonarchimedean absolute value. One's first inclination might be that nonarchimedean absolute values are rare in comparison to "non-nonarchimedean" (i.e. "archimedean") norms, due to the nonarchimedean triangle inequality being a rather strong condition. Luckily this intuition proves to be incorrect; let us make this somewhat precise:

Problem 2.1. Let $|\cdot|$ be a norm on F.

(a) Prove that the following are equivalent:

(i) the norm $|\cdot|$ is nonarchimedean,
(ii) one has $|n{\cdot}1_F| \leqslant 1$ for all $n \in \mathbf{Z}$,
(iii) the set $\{|n{\cdot}1_F| : n \in \mathbf{Z}\}$ is a bounded subset of $\mathbf{R}$.

[Hint: the nontrivial implication is (iii) $\Longrightarrow$ (i). If $|n{\cdot}1_F| \leqslant C$ for all n, then for $x, y \in F$ we want to see that $|x + y| \leqslant \max\{|x|, |y|\}$. To this end, for any n use binomial expansion and the usual triangle inequality to obtain an inequality of the form $|x+y|^n \leqslant \sum_{i=0}^{n} |\binom{n}{i} x^i y^{n-i}|$, and conclude $|x+y|^n \leqslant (n+1)C \max\{|x|, |y|\}^n$. Take nth roots of both sides and then take the limit of both sides as $n \longrightarrow \infty$.]

(b) Conclude if F has characteristic p then any norm on F is nonarchimedean.

Less important problem 2.2. Let F be a nonarchimedean normed field.

(a) Prove if $r > 0$ and $a, b \in F$ with $|a - b| < r$, then $B_r(a) = B_r(b)$.
(b) Conclude open balls of equal radius are either disjoint or equal.

Problem 2.3. Let $|\cdot|$ be a nonarchimedean norm on a field F. Prove the following improvement upon the nonarchimedean triangle equality:

$$\text{If } x, y \in F \text{ with } |x| \neq |y|, \text{ then } |x + y| = \max\{|x|, |y|\}.$$

[Hint: suppose without loss of generality that $|x| < |y|$, and suppose we have strict inequality $|x + y| < \max\{|x|, |y|\} = |y|$. Then consider $|y| = |(x + y) - x|$.]

For the next problem recall the notion of closed subset as in Definition 1.9

Problem 2.4. Let F be a nonarchimedean normed field.

(a) Prove any open ball $B_r(a)$ is also closed. [Hint: one needs to show the complement $F \setminus B_r(a)$ is open. For this you need to take an arbitrary $x \in F \setminus B_r(a)$ and then find $r' > 0$ such that $B_{r'}(x) \subseteq F \setminus B_r(a)$; you can take $r = r'$ and get the desired inclusion by taking $y \in B_r(x)$ and writing $|y - a| = |(y - x) + (x - a)|$, then applying the previous problem.]

(b) Prove any closed ball $\overline{B}_r(a)$ for $r > 0$ is also open. [Hint: we need to show that if $x \in \overline{B}_r(a)$ then there exists $B_{r'}(x) \subseteq \overline{B}_r(a)$ for some $r' > 0$. You can take $r' = r$ and use a similar strategy as in part (a).]

The facts proved in the previous problem have an alternative proof in the language of topological groups; we will present these in a set of challenge problems.

One nice aspect of nonarchimedean normed fields is that they have a nice algebraic theory. Let us develop this a bit:

Definition 2.5. Let F be a nonarchimedean normed field. We define the *valuation ring* of F to be

$$\mathcal{O}_F := \{x \in F : |x| \leqslant 1\}.$$

We also define the *valuation ideal* of F to be

$$\mathfrak{m}_F := \{x \in F : |x| < 1\}.$$

We can justify these names due to the following problem:

Important problem 2.6. Prove that in the situation of Definition 2.5, the subset $\mathcal{O}_F$ is a subring of F and $\mathfrak{m}_F$ is an ideal of $\mathcal{O}_F$.

Remark 2.7. Notice that $\mathcal{O}_F = \overline{B}_1(0)$ and $\mathfrak{m}_F = B_1(0)$, so by Problem 2.4 both $\mathcal{O}_F$ and $\mathfrak{m}_F$ are both open and closed.

We can say a bit more algebraically about the subring $\mathcal{O}_F$: for this problem recall a *local ring* is a ring with a unique maximal ideal. One often says phrases like "let $(A, \mathfrak{m})$ be a local ring" to mean that A is a local ring with maximal ideal $\mathfrak{m}$.

Problem 2.8. Let F be a nonarchimedean normed field.

(a) Prove that if A is a ring and $\mathfrak{m}$ is an ideal of A, then A is a local ring with maximal ideal $\mathfrak{m}$ if and only if $A^\times = A \setminus \mathfrak{m}$.
(b) Prove that $\mathcal{O}_F^\times = \{x \in \mathcal{O}_F : |x| = 1\}$.
(c) Conclude $\mathcal{O}_F$ is a local ring with unique maximal ideal $\mathfrak{m}_F$.

Here is a problem for those who know what the field of fractions of an integral domain is:

Challenge problem 2.9. Show F is the field of fractions of $\mathcal{O}_F$.

Recall that an ideal $\mathfrak{m} \subseteq A$ is maximal if and only if $A/\mathfrak{m}$ is a field. In the case of a local ring $(A, \mathfrak{m})$, one often refers to the field $A/\mathfrak{m}$ as the *residue field of* A. As we have just proved, for a nonarchimedean normed field F, we have that $(\mathcal{O}_F, \mathfrak{m}_F)$ is a local ring, and we refer to $k_F := \mathcal{O}_F/\mathfrak{m}_F$ as the *residue field* of F.

Problem 2.10.

(a) Let F be any field equipped with the trivial norm. Calculate $\mathcal{O}_F, \mathfrak{m}_F$ and k_F.
(b) Consider $F := \mathbf{Q}$ equipped with the p-adic norm for a prime p. Describe $\mathcal{O}_F$ and $\mathfrak{m}_F$ as subsets of $\mathbf{Q}$. Show the residue field is isomorphic to $\mathbf{F}_p$. [Hint: you should have a natural map $\mathbf{Z} \longrightarrow \mathcal{O}_F$. Consider the composition $\mathbf{Z} \longrightarrow \mathcal{O}_F \longrightarrow k_F$.]

2.2 Sequences

Let us recall some basic definitions regarding sequences.

Definition 2.11. Let F be a normed field.

(i) A sequence $(x_n)_{n \geqslant 0}$ in F *converges* to $x \in F$ if for all $\epsilon > 0$ there exists $N > 0$ such that $|x_n - x| < \epsilon$ for all $n \geqslant N$. [Note: in this context you will often see the N suppressed, replaced by phrases like "$|x_n - x| < \epsilon$ for all sufficiently large n".] We will often denote this by $x_n \longrightarrow x$. A sequence $(x_n)_{n \geqslant 0}$ is *convergent* if it converges to some element.

(ii) We say a sequence $(x_n)_{n \geqslant 0}$ in F is *cauchy* if for all $\epsilon > 0$ there exists $N > 0$ such that $|x_n - x_m| < \epsilon$ for all $n, m \geqslant N$.

Problem 2.12 (Ignore if you do not care about using the language of metric spaces)**.** Generalize the above definitions of convergent/cauchy sequences to arbitrary metric spaces.

Problem 2.13.

(a) Let F be a field equipped with the trivial absolute value. Prove a sequence $(x_n)_{n\geqslant 0}$ in F converges if and only if it is eventually constant, i.e. if there exists N such that $x_N = x_{N+1} = x_{N+2} = \cdots$.
(b) Prove the sequence (p^n) converges to 0 in $(\mathbf{Q}, |\cdot|_p)$.

Problem 2.14. Let F be a normed field.

(a) Prove any convergent sequence is cauchy.
(b) Prove cauchy sequences are *bounded*, i.e. if $(x_n)_{n\geqslant 0}$ is a cauchy sequence then there exists some $M \in \mathbf{R}^{>0}$ such that $|x_n| \leqslant M$ for all n.

Problem 2.15. Let F be a normed field.

(a) Prove limits of convergent sequences are unique; in other words, prove if $(x_n)_{n\geqslant 0}$ is a sequence converging to both x and x', then $x = x'$. [Remark: this should rely heavily on the fact that $|x| \neq 0$ for $x \neq 0$.] For an extra challenge generalize your proof to arbitrary metric spaces.
(b) Let $A \subseteq F$ be a closed subset (see Definition 1.9). Suppose (x_n) is a sequence in F with $x_n \in A$ for all n. Prove if $x_n \longrightarrow x$ then $x \in A$. This can also be generalized to any metric space.

Challenge problem 2.16. Let F be a normed field.

(a) Prove a sequence (x_n) converges to x if and only if the following holds: for every open neighborhood U of x, there exists $N > 0$ such that $x_n \in U$ for all $n \geqslant N$.
(b) Formulate and prove an analogous condition for a sequence to be cauchy. [Hint: we no longer have the element x to take a neighborhood U of. Rather, take an open neighborhood U of 0 in your definition.]

This problem says that the definitions of convergent and cauchy can be stated purely in terms of open sets, i.e. makes sense in the language of topology. Indeed, the condition from (a) recovers the definition of "convergent sequence" one makes for topological spaces, and the condition from (b) is the definition of "cauchy" one makes for topological groups.

2.3 Continuity of field operations

Our goal for this section is to show that our various operations on a normed field F are actually continuous operations. First we must recall the definition of continuous:

Definition 2.17. Let (X, d_X) and (Y, d_Y) be metric spaces and $f : X \longrightarrow Y$ be a function.

- For a point $x_0 \in X$, we say that f is *continuous at* x_0 if for every $\epsilon > 0$, there exists some $\delta > 0$ such that $d(x, x_0) < \delta$ implies $d(f(x), f(x_0)) < \epsilon$. We say f is *continuous* if it is continuous at all points of X.
- In the special case of a function $f : F \longrightarrow F'$ between normed fields $(F, |\cdot|)$ and $(F', |\cdot|')$, we have that f is *continuous at* $a \in F$ if for all $\epsilon > 0$ there exists $\delta > 0$ such that, for all $x \in F$, $|x - a| < \delta$ implies $|f(x) - f(a)|' < \epsilon$, and f is *continuous* if it is continuous at all $a \in F$.

Problem 2.18. Consider two metric spaces (X, d_X) and (Y, d_Y). Prove the following function is a metric on $X \times Y$:

$$d : X \times Y \longrightarrow \mathbf{R}^{\geqslant 0}, \quad d((x, y), (x', y')) = \sqrt{d(x, x')^2 + d(y, y')^2}.$$

[Hint: you will use an inequality of the form $\sqrt{a + b} \leqslant \sqrt{a} + \sqrt{b}$, which can be seen by squaring both sides.]

We call this the *product metric* and refer to $(X \times Y, d)$ as the *product* of (X, d_X) and (Y, d_Y).

Remark 2.19. Also notice one other "operation" we have for metric spaces: if (X, d) is a metric space and $A \subseteq X$, then the restriction $d|_A : A \longrightarrow \mathbf{R}^{\geqslant 0}$ is also a metric, so A is naturally a metric space via $d|_A$.

If you do not wish to use the general language of metric spaces, just prove parts (a)-(b) of the following problem and read the statement of the other parts. In general, the proofs of the latter parts of the problem can be a bit tricky, and knowing the statements is more important than knowing the proofs.

Problem 2.20. Let $(F, |\cdot|)$ be a normed field; recall F is a metric space as in Problem 1.6.

(a) Prove that $|\cdot|$, considered as a function $|\cdot| : F \longrightarrow \mathbf{R}$, is continuous where $\mathbf{R}$ is given its usual structure as a metric space coming from its absolute value.
(b) Prove the "negation" function $F \longrightarrow F$, i.e. $x \mapsto -x$, is continuous.

(c) Prove that the addition function $F \times F \longrightarrow F$ is continuous, where we consider $F \times F$ to be a metric space as in Problem 2.18.
(d) Prove that multiplication is continuous as a function $F \times F \longrightarrow F$.
(e) Prove that inversion $F^\times \longrightarrow F^\times$, i.e. $x \mapsto x^{-1}$, is continuous, where we consider $F^\times$ a metric space as in Remark 2.19.

[Remark: these problems may be easier if you assume the norm to be nonarchimedean, and you are free to make this hypothesis if you wish.]

We can use the continuity of these operations to establish some facts about operations on sequences. We will do this using some facts about metric spaces; if you do not wish to use the language of metric spaces you may skip forward to Problem 2.22 and try to give direct proofs of the results. For those willing to use metric spaces, let us first establish the following facts:

Problem 2.21. Let (X, d_X) and (Y, d_Y) be metric spaces.

(a) Prove that if $f : X \longrightarrow Y$ is a continuous function, then for any convergent sequence $x_n \longrightarrow x$ in X we then have $f(x_n) \longrightarrow f(x)$ in Y.
(b) Prove if we are given convergent sequences $x_n \longrightarrow x$ and $y_n \longrightarrow y$ in X and Y, respectively, then $(x_n, y_n) \longrightarrow (x, y)$ in $X \times Y$.

Problem 2.22. Let $(F, |\cdot|)$ be a normed field and suppose we are given convergent sequences $a_n \longrightarrow a$ and $b_n \longrightarrow b$ in F.

(a) Using continuity of $|\cdot| : F \longrightarrow \mathbf{R}$, show that $\lim_{n\to\infty} |a_n| = |a|$.
(b) Using continuity of negation, prove $\lim_{n\to\infty}(-a_n) = -(\lim_{n\to\infty} a_n)$.
(c) Use the previous problem and continuity of addition to show $\lim_{n\to\infty}(a_n + b_n) = a + b$.
(d) Similarly, show $\lim_{n\to\infty}(a_n b_n) = ab$.
(e) Suppose $a \neq 0$. Show there is some N such that $a_n \neq 0$ for all $n \geqslant N$, and then show that the sequence $(a_n^{-1})_{n\geqslant N}$ converges to a^{-1}.

2.4 Challenge section: some topological notions

Challenge problem 2.23. Let X and Y be metric spaces and $f : X \longrightarrow Y$ be a function. Prove f is continuous if and only if for every open subset $V \subseteq Y$, the subset $f^{-1}(V) \subseteq X$ is also open. [Hint: for the forward direction, consider $x_0 \in f^{-1}(V)$. Because $f(x_0) \in V$

and V is open, we can find some $r > 0$ such that $B_r(f(x_0)) \subseteq V$. Take $\epsilon = r$ and apply the definition of f being continuous at x_0. In the reverse direction, if we want to show f is continuous at a point x_0, for an arbitrary $\epsilon > 0$ consider $V = B_\epsilon(f(x_0))$.]

The previous problem gives us a condition for continuity purely in terms of open sets, and it is the correct definition generalizing to arbitrary topological spaces. That is,

Challenge definition 2.24. If $(X, \mathscr{T}_X)$ and $(Y, \mathscr{T}_Y)$ are topological spaces then a function $f : X \longrightarrow Y$ is defined to be *continuous* if $V \in \mathscr{T}_Y$ implies $f^{-1}(V) \in \mathscr{T}_X$.

In the language one really uses in practice (see the discussion following Definition 1.12), we would say if X and Y are topological spaces, then a function $f : X \longrightarrow Y$ is *continuous* if for every open subset $V \subseteq Y$, the subset $f^{-1}(V) \subseteq X$ is also open.

The phenomenon we have observed in Problem 2.20, i.e. that the field F has a metric (or more generally a topology) with respect to which various operations are continuous, is a phenomenon we give a name to; first we just focus on the case of a (abelian) group:

Challenge definition 2.25. Let A be an abelian group equipped with a topology (i.e. in the most precise sense we are considering a trio $(A, +, \mathscr{T})$ such that $(A, +)$ is a group and $(A, \mathscr{T})$ is a topological space). We say that A is a *topological (abelian) group* if the operations of addition $A \times A \longrightarrow A$ and negation $A \longrightarrow A$ are both continuous, where for the former operation we consider $A \times A$ to have the *product topology*.

Remark 2.26. To work carefully with the above definition one needs to understand the definition of *product topology*. I will not give the definition here in full, if you are interested you should take a look at the book Topology by Munkres, you will first need to find the definition of a basis in §13 before reading the definition of product topology in §15. If you decide to do this you should prove as an exercise that the product metric in Problem 2.18 induces the product topology.

With this language we see that parts (b)-(c) of the previous problem tell us that a normed field F is a topological group for its natural topology as a metric space. We can take this a step further we like: given a ring A with a topology, if condition (b)-(d) holds one might say A is a *topological ring*, and then in the case A is a field, if (e) holds as well then we might say that A is a *topological field*. Thus the problem tells us that F is in fact a topological field for its natural topology.

In the following we prove some important facts about topological groups, and in particular we will obtain a purely "topological" proof of Problem 2.4.

Challenge problem 2.27. Let A be a topological (abelian) group.

(a) Prove that for any $a \in A$, the function $A \longrightarrow A$ defined by $x \mapsto a + x$ is continuous. [Hint: for a fixed $a \in A$, the function $A \longrightarrow A \times A$ defined by $x \mapsto (a, x)$ is continuous (where $A \times A$ has the product topology; you can take this fact for granted if you are not intimitely familiar with the product topology). Then try to write the function in question as a specific composition of continuous functions.]

(b) Prove that if $a \in A$ and U is an open subset of A, then U is open (resp. closed) if and only if $a + U$ is open (resp. closed) where $a + U = \{a + x : x \in U\}$. [Hint: U is exactly the pre-image of $a + U$ under the continuous function from (a).]

(c) Prove that any open subgroup of a topological group is closed. [Hint: if $H \subseteq A$ is an open subgroup, then write $A \setminus H$ as a union of cosets, each of which is open by (b).]

(d) Conclude if F is a nonarchimedean field then any open ball $B_r(a)$ is closed. [Hint: prove that $B_r(a) = a + B_r(0)$ and use part (b) to reduce to the case of $a = 0$; then use part (c).]

3 Week 3

3.1 Sequences and series in the nonarchimedean/complete cases

Definition 3.1. A normed field F (or more generally a metric space X) is *complete* if every cauchy sequence converges.

Problem 3.2. Suppose (X, d) is a complete metric space. Show that if $A \subseteq X$ is a closed subset then $(A, d|_A)$ is a complete metric space (see Remark 2.19). [Hint: use Problem 2.15.]

Problem 3.3.

(a) Let $|\cdot|_{\text{triv}}$ denote the trivial norm on a field F. Prove $(F, |\cdot|_{\text{triv}})$ is complete.
(b) Let $p \geqslant 5$ be a prime and choose an integer $1 < a < p - 1$. Prove $(\mathbf{Q}, |\cdot|_p)$ is not complete by proving the sequence $(a^{p^n})_{n\geqslant 0}$ is cauchy but not convergent. [Hint: suppose the sequence has a limit $x \in \mathbf{Q}$. First notice using Fermat's little theorem that $a^{p^n} \in B_1(a)$ for each n. Then use Problems 2.4 and 2.15 to deduce $x \in B_1(a)$, i.e. $|x - a|_p < 1$. Now use the fact that $z \mapsto z^p$ is a continuous map with respect to $|\cdot|_p$ to deduce $x^p = x$. Show $x \neq 0$ so $x^{p-1} = 1$, and then because $x \in \mathbf{Q}$ conclude $x = \pm 1$. Use the fact $|x - a|_p < 1$ to show neither is possible by our choice of a.]

Definition 3.4. Let F be a normed field. Recall a *series* in F is an "infinite sum", i.e. an of the form $\sum_{n=0}^{\infty} a_n$ where $a_n \in F$. We say the series $\sum_{n=0}^{\infty} a_n$ *converges* to $a \in F$ if the sequence of partial sums $s_n = \sum_{i=0}^{n} a_i$ converges to a. Similarly, the series is *cauchy* if the sequence of partial sums is cauchy.

Problem 3.5. Let F be a normed field. Prove if a series $\sum_{n=0}^{\infty} a_n$ is cauchy then $a_n \longrightarrow 0$. [Hint: consider the sequence s_n of partial sums, and notice that $a_n = s_n - s_{n-1}$.]

The converse to the above statement is not true over arbitrary (complete) normed fields, a typical example is the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$ which does not converge in $\mathbf{R}$ even though its terms tend to zero. We will show in the following problems that such behavior cannot happen in the nonarchimedean case.

Problem 3.6. Let F be a nonarchimedean normed field. Prove a sequence $(x_n)_{n\geqslant 0}$ in F is cauchy if and only if the following property holds: for every $\epsilon > 0$ there exists $N > 0$ such that $|x_{n+1} - x_n| < \epsilon$ for all $n \geqslant N$.

Problem 3.7. Let F be a nonarchimedean normed field.

(a) Prove a series $\sum_{n=0}^{\infty} a_n$ is cauchy if and only if $a_n \longrightarrow 0$.
(b) Conclude if F is complete then $\sum_{n=0}^{\infty} a_n$ converges if and only if $a_n \longrightarrow 0$.
(c) Prove as a corollary if F is complete, then any "absolutely convergent" series converges, i.e. for a series $\sum_{n=0}^{\infty} a_n$, if the series $\sum_{n=0}^{\infty} |a_n|$ converges in $\mathbf{R}$ then the original series converges in F.

Problem 3.8. Suppose F is a nonarchimedean normed field. Prove if the series $\sum_{n=0}^{\infty} a_n$ converges then

$$\Big|\sum_{n=0}^{\infty} a_n\Big| \leqslant \max_{n\geqslant 0}\big\{|a_n|\big\}.$$

Problem 3.9. Suppose F is a nonarchimedean normed field. Prove if $\sum_{n=0}^{\infty} a_n = a$ and $\sum_{n=0}^{\infty} b_n = b$, then then for $c_n := \sum_{i+j=n} a_i b_j$, the sum $\sum_{n=0}^{\infty} c_n$ is convergent with value ab.

3.2 Constructing the completion

Let F be a normed field. We will show that there is a "completion" of F, i.e. a "smallest complete normed field containing F"; the word "smallest" here is not strictly meaningful, but we will come up with a universal property to characterize completions, and deduce the completion is "unique" in a sense. Before we get into these more abstract viewpoints, let us first construct the completion.

Throughout the rest of this section let $(F, |\cdot|)$ denote a fixed normed field.

Problem 3.10. Take for granted (or prove if you like) that the set of sequences in F, i.e. $F^{\mathbf{N}} = \{(a_0, a_1, \cdots) \mid a_n \in \mathbf{N}\}$, is a ring under component-wise addition and multiplication, i.e. with the operations

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots), \quad (a_0, a_1, \dots)(b_0, b_1, \dots) = (a_0 b_0, a_1 b_1, \dots).$$

Let $\mathscr{C}$ denote the subset of F consisting of cauchy sequences.

(a) Show if $(a_0, a_1, \dots)$ and $(b_0, b_1, \dots)$ are cauchy sequences, then $(a_0 + b_0, a_1 + b_1, \dots)$ is also a cauchy sequence. Notice that $(0, 0, \dots)$ is a cauchy sequence, and deduce that $\mathscr{C}$ is an additive subgroup of $F^{\mathbf{N}}$.

(b) Similarly, show the product of two cauchy sequences is cauchy. Notice that $(1, 1, \dots)$ is a cauchy sequence and conclude that $\mathscr{C}$ is a (unital) subring of $F^{\mathbf{N}}$. [Hint: for $m \geqslant n$ write $a_m b_m - a_n b_n = (a_m b_m - a_m b_n) + (a_m b_n - a_n b_n)$, and use the fact that cauchy sequences are bounded, i.e. Problem 2.14(b).]
(c) Let us say a sequence $(a_n)_{n\geqslant 0}$ is a *null sequence* if $a_n \longrightarrow 0$. Let $\mathscr{N}$ denote the set of null sequences, and notice that $\mathscr{N} \subseteq \mathscr{C}$. Prove $\mathscr{N}$ is an ideal of $\mathscr{C}$.

The field for our completion will be $\mathscr{C}/\mathscr{N}$; we need to prove this is in fact a field.

Problem 3.11. In this problem we prove $\mathscr{C}/\mathscr{N}$ is a field. Notice two cauchy sequences $(a_n)_{n\geqslant 0}$ and $(b_n)_{n\geqslant 0}$ are equal in $\mathscr{C}/\mathscr{N}$ if and only if $a_n - b_n$ converges to 0. If $(a_n)_{n\geqslant 0} \in \mathscr{C}$ let us write $[(a_n)_{n\geqslant 0}]$ for the associated element of $\mathscr{C}/\mathscr{N}$.

(a) Notice if $(a_n)_{n\geqslant 0}$ is a sequence and $N > 0$ is fixed, then $(a_n)_{n\geqslant 0}$ is cauchy if and only if the sequence $(a_{n+N})_{n\geqslant 0}$ is cauchy. Prove in this case we have $[(a_n)_{n\geqslant 0}] = [(a_{n+N})_{n\geqslant 0}]$.
(b) Suppose we have an element $(a_n)_{n\geqslant 0} \in \mathscr{C} \setminus \mathscr{N}$. Prove there exists some $C > 0$ and $N > 0$ such that $|a_n| \geqslant C$ for all $n \geqslant N$.
(c) Let (a_n) be as in the previous part. Define a sequence $(b_n)_{n\geqslant 0}$ by

$$b_n = \begin{cases} 0 & \text{if } n < N, \\ \frac{1}{a_n} & \text{if } n \geqslant N. \end{cases}$$

Prove $(b_n)_{n\geqslant 0}$ is a cauchy sequence. [Hint: let C be as in part (b). For $\epsilon > 0$ you can take some N' such that $|a_n - a_m| < \epsilon C^2$ for all $n, m \geqslant N'$. Do some algebra and use the fact that $|a_n| > C$ for $n \geqslant N$ to prove that $|\frac{1}{a_n} - \frac{1}{a_m}| < \epsilon$ for all $n, m \geqslant \max(N, N')$.]
(d) Prove $[(b_n)_{n\geqslant 0}]$ is an inverse for $[(a_n)_{n\geqslant 0}]$ in $\mathscr{C}/\mathscr{N}$. Conclude $\mathscr{C}/\mathscr{N}$ is a field.

At this point we will start writing $\widehat{F} := \mathscr{C}/\mathscr{N}$, which is a field. We next need to define the norm on $\widehat{F}$.

Problem 3.12.

(a) Prove if $(a_n)_{n\geqslant 0}$ is a cauchy sequence in F then $(|a_n|)_{n\geqslant 0}$ is a cauchy sequence in $\mathbf{R}$, and conclude $\lim_{n\to\infty} |a_n|$ exists in $\mathbf{R}$.
(b) Show defining $\|\cdot\| : \widehat{F} \longrightarrow \mathbf{R}^{\geqslant 0}$ by $\|[(a_n)_{n\geqslant 0}]\| := \lim_{n\to\infty} |a_n|$ is well-defined.
(c) Prove $\|\cdot\|$ is a norm on $\widehat{F}$.

Thus we see that $(\widehat{F}, \|\cdot\|)$ is a normed ring. If we are going to refer to this as the "completion of F" we should start by relating it to F:

Problem 3.13. Let us define $i : F \longrightarrow \widehat{F}$ by taking $x \in F$ to the equivalence class of the constant (cauchy) sequence $(x, x, x, \dots)$.

(a) Prove that $i : F \longrightarrow \widehat{F}$ is an injective ring homomorphism satisfying $\|i(x)\| = |x|$ for $x \in F$.
(b) Prove that if $|\cdot|$ is nonarchimedean then $\|\cdot\|$ is also nonarchimedean. [Hint: for a slick proof use Problem 2.1.]

Now our final task is to show that $(\widehat{F}, \|\cdot\|)$ is actually complete! Otherwise calling it the "completion" would be nonsensical. Let us begin with a slight digression:

Definition 3.14. A subset S of a normed field K is *dense* if for every $x \in K$ and $\epsilon > 0$, there exists some $a \in S$ such that $|x - a| < \epsilon$. In other words $B_\epsilon(x) \cap S \neq \emptyset$ for any $x \in K$ and $\epsilon > 0$. [Note this definition extends to metric spaces as well.]

Problem 3.15. Let $i : F \longrightarrow \widehat{F}$ be as in Problem 3.13. Prove that i identifies F with a dense subset of $\widehat{F}$, i.e. prove that for any $x \in \widehat{F}$ and $\epsilon > 0$ there exists some $a \in F$ such that $\|x - i(a)\| < \epsilon$. [Hint: write $x = [(a_n)_{n\geqslant 0}]$ and apply the hypothesis that (x_n) is cauchy to $\epsilon' = \epsilon/2$. For whatever N you get, let $a = x_N$.]

With this we are in a better position to prove $\widehat{F}$ is complete.

Important problem 3.16. Let $(x_n)_{n\geqslant 0}$ be a cauchy sequence in $\widehat{F}$.

(a) For each n, use Problem 3.15 to choose $a_n \in F$ such that $\|x_n - i(a_n)\| < 1/n$, so that $(x_n - i(a_n))_{n\geqslant 0}$ is a null sequence in $\widehat{F}$.
(b) Conclude $(i(a_n))_{n\geqslant 0}$ is a cauchy sequence in $\widehat{F}$. Use this to show that $(a_n)_{n\geqslant 0}$ is a cauchy sequence in F, so we can consider the element $x := [(a_n)_{n\geqslant 0}] \in \widehat{F}$. [Hint: Problem 3.13.]
(c) Prove that $(i(a_n))_{n\geqslant 0}$ converges to x in $\widehat{F}$, and conclude that $x_n \longrightarrow x$ as well. [Hint: you may want to use Problem 2.22(c) for the second part.]
(d) Conclude $\widehat{F}$ is complete.

Thus we have a complete normed field $(\widehat{F}, \|\cdot\|)$, which is nonarchimedean when $(F, |\cdot|)$ is. We refer to $(\widehat{F}, \|\cdot\|)$ as the *completion* of $(F, |\cdot|)$. When the norm on F is known from context we often just say that $\widehat{F}$ is the completion of F, and one often uses the same symbol to denote the norms on $\widehat{F}$ and F; due to part (a) of the previous problem this does not cause too much harm.

With this done we finally define the p-adic numbers:

Definition 3.17. For a prime p, we define the *p-adic numbers*, denoted $\mathbf{Q}_p$, to be the completion of $(\mathbf{Q}, |\cdot|_p)$.

We also define the *p-adic integers*, denoted $\mathbf{Z}_p$, to be the valuation subring of $\mathbf{Q}_p$, i.e. $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x| \leqslant 1\}$.

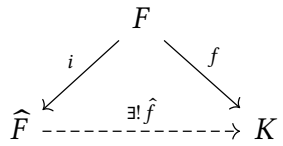
By Problem 3.13 and Problem 3.16, the p-adic numbers are a complete nonarchimedean normed field. Next week we will look at alternative descriptions of the elements.

3.3 Universal property of completion

In this section we describe a "universal property" for completions. For the proof we will need a general lemma, which we prove before starting the proof of the main result:

Problem 3.18. Suppose S is a dense subset of a normed field E (see Problem 3.14), and $f, g : E \longrightarrow E'$ are continuous functions to another normed field E' such that $f|_S = g|_S$, then $f = g$ on all of E. [Hint: if $x \in E$, for each $n \in \mathbf{N}$ take $\epsilon = 1/n$ to obtain a corresponding element $x_n \in S$ as in the definition of dense subset. Conclude (x_n) is a sequence converging to x, and use continuity (Problem 2.21) to show that $y_n := f(x_n) = g(x_n)$ is a sequence which converges to both $f(x)$ and $g(x)$, then use uniqueness of limits (Problem 2.15(a)) to conclude $f(x) = g(x)$.] Note: the corresponding for metric spaces holds as well with the analagous proof.

Important problem 3.19 (Universal property of completion)**.** We prove the natural map $i : F \longrightarrow \widehat{F}$ satisfies the following property: if K is a complete normed field (let's write the norm on K as $|\cdot|_K$) and $f : F \longrightarrow K$ is a continuous field homomorphism, then there exists a unique continuous field homomorphism $\hat{f} : \widehat{F} \longrightarrow K$ such that $f = \hat{f} \circ i$. One often summarizes this with the following "commuting diagram":



(a) Given a cauchy sequence $(a_n)_{n\geqslant 0}$ in F, show that $(f(a_n))_{n\geqslant 0}$ is also a cauchy sequence in K, so then this sequence has a limit in K (necessarily unique by Problem 2.15(a)).

(b) Prove the resulting function $\mathscr{C} \longrightarrow K$ taking $(a_n)_{n\geqslant 0}$ to $\lim_{n\to\infty} f(a_n)$ is a ring homomorphism. Notice every null sequence maps to 0 under this homomorphism, so

it induces a ring homomorphism $\hat{f} : \widehat{F} \to K$. [Hint: for the first part you should be using continuity of field operations on K to prove the limits will commute with addition/multiplication.]

(c) Prove $\hat{f}$ is continuous and that $f = \hat{f} \circ i$; this gives us the existence of $\hat{f}$. [Hint: first prove if $x \in \widehat{F}$ then $|\hat{f}(x)|_K = \|x\|$. Then use this to show that $|f(x) - f(a)|_K = \|x - a\|$ for any $x, a \in \widehat{F}$, and decude $\widehat{F}$ is continuous.]

(d) Use Problem 3.18 and Problem 3.15 to prove uniqueness of $\hat{f}$. That is, prove if $g : \widehat{F} \to K$ is a continuous field homomorphism satisfying $f = g \circ i$, prove $g = \hat{f}$. [Hint: take $E = \widehat{F}$ and $S = i(F)$ in Problem 3.18.]

One thing we can quickly prove with the universal property is that a map between normed fields induces a map between the completions:

Problem 3.20. Let $f : F \to F'$ be a continuous homomorphism between normed fields. Prove there is a unique coninuous homomorphism $\hat{f} : \widehat{F} \to \widehat{F'}$ which "extends" f, i.e. we have the commutative diagram

$$\begin{array}{ccc} F & \xrightarrow{f} & F' \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i'} \\ \widehat{F} & \xrightarrow{\exists! \hat{f}} & \widehat{F'} \end{array}$$

[Hint: apply the universal property of completion to the composition $F \to F' \to \widehat{F'}$.]

We also have the following "uniqueness" consequence of the universal property:

Challenge problem 3.21. Prove the completion pair $(\widehat{F}, i)$ is "unique up to unique isomorphism": i.e. prove that if (F', i') is a pair with F' a complete normed field and $i' : F \to F'$ a continuous homomorphism satisfying the universal property of the completion of F, then there exists exactly one isomorphism $\varphi : \widehat{F} \to F'$ such that φ and φ^{-1} are both continuous and $\varphi \circ i = i'$. [Hint: use the existence part of the univeral property of completion to find continuous homomorphisms $\varphi : \widehat{F} \to F'$ and $\psi : F' \to \widehat{F}$ satisfying $i' = \varphi \circ i$ and $i = \psi \circ i'$. Use the uniqueness part of the universal property to prove $\varphi \circ \psi = \mathrm{id}_{F'}$ and $\psi \circ \varphi = \mathrm{id}_{\widehat{F}}$.

4 Week 4

4.1 Ostrowski's theorem

In this section we attempt to make precise the fact that $\mathbf{R}$ and $\mathbf{Q}_p$ (for varying primes p) are the "only" completions of $\mathbf{Q}$.

Definition 4.1. An norm on a field F is *trivial* if it is equal to the trivial norm. Otherwise the norm is *nontrivial*.

We will define what it means for two norms to be "equivalent". We start with an example of what two "equivalent" norms might look like (we will end up showing that this is the only way two equivalent norms can occur):

Less important problem 4.2. Let $|\cdot|$ be a norm on a field F.

(a) Let $0 < \alpha \leqslant 1$ be a real number. Prove that $|\cdot|^\alpha$ (i.e. the function $x \mapsto |x|^\alpha$) is also a norm on F. [Hint: the only issue is the triangle inequality; we need to know that $(a+b)^\alpha \leqslant a^\alpha + b^\alpha$ holds. Notice this is trivial if a or b is zero, so suppose without loss of generality $a \geqslant b > 0$, and reduce to show the inequality $(t+1)^\alpha \leqslant t^\alpha + 1$ for all $t \geqslant 1$. For this, notice it is true at $t = 1$ and use calculus to prove the inequality remains true for all $t > 1$.]

(b) Suppose now the norm $|\cdot|$ is nonarchimedean. Prove that $|\cdot|^\alpha$ is a nonarchimedean norm for any $\alpha > 0$.

Problem 4.3. Let $|\cdot|$ and $|\cdot|'$ be two norms on a field F. Consider the following conditions (all will end up being equivalent):

(i) there exists some $\alpha > 0$ such that $|\cdot|' = |\cdot|^\alpha$, i.e. $|x|' = |x|^\alpha$ for all $x \in F$,
(ii) for a sequence (x_n) in F one has $x_n \longrightarrow x$ for $|\cdot|$ if and only if $x_n \longrightarrow x$ for $|\cdot|'$,
(iii) for $x \in F$ one has $|x| < 1 \iff |x|' < 1$.

(a) Prove (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). [Hint: for (i) $\Longrightarrow$ (ii), if $x_n \longrightarrow x$ for $|\cdot|$ then for $\epsilon > 0$ find that $|x_n - x| < \epsilon^t$ for sufficiently large n, and deduce $|x_n - x|' < \epsilon$ for such n. To prove (ii) $\Longrightarrow$ (iii) consider the sequence (x^n).]

(b) Prove (iii) $\Longrightarrow$ (i) in the following steps;

(1) Show (iii) $\Longrightarrow$ (i) when either norm is trivial, so we can assume both norms are nontrivial.
(2) Prove if $x \in F$ then $|x| > 1 \iff |x|' > 1$ and $|x| = 1 \iff |x|' = 1$.
(3) Prove it suffices to find some value of t such that $|x|' = |x|^t$ when $|x| > 1$. Conclude it suffices to prove that $\frac{\log|x|'}{\log|x|}$ is a constant value for all $|x| > 1$.
(4) Let $x, y \in F$ such that $|x|, |y| > 1$ and suppose (without loss of generality) $\frac{\log|x|'}{\log|x|} < \frac{\log|y|'}{\log|y|}$. Show there are positive integers a, b satisfying $\frac{\log|x|'}{\log|y|'} < \frac{a}{b} < \frac{\log|x|}{\log|y|}$. Prove the element $z = x^b/y^a \in F$ satisfies $|z|' < 1$ but $|z| > 1$ and conclude the result.

Definition 4.4. We say that two norms $|\cdot|$ and $|\cdot|'$ on a field F are *equivalent* if they satisfy the equivalent conditions of Problem 4.3.

Challenge problem 4.5. Show the following condition can be added to the list of equivalent conditions from Problem 4.3:

(iv) the norms $|\cdot|$ and $|\cdot|'$ define the same open subsets of F (in fancy terms they *induce the same topology* on F).

[Hint: it probably would be easiest to prove that (i) $\Longrightarrow$ (iv) $\Longrightarrow$ (ii).]

Less important problem 4.6. Show if a norm on F is equivalent to the trivial norm, then that norm is equal to the trivial norm. Thus we do not need to worry about any sort of equivalence conditions in Definition 4.1.

The following is the statement of Ostrowski's Theorem:

Theorem 4.7 (Ostrowski)**.** Let $|\cdot|$ be a nontrivial norm on $\mathbf{Q}$. If $|\cdot|$ is archimedean (i.e. if $|\cdot|$ is not nonarchimedean) then it is equivalent to $|\cdot|_\infty$, and if $|\cdot|$ is nonarchimedean then it is equivalent to $|\cdot|_p$ for some prime p. Thus, up to equivalence, the only norms on $\mathbf{Q}$ are the trivial norm, the usual norm, and the p-adic norms for varying p.

Problem 4.8. Read the proof of Ostrowski's theorem, there is a link on the course website.

Problem 4.9. Prove if $|\cdot|$ and $|\cdot|'$ are equivalent norms on F, then the completions of $(F, |\cdot|)$ and $(F, |\cdot|')$ are isomorphic. [Hint: use the universal property of completion.]

Combining the problem with Ostrowski's theorem, we see that $\mathbf{R}$ and $\mathbf{Q}_p$ (for varying p) are indeed, up to isomorphism, the only nontrivial completions of $\mathbf{Q}$. As an extra remark, we notice that the norms $|\cdot|_p$ on $\mathbf{Q}$ are indeed distinct for distinct primes p:

Problem 4.10. Show if $p \neq q$ are primes then $|\cdot|_p$ is not equivalent to $|\cdot|_q$.

Note this does not actually imply immediately that $\mathbf{Q}_p \neq \mathbf{Q}_q$ for $p \neq q$; next week we will have an easy way to see this.

In number theory a recurring theme is the so-called *local-global principle*. Vaguely, a local-global principle is something like the following: fix an equation (think something like $x^n + y^n = z^n$) and let $P(F)$ be be the statement that our equation has (nontrivial) solution in the field F. Then we say the local-global principle is satisfied if the following holds:

$$P(\mathbf{Q}) \text{ is true if and only if } P(\mathbf{R}) \text{ is true and } P(\mathbf{Q}_p) \text{ is true for all primes } p.$$

Clearly a solution over $\mathbf{Q}$ leads to a solution over each completion, so the question we are asking is really the following: can solutions over $\mathbf{R}$ and $\mathbf{Q}_p$ (these are the so-called "local" solutions) in some way "glue" to a solution over $\mathbf{Q}$?

Next section we will give our first example of a local-global principle (see Problem 4.14). For now we content ourselves with the following (sometimes quite useful) observation about how the varying norms on $\mathbf{Q}$ interact pleasantly. Recall for this problem that we denote the usual absolute value on $\mathbf{Q}$ (i.e. the one coming from $\mathbf{R}$) by $|\cdot|_\infty$, and let $\mathbb{P}$ denote the set of prime numbers:

Problem 4.11 (Product formula)**.** Prove that if $x \in \mathbf{Q}^\times$ then

$$\prod_{p \in \mathbb{P} \cup \{\infty\}} |x|_p = 1.$$

4.2 Some algebraic aspects of $\mathbf{Q}_p$

Before we begin this section we make one extra remark about completions of nonarchimedean normed fields. We make the following definition:

Definition 4.12. If $(F, |\cdot|)$ is a normed field we write $|F^\times| = \{|x| : x \in F^\times\}$; notice this is a subgroup of $\mathbf{R}^{>0}$. This is sometimes referred to as the *value group* of F.

Problem 4.13. Prove if $(F, |\cdot|)$ is a nonarchimedean normed field and $(\widehat{F}, \|\cdot\|)$ is the completion, one has

$$|F^\times| = \|\widehat{F}^\times\|.$$

[Hint: one inclusion is clear from Problem 3.13. On the other hand if you have $x \in \widehat{F}^\times$, using density choose $a \in F^\times$ such that $\|x - i(a)\| < \|x\|$. Then apply Problem 2.3.]

Recall we've defined the p-adic numbers, denoted $\mathbf{Q}_p$, as the completion of $\mathbf{Q}$ for the p-adic norm $|\cdot|_p$. We also let $|\cdot|_p$ denote the norm on $\mathbf{Q}_p$, and we consider $\mathbf{Q}$ as a subset of $\mathbf{Q}_p$ via the injecive homomorphism from Problem 3.13. We see that we can apply the above result to the p-adic numbers, and so we have

$$|\mathbf{Q}_p^\times|_p = |\mathbf{Q}^\times|_p = \{p^{-n} : n \in \mathbf{Z}\}.$$

Thus we see that for every $x \in \mathbf{Q}_p^\times$ we have $|x|_p = p^{-n}$ for some $n \in \mathbf{Z}$. If we write $v_p(x) = n$ for this choice of n, and write $v_p(0) = \infty$ as before, we see that the p-adic valuation extends to $v_p : \mathbf{Q}_p \to \mathbf{Z}$ in a natural way (notice it agrees with our original definition of p-adic valuation for $x \in \mathbf{Q}$). As a small detour, we notice this allows us to give our first local-global principle:

Problem 4.14.

(a) Prove if $x \in \mathbf{Q}^\times$ then $x = \pm \prod_{p \in \mathbb{P}} p^{v_p(x)}$.
(b) Let $x \in \mathbf{Q}$. Prove that x is a square in $\mathbf{Q}$ if and only if x is a square in $\mathbf{R}$ and in $\mathbf{Q}_p$ for every prime p. [Hint: the case $x = 0$ is trivial; if $x \neq 0$ and x is a square in $\mathbf{Q}_p$ for each p, then conclude that $v_p(x)$ is even for each p, and then consider the formula above, notice that $x > 0$ because x is a square in $\mathbf{R}$.]

Now returning to our discussion of algebraic aspects of $\mathbf{Q}_p$, notice also from the previous discussion that $|p| = p^{-1}$ generates the value group of $\mathbf{Q}_p$. From this statement we can get quite a bit of mileage in describing how elements of $\mathbf{Q}_p$ look. We will make a general statement for any nonarchimedean normed field F. If necessary, go back and review the definitions of $\mathcal{O}_F$ and $\mathfrak{m}_F$ as in Definition 2.5.

Problem 4.15. Let F be a nonarchimedean normed field.

(a) Prove if $x, y \in \mathcal{O}_F$ then $x\mathcal{O}_F \subseteq y\mathcal{O}_F \iff |x| \leqslant |y|$.
(b) Prove we have $|x| = |y|$ if and only if there exists $u \in \mathcal{O}_F^\times$ such that $x = yu$.
(c) Prove every finitely generated ideal of $\mathcal{O}_F$ is principal.

For the following problem recall a ring is Noetherian if every ideal is finitely generated (many sources may use a different initial definition, but a typical first result is that it is equivalent to this definition).

Problem 4.16. Let F be a nonarchimedean normed field such that the norm is nontrivial. Prove the following are equivalent:

(i) $\mathcal{O}_F$ is Noetherian,
(ii) $\mathfrak{m}_F$ is a principal ideal (say generated by π),
(iii) $|F^\times|$ is cyclic (say generated by $|\pi|$ for $\pi \in \mathfrak{m}_F$),
(iv) there exists an element $\pi \in \mathfrak{m}_F$ such that every element of $F^\times$ can be written uniquely in the form $\pi^n u$ for some $n \in \mathbf{Z}$ and $u \in \mathcal{O}_F^\times$,
(v) there exists an element $\pi \in \mathfrak{m}_F$ such that every nonzero ideal I of $\mathcal{O}_F$ can be written as $I = \pi^n \mathcal{O}_F$ for some $n \in \mathbf{Z}^{\geqslant 0}$.

Moreover, the same π can be taken for conditions (ii)-(v). [Hint: for (i) $\implies$ (ii) and (iii) $\implies$ (iv) use the previous problem. To prove uniqueness in (iv), if one has $\pi^n u = \pi^m v$ for some $n, m \in \mathbf{Z}$ then one can deduce $n = m$ by looking taking the norm, and then one deduces $u = v$ easily. For (iv) $\implies$ (v) let $N = \min\{n \geqslant 0 : \pi^n \in I\}$ and prove that $I = \pi^N \mathcal{O}_F$.]

Definition 4.17. Let F be a nonarchimedean normed field. We say that F (or $|\cdot|$) is *discrete* if the value group $|F^\times|$ is a cyclic group. This means that either $|\cdot|$ is trivial or $|\cdot|$ is nontrivial satisfies the equivalent conditions of Problem 4.16. In the latter case we say that $\mathcal{O}_F$ is a *discrete valuation ring* (or *DVR*).

Remark 4.18. The definition can be given in a purely ring-theoretic way, i.e. without having to mention a norm. One has that an integral domain D is a DVR if and only if D is Noetherian and local with principal maximal ideal. Also note, one can see from condition (v) that any DVR is a PID.

Recall for $F = \mathbf{Q}_p$ we denote the valuation subring by $\mathbf{Z}_p$, which we call the p-adic integers. From our previous discussion we see that the equivalent conditions of this problem can be applied to $F = \mathbf{Q}_p$, so in the language above we have that $\mathbf{Z}_p$ is a DVR, $\mathfrak{m}_{\mathbf{Q}_p} = p\mathbf{Z}_p$ and every nonzero ideal of $\mathbf{Z}_p$ has the form $p^n \mathbf{Z}_p$ for some n. In addition every element of $x \in \mathbf{Q}_p$ can be written in the form $x = p^n u$ for unique $n \in \mathbf{Z}$ and $u \in \mathbf{Z}_p^\times$. In this situation note that $n \geqslant 0 \iff x \in \mathbf{Z}_p$, and also note in this situation that $|x|_p = |p^n| = p^{-n}$.

As few more minor algebraic remarks:

Problem 4.19. Suppose F satisfies the equivalent conditions of Problem 4.16.

(a) Recall we have from Problem 2.9 that F is the field of fractions of $\mathcal{O}_F$, meaning any element of F can be written as a fraction of elements of $\mathcal{O}_F$. Show in fact that any element $x \in F$ can be written in the form $x = a/\pi^n$ for some $a \in \mathcal{O}_F$ and $n \in \mathbf{N}$. This is often summarized as saying that $F = \mathcal{O}_F[1/\pi]$. For those familiar with localization, one can say that F is the localization of $\mathcal{O}_F$ at the element π.

(b) Prove $\bigcap_{n \geqslant 0} \pi^n \mathcal{O}_F = \{0\}$.

Recall that $\mathbf{Q}$ is dense in $\mathbf{Q}_p$ by Problem 3.15. We claim that $\mathbf{Z}$ is also dense in $\mathbf{Z}_p$; in fact we will show something a bit more precise:

Problem 4.20. Consider the p-adic integers $\mathbf{Z}_p$.

(a) Let $x \in \mathbf{Z}_p$. Prove if $n \in \mathbf{Z}^+$, there exists some $a \in \mathbf{Z}$ such that $|x - a|_p \leqslant p^{-n}$. [Hint: you know you can choose a rational $a/b \in \mathbf{Q}^\times$ (let's say written so that $(a, b) = 1$) such that $|x - a/b|_p \leqslant p^{-n}$. Show then one also has $a/b \in \mathbf{Z}_p$, and then conclude $p \nmid b$. Thus you can choose $b' \in \mathbf{Z}$ such that $bb' \equiv 1 \bmod p^n$. Prove that $|a/b - ab'|_p \leqslant p^{-n}$, and conclude $|x - ab'|_p \leqslant p^{-n}$.]
(b) Fix some $n \in \mathbf{Z}^+$. Define a function $\pi_n : \mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ as follows: for $x \in \mathbf{Z}_p$ choose some $a \in \mathbf{Z}$ with $|x - a|_p \leqslant p^{-n}$, and define $\pi_n(x) = a \bmod p^n \in \mathbf{Z}/p^n\mathbf{Z}$. Prove this is a well-defined surjective ring homomorphism with kernel $p^n\mathbf{Z}_p$.]
(c) Conclude we have an isomorphism of rings $\mathbf{Z}_p/p^n\mathbf{Z}_p \simeq \mathbf{Z}/p^n\mathbf{Z}$. In particular conclude the residue field of $\mathbf{Q}_p$ is $\mathbf{F}_p$.

5 Week 5

5.1 Inverse limits and an algebraic description of $\mathbf{Z}_p$

We make here a general algebraic construction which one is sure to encounter very often if they proceed deeper into most algebraic subjects:

Definition 5.1. Let $\{A_n\}_{n\in\mathbf{Z}^+}$ be a collection of rings, and suppose for each n we have a ring homomorphism $f_n : A_{n+1} \longrightarrow A_n$. One typically imagines these as a diagram

$$\cdots \xrightarrow{f_n} A_n \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1 \ .$$

One also refers to the collections of rings and homomorphisms $(\{A_n\}_{n\in\mathbf{Z}^+}, \{f_n\}_{n\in\mathbf{Z}^+})$ as an *inverse system* (or *projective system*) of rings.

Remark 5.2. If one encounters projective systems elsewhere, you will find that often the rings and homomorphisms are indexed by an arbitrary poset, rather than $\mathbf{Z}^+$. The case we are introducing is all we need and simpler for a first exposure to the construction.

Problem 5.3. Let $\{A_n\}_{n\in\mathbf{Z}^+}$ and $\{f_n\}_{n\in\mathbf{Z}^+}$ be as above. We define a ring A as follows:

$$A = \Big\{(\dots, a_n, \dots, a_2, a_1) \,:\, a_i \in A_i \text{ and } f_i(a_{i+1}) = a_i \text{ for each } i\Big\}.$$

(a) Prove that A is a ring under component-wise addition and multiplication.
(b) Prove that for each $n \in \mathbf{Z}^+$ we have a ring homomorphism $\varphi_n : A \longrightarrow A_n$ via projection onto the nth component.
(c) Prove for φ_n as above one has $f_n \circ \varphi_{n+1} = \varphi_n$ (one might say these φ_n are *compatible*).

Definition 5.4. The pair $(A, \{\varphi_n\}_{n\in\mathbf{Z}^+})$ constructed above is called the *inverse limit* (or the *projective limit*, or even just the *limit*) of the inverse system $(\{A_n\}_{n\in\mathbf{Z}^+}, \{f_n\}_{n\in\mathbf{Z}^+})$; we denote it by $\varprojlim A_n$ (this refers to the ring, and we generally suppress the explicit maps $\{\varphi_n\}$). but it is important to remember that these are a relevant part of the data of an inverse limit. Notice the projective limit also depends on the functions f_n, although we do not make this explicit in our notation for the inverse limit.

Remark 5.5. Notice we are specifically interested in rings, but this is not a necessity to talk about inverse limits. If, from the start of this section, one replaced every instance of the phrase "ring homomorphism" with "group homomorphism", then one gets a valid notion of the inverse limit of an inverse system of groups. More generally, the notion of inverse limit makes sense in any *category*.

The following is a concrete example to get a feel for what inverse limits are meant to capture:

Problem 5.6. For sets X and Y write $\mathrm{Fun}(X, Y)$ for the set of functions $X \longrightarrow Y$. Let X and Y be sets and suppose one has an increasing sequence of subsets of X

$$X_1 \subseteq X_2 \subseteq X_3 \subseteq \cdots$$

such that $X = \bigcup_n X_n$. One has a map $r_n : \mathrm{Fun}(X_{n+1}, Y) \longrightarrow \mathrm{Fun}(X_n, Y)$ via restriction. Then $(\{\mathrm{Fun}(X_n, Y)\}_{n\in\mathbf{Z}^+}, \{r_n\}_{n\in\mathbf{Z}^+})$ forms an inverse system of sets. Prove there is a natural bijection $\mathrm{Fun}(X, Y) \longrightarrow \varprojlim \mathrm{Fun}(X_n, Y)$.

In the above setting, one should think that "defining a function on X is the same as defining a function on each X_n in a compatible way". Here is an example relating to Galois theory:

Less important problem 5.7. Suppose E/F is a (possibly infinite) normal extension of fields, and that one has an increasing sequences of subfields $E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots$ of E, each containing F, such that E_n/F is normal and $E = \bigcup_n E_n$. By normality of E_n/F one has a well-defined restriction map $r_n : \mathrm{Aut}_F(E_{n+1}) \longrightarrow \mathrm{Aut}_F(E_n)$. Thus the automorphism groups with restriction maps form an inverse system of groups. Prove that one has a naturally occuring isomorphism $\mathrm{Aut}_F(E) \simeq \varprojlim \mathrm{Aut}_F(E_n)$.

The following we will not use, but will help get you thinking about inverse limits:

Less important problem 5.8. Suppose we have inverse systems $(\{A_n\}_{n\in\mathbf{Z}^+}, \{f_n\}_{n\in\mathbf{Z}^+})$ and $(\{B_n\}_{n\in\mathbf{Z}^+}, \{g_n\}_{n\in\mathbf{Z}^+})$, and ring homomorphisms $\varphi_n : A_n \longrightarrow B_n$ for each n. Do we necessarily get an induced homomorphism $\varphi : \varprojlim A_n \longrightarrow \varprojlim B_n$? If not, what conditions needs to be added for this to hold? [Hint: a good guess would be to send $(\ldots, a_n, \ldots, a_2, a_1) \mapsto (\ldots, \varphi_n(a_n), \ldots, \varphi_2(a_2), \varphi_1(a_1))$. Try to show this is well-defined to find what condition is needed.]

Problem 5.9. Prove the inverse limit has the following universal property: if we have another ring R with "compatible" homomorphisms $\psi_n : R \longrightarrow A_n$ for each n, i.e. satisfying $f_n \circ \psi_{n+1} = \psi_n$. Prove there is a unique homomorphism $\psi : R \longrightarrow \varprojlim A_n$ satisfying $\varphi_n \circ \psi = \psi_n$ for each n.

Challenge problem 5.10. Prove this characterizes the inverse limit up to unique isomorphism, i.e. if $(A, \{\varphi_n\}_{n\in\mathbf{Z}^+})$ and $(A', \{\varphi'_n\}_{n\in\mathbf{Z}^+})$ both satisfy the universal property of the inverse limit of the projective system $(\{A_n\}, \{f_n\})$, then there is exactly one isomorphism $\theta : A \longrightarrow A'$ such that $\varphi'_n \circ \theta = \varphi_n$.

With the inverse limit construction defined, we can use it to give an algebraic description of the p-adic integers:

Important problem 5.11. In the notation of this section, consider $A_n = \mathbf{Z}/p^n\mathbf{Z}$ with $f_n : \mathbf{Z}/p^{n+1}\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$ being the natural projection map. Use the maps $\pi_n : \mathbf{Z}_p \to \mathbf{Z}/p^n\mathbf{Z}$ constructed earlier to construct a ring homomorphism $\pi : \mathbf{Z}_p \to \varprojlim \mathbf{Z}/p^n\mathbf{Z}$, and show this map is an isomorphism. [Hint: for surjectivity, if $(\dots, \alpha_n, \dots, \alpha_2, \alpha_1) \in \varprojlim \mathbf{Z}/p^n\mathbf{Z}$, for each n write $\alpha_n = a_n \bmod p^n$ for some $a_n \in \mathbf{Z}$. Then the compatibility condition says $a_{n+1} \equiv a_n \bmod p^n$; deduce the sequence $(a_1, a_2, \dots)$ is cauchy, and use this to find an $a \in \mathbf{Z}_p$ which maps to our original element. It is important to check that the element a you get is independent of the choice of a_n made: i.e. if one chooses different elements $a_n' \in \mathbf{Z}_p$ with $\alpha_n = a_n' \bmod p^n$, show that the resulting element a is unaffected.]

Challenge problem 5.12. For each n consider $\mathbf{Z}/p^n\mathbf{Z}$ as having the discrete topology. Notice that $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ is a subset of $\prod_{n\in\mathbf{Z}^+} \mathbf{Z}/p^n\mathbf{Z}$. Consider the product topology on $\prod_{n\in\mathbf{Z}^+} \mathbf{Z}/p^n\mathbf{Z}$ and then consider $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ with the subspace topology.

(a) Prove that for the isomorphism π from Problem 5.11, both π and π^{-1} are continuous, where $\mathbf{Z}_p$ has the topology coming from the metric on $\mathbf{Q}_p$. One says that π is then a "topological isomorphism".
(b) Prove that $\varprojlim \mathbf{Z}/p^n\mathbf{Z}$ is a closed subset of the product $\prod_{n\in\mathbf{Z}^+} \mathbf{Z}/p^n\mathbf{Z}$. [Hint: the inverse limit is the intersection over the sets $Z_i = \{(\dots, a_n, \dots, a_2, a_1) \mid f_i(a_i) = a_{i-1}\}$, so just show Z_i is closed.]
(c) Deduce from parts (a) and (b), along with Tychonoff's Theorem, that $\mathbf{Z}_p$ is compact.

5.2 Digit expansions of p-adic numbers

Our goal is to show elements of $\mathbf{Q}_p$ can be thought of as infinite digit expansions in base p. We start by doing this for elements of $\mathbf{Z}_p$:

Problem 5.13.

(a) Prove every element $x \in \mathbf{Z}_p$ can be written as the limit of a convergent series

$$x = a_0 + a_1 p + a_2 p^2 + \cdots$$

for integers $a_n \in [0, p-1]$. [Hint: by the results of the previous section, one can choose an integer a_0 such that $|x - a_0| \le p^{-1}$. Replace a_0 with the unique integer

$a_0' \in [0, p-1]$ such that $a_0 \equiv a_0' \bmod p$, and notice then one still has $|x - a_0| \leq p^{-1}$. Show this means we can write $x = a_0 + px_1$ for some $x_1 \in \mathbf{Z}_p$. Repeat this process with for x_1 to come up with an integer $a_1 \in [0, p-1]$ such that $x_1 = a_1 + px_2$. Continue inductively to get a sequence of integers $(a_n)_{n \geqslant 0}$ with $a_n \in [0, p-1]$ and at each step notice $x \equiv a_0 + a_1 p + \cdots + a_n p^n \bmod p^{n+1}\mathbf{Z}_p$. Conclude the sequence in question converges to x in $\mathbf{Q}_p$.]

(b) Prove this series representation is unique. [Hint: suppose $\sum_{n \geqslant 0} a_n p^n = \sum_{n \geqslant 0} b_n p^n$ for $a_n, b_n \in [0, p-1]$. Look at the values modulo p (i.e. apply the function π_1 from Problem 4.20) and deduce $a_0 = b_0$, then subtract this common value to find $\sum_{n \geqslant 0} a_{n+1} p^n = \sum_{n \geqslant 0} b_{n+1} p^n$. Repeat the process to get $a_1 = b_1$, then continue inductively.]

If $x = \sum_{n=0}^{\infty} a_n p^n$ with $a_i \in [0, p-1]$ one will often write this as a digit expansion $x = a_0 a_1 a_2 a_3 \cdots$, or $x = 0.a_0 a_1 a_2 a_3 \cdots$. Notice multiplication by p will shift this digit expansion, so $px = 0.0 a_0 a_1 a_2 \cdots$.

In fact one can take this a step further, and show an actual isomorphism that lets us think of $\mathbf{Z}_p$ as a ring of power series in p: first we recall the notion of formal power series:

Definition 5.14. Let R be a ring. The *ring of formal power series* over R is the set

$$R[\![X]\!] := \{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in R \},$$

equipped with formal addition and multiplication, i.e. one defines

$$\Big(\sum_{n=0}^{\infty} a_n x^n \Big) + \Big(\sum_{n=0}^{\infty} b_n x^n \Big) := \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

and

$$\Big(\sum_{n=0}^{\infty} a_n x^n \Big) \Big(\sum_{n=0}^{\infty} b_n x^n \Big) := \sum_{n=0}^{\infty} c_n x^n, \quad \text{where } c_n := \sum_{i+j=n} a_i b_j.$$

Notice each coefficient c_n in the multiplication makes sense because it is defined as a finite sum (i.e. we do not ever require any type of infinite summation, which allows us to have an arbitrary ring R here).

Problem 5.15. Define a function

$$\mathbf{Z}[\![x]\!] \longrightarrow \mathbf{Z}_p, \quad \sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} a_n p^n,$$

(notice the latter sum converges in $\mathbf{Z}_p$). Prove this is a surjective ring homomorphism with kernel $(x-p)$, so we obtain an isomorphism $\mathbf{Z}[\![x]\!]/(x-p) \simeq \mathbf{Z}_p$. [Hint: to show it is a homomorphism you will use the fact that addition and multiplication commute with limits. To calculate the kernel, suppose $\sum_{n=0}^{\infty} a_n p^n = 0$; one wants to find a sequence of integers $(b_n)_{n\geqslant 0}$ such that $\sum_{n=0}^{\infty} a_n x^n = (p-x)(\sum_{n=0}^{\infty} b_n x^n)$. To do this, take the equality $\sum_n a_n p^n = 0$ and reduce mod p to deduce that $p \mid a_0$, so $a_0 = b_0 p$ for some $b_0 \in \mathbf{Z}$. Replacing a_0 in the previous equation one has $(b_0 + a_1)p + a_2 p^2 + \cdots = 0$, and cancel a copy of p (recall $\mathbf{Z}_p$ is an integral domain) and repeat to write $b_0 + a_1 = b_1 p$ for some $b_1 \in \mathbf{Z}$, and continue this process inductively. Show the sequence (b_n) obtained is the one we desire.]

Remark 5.16. Notice that, if you are thinking of p-adic integers as series $\sum_{n=0}^{\infty} a_n p^n$ with $a_n \in [0, p-1]$, it is not necessarily true that addition (or multiplication) is given by term-wise addition modulo 3. For example, if $p = 3$ then $(1 + 1\cdot 3 + 1\cdot 3^2 + \cdots) + (2 + 2\cdot 3 + 2\cdot 3^2 + \cdots)$ is not just $0 + 0\cdot 3 + 0\cdot 3^2 + \cdots$. Rather, if one wants to get the 3-adic expansion one needs to do some "carrying", so one would get $0 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + \cdots$.

One knows that a real number is rational if and only if its decimal expansion eventually repeats (where we consider a terminal decimal expansion to end in repeating zeros). One can make a similar statement for p-adic digit expansions. We will use the bar notation for repeating digit expansions, so for instance $0.12\overline{13} = 0.1213131313131313\cdots$.

Problem 5.17. Prove that $-1 = \overline{(p-1)}$, i.e. $-1 = (p-1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots$.

Let us give an example on calculating a digit expansion of a rational number. First we start with the following

Problem 5.18. Suppose $x \in \mathbf{Q}_p$ with $|x| < 1$. Prove that $(1 + x + x^2 + \cdots)(1-x) = 1$, so one can safely write the expression $\frac{1}{1-x} = 1 + x + x^2 + \cdots$. [Hint: you should use the fact that multiplication commutes with limits to be fully precise.]

Problem 5.19.

(a) Prove if $x \in \mathbf{Q} \cap [-1, 0)$ (the real interval) satisfies $|x|_p = 1$ then x has a repeating p-adic digit expansion. [Hint: write $x = \frac{a}{b}$ with $a < 0$ and $b \leqslant 1$, where $p \nmid b$. Use the latter fact to find $k \in \mathbf{Z}^+$ with $p^k \equiv 1 \bmod b$, and write $p^k = 1 + bb'$ for $b' \in \mathbf{Z}^+$. Deduce one has $x = \frac{-ab'}{1-p^k}$; use the fact that $-1 \leqslant x < 0$ to get $0 < -ab' \leq p^k - 1$, and thus you can write a p-adic decimal expansion $-ab' = a_0 a_1 \cdots a_{k-1}$ for $a_i \in [0, p-1]$. Then one has $x = (a_0 \cdots a_{k-1})(1 + p^k + p^{2k} + p^{3k} + \cdots)$, show this is equal to $\overline{a_0 \cdots a_{k-1}}$).]

(b) Use the method from part (a) to write a 3-adic digit expansion of $\frac{2}{5}$. [Hint: do it for $-\frac{2}{5}$ and then take the negative.]

5.3 Hensel's lemma

Throughout the following we let t denote an indeterminate, and we will consider the ring $\mathcal{O}_F[t]$ of polynomials with coefficients in $\mathcal{O}_F$. Given an ideal $I \subseteq \mathcal{O}_F$ we write $f \equiv g \bmod I$ if this is true "coefficient-by-coefficient", i.e. if we write $f(t) = \sum_i a_i t^i$ and $g(t) = \sum_i b_i t^i$ then this means that $a_i \equiv b_i \bmod I$ for each i. In the case we have an element π with $0 < |\pi| < 1$, we say $f \equiv g \bmod \pi^n$ to mean $f \equiv g \bmod \pi^n \mathcal{O}_F$.

The following is the most commonly seen version of Hensel's lemma in the literature:

Important problem 5.20 (Hensel's lemma, version 1)**.** Let F be a complete nonarchimedean normed field. Let $f \in \mathcal{O}_F[t]$ be a polynomial and write $\bar{f}$ for the image of f in $k_F[t]$, i.e. where we consider the coefficients modulo $\mathfrak{m}_F$. Suppose there exist elements $\bar{g}, \bar{h} \in k_F[t]$ such that

(i) $\bar{g}$ is monic,
(ii) $\gcd(\bar{g}, \bar{h}) = 1$ in $k_F[t]$,
(iii) $\bar{f}(t) = \bar{g}(t)\bar{h}(t)$.

You will show there exist $g, h \in \mathcal{O}_F[t]$ such that

(i) g is monic,
(ii) $g \equiv \bar{g} \bmod \mathfrak{m}_F$ and $h \equiv \bar{h} \bmod \mathfrak{m}_F$,
(iii) $f(t) = g(t)h(t)$.

Proceed in the following steps:

(a) Prove if the norm on F is trivial then the conclusion is trivial, so we can suppose F has a nontrivial norm.
(b) Because the norm is nontrivial, there exist elements $\pi \in F$ with $0 < |\pi| < 1$. Prove for any such π, to get the desired conclusion, it suffices to construct two sequences of polynomials $(g_n)_{n \geqslant 1}$ and $(h_n)_{n \geqslant 1}$ satisfying
    (i) $g_1 \equiv \bar{g} \bmod \mathfrak{m}_F$ and $h_1 \equiv \bar{h} \bmod \mathfrak{m}_F$,
    (ii) each g_n is monic of degree $\deg(\bar{g})$,
    (iii) $g_{n+1} \equiv g_n \bmod \pi^n$ and $h_{n+1} \equiv h_n \bmod \pi^n$,
    (iv) $f(t) \equiv g_n(t)h_n(t) \bmod \pi^n$.
(b) Choose lifts $g_1, h_1 \in \mathcal{O}_F[t]$ of $\bar{g}, \bar{h}$ where g_1 is monic with $\deg(g_1) = \deg(\bar{g})$. By hypothesis $f - g_1 h_1 \in \mathfrak{m}_F[t]$; thus if we let $\tilde{\pi}$ be the coefficient of $f - g_1 h_1$ with

largest absolute value, then $0 < |\tilde{\pi}| < 1$ (unless $f - g_1 h_1 = 0$, in which case we have the desired conclusion anyways) and $f \equiv g_1 h_1 \bmod \tilde{\pi}$. Thus we can write $f = g_1 h_1 + \tilde{\pi}\, u_1$ for some $u_1 \in \mathcal{O}_F[t]$.

(c) Show we can find $\tilde{a}_1, \tilde{b}_1 \in \mathcal{O}_F[t]$ such that $\tilde{a}_1 h_1 + \tilde{b}_1 g_1 - u_1 \in \mathfrak{m}_F[t]$. If all coefficients of this difference are inside $\tilde{\pi}\mathcal{O}_F$ then let $\pi = \tilde{\pi}$ and proceed to part (d). Otherwise, let π be the coefficient of $\tilde{a}_1 h_1 + \tilde{b}_1 g_1 - u_1$ with largest absolute value, so $|\tilde{\pi}| \leqslant |\pi| < 1$. Replace u_1 by $(\tilde{\pi}/\pi)u_1$, replace $\tilde{a}_1$ by $(\tilde{\pi}/\pi)\tilde{a}_1$, and replace $\tilde{b}_1$ by $(\tilde{\pi}/\pi)b_1$. Verify we now have $f = g_1 h_1 + \pi u_1$ and $\tilde{a}_1 h_1 + \tilde{b}_1 g_1 \equiv u_1 \bmod \pi$.

(d) Show we can apply the division algorithm to find $q, a_1 \in \mathcal{O}_F[t]$ such that $\tilde{a}_1(t) = g_1(t)q(t) + a_1(t)$ with $\deg(a_1) < \deg(g_1)$. Define $b_1(t) = h_1(t)q(t) + \tilde{b}_1(t)$. Prove we have $a_1 h_1 + b_1 g_1 \equiv u_1 \bmod \pi$.

(e) Let $g_2 = g_1 + \pi a_1$ and $h_2 = h_1 + \pi b_1$. Prove g_2 is monic with $\deg(g_2) = \deg(\bar{g})$, and show $f(t) \equiv g_2(t)h_2(t) \bmod \pi^2$.

(f) Show we can continue this process for each n, obtaining sequences (g_n) and (h_n) as required in part (a).

The following is the more common version of Hensel's lemma to see in an introductory text. For the statement, recall the notion of a *formal derivative*: if A is a ring and we have a polynomial $f(t) = a_0 + \cdots + a_n t^n \in A[t]$, then the formal derivative of f is $f'(t) = a_1 + 2a_2 t + \cdots + (n-1)a_{n-1}t^{n-2} + n a_n t^{n-1}$.

Important problem 5.21 (Hensel's lemma, version 2)**.** Let F be a complete nonarchimedean normed field. Let $f \in \mathcal{O}_F[t]$ be a polynomial, and let $\bar{f}$ denote its image in $k_F[t]$. Suppose $\alpha \in k_F$ is a simple root of $\bar{f}$, i.e. $\bar{f}(\alpha) = 0$ and $\bar{f}'(\alpha) \neq 0$. Prove there exists a unique lift $a \in \mathcal{O}_F$ of α (i.e. an element such that $\alpha = a \bmod \mathfrak{m}_F$) such that $f(a) = 0$. [Hint: in our first version of Hensel's lemma, take $\bar{g}(t) = t - \alpha$; use the fact that α is a simple root to see that $\gcd(\bar{g}, \bar{h}) = 1$. For uniqueness again use the fact that α is a simple root of $\bar{f}$.]

Here is one more version of Hensel's lemma: the upside is that it is a bit more general than our version 2, the down side is it does not seem to follow direct from our first version. There may not be many occasions where one needs version 3 in lieu of version 2, but we will give one example in this section. You should feel free to take the following result on faith, or to read a proof (I will provide a link on the course webpage):

Less important problem 5.22 (Hensel's lemma, version 3)**.** Let F be a complete nonarchimedean normed field. Let $f \in \mathcal{O}_F[t]$ be a polynomial, and suppose we are given some $\bar{a} \in \mathcal{O}_F$ such that $|f(\bar{a})| < |f'(\bar{a})|^2$. Then there is a unique element $a \in \mathcal{O}_F$ such that $f(a) = 0$ and $|a - \bar{a}| < |f'(\bar{a})|$.

The uniqueness aspect of Hensel's lemma can seem irrelevant compared to the existence statement, but it is very important in applications as well. For instance, you will use both existence and uniqueness for the following first application of Hensel's lemma. For the problem, recall that an nth root of unity in a field F is an element $\zeta \in F$ satisfying $\zeta^n = 1$, and that we say ζ is a *primitive* nth root of unity if the order of ζ in $F^\times$ is exactly n, i.e. we do not have $\zeta^k = 1$ for any $1 \leqslant k < n$.

Problem 5.23. Let $m \in \mathbf{Z}^+$ be coprime to p. Show that $\mathbf{Q}_p$ contains a primitive mth root of unity if and only if $m | p - 1$. [Hint: recall the residue field of $\mathbf{Q}_p$ is $\mathbf{F}_p$. If $m | p - 1$ then one can find an element $\alpha \in \mathbf{F}_p^\times$ of order m, then take $f(t) = t^m - 1$ and use Hensel's lemma (version 2); the fact that p does not divide m will give $\bar{f}'(\alpha) \neq 0$. To see the lift ζ has order exactly m, notice if ζ is a root of $t^k - 1$ for $k < m$ then so is α. Conversely, if $\zeta \in \mathbf{Q}_p^\times$ is a primitive nth root of unity, prove necessarily $\zeta \in \mathbf{Z}_p^\times$, so one can consider its residue $\bar{\zeta} \in \mathbf{F}_p^\times$. Let $d = o(\bar{\zeta})$ and notice $d | m$. Use Hensel's lemma to lift $\bar{\zeta}$ to a root a of $x^d - 1$, but then notice a is also a root of $x^m - 1$, and then use the uniqueness of Hensel's lemma to deduce $a = \zeta$ and deduce $d = m$, so $m = o(\bar{\zeta})$ which divides $p - 1$ by Lagrange's theorem.]

Problem 5.24.

(a) Suppose $p \neq 2$, and suppose we are given some $b \in \mathbf{Z}_p^\times$ which is a square modulo p, i.e. there exists some $\alpha \in \mathbf{F}_p$ such that $\alpha^2 = \bar{b}$ in $\mathbf{F}_p$. Prove that b is a square in $\mathbf{Z}_p$ (i.e. there exists $a \in \mathbf{Z}_p$ such that $a^2 = b$).

(b) Show that $\mathbf{Q}_2$ contains a square root of -7. [Hint: use Hensel's lemma, version 3.]

Problem 5.25. Suppose $p \neq q$ are odd primes. Prove $\mathbf{Q}_p \neq \mathbf{Q}_q$ as fields. [Hint: Since $q \neq 2$ one can choose some $c \in \mathbf{Z}$ such that $t^2 = c$ does not have a solution in $\mathbf{F}_q$, and use Chinese Remainder Theorem to choose an integer b with $b \equiv 1 \bmod p$ and $b \equiv c \bmod q$. Show b is a square in $\mathbf{Q}_p$ but not a square in $\mathbf{Q}_q$.]

6 Week 6

6.1 Normed vector spaces

Definition 6.1. Let $(F, |\cdot|)$ be a normed field and let V be an F-vector space. An *F-vector space norm* (or simply *norm*) on V is a function $\|\cdot\| : V \longrightarrow \mathbf{R}^{\geqslant 0}$ such that for $v, w \in V$ and $c \in F$ one has

(i) $\|v\| = 0 \iff v = 0$,
(ii) $\|cv\| = |c|\,\|v\|$,
(iii) $\|v + w\| \leqslant \|v\| + \|w\|$.

A *normed vector space over F* is a pair $(V, \|\cdot\|)$ where $\|\cdot\|$ is an F-vector space norm.

Notice, similarly to the case of a normed field, defining $d : V \times V \longrightarrow \mathbf{R}^{\geqslant 0}$ by $d(v, w) := \|v - w\|$ gives any normed vector space the structure of a metric space, so in particular one can talk about the open subsets of V, etc. One can also talk about whether V is complete, using the exact same definition as for normed fields (or alternatively it is equivalent to being complete as a metric space).

Definition 6.2. If V is an F-vector space then two vector spaces norms $\|\cdot\|$ and $\|\cdot\|'$ are *equivalent* if there exist constants $C, C' > 0$ such that $\|\cdot\| \leqslant C\|\cdot\|'$ and $\|\cdot\|' \leqslant C'\|\cdot\|$.

Problem 6.3. Suppose the norm on our field F is nontrivial and let V be an F-vector space. Prove that two vector space norms $\|\cdot\|$ and $\|\cdot\|'$ are equivalent if and only if they define the same open subsets of V. [Hint: the reverse direction is the more interesting direction. The subset $\{v \in V : \|v\| < 1\}$ is open for $\|\cdot\|$, hence also for $\|\cdot\|'$, so one can find some $r > 0$ such that $\{v \in V : \|v\|' < r\} \subseteq \{v \in V : \|v\| < 1\}$. If one takes $c \in F$ satisfying $|c| > 1$, prove for any $v \in V$ one can find some $n \in \mathbf{Z}$ such that $|c|^n \leqslant \|v\|'/r < |c|^{n+1}$. Use the inclusion above to show that $\|c^{-(n+1)}v\| < 1$ and deduce that one can take $C = |c|/r$. Do a completely symmetric process to find C'.]

Problem 6.4. Let F be a normed field and V an F-vector space with a given basis $\{e_1, \ldots, e_m\}$. Define the function

$$\|\cdot\|_{\sup} : V \longrightarrow \mathbf{R}^{\geqslant 0}, \quad \Big\|\sum_{i=1}^{m} c_i e_i\Big\|_{\sup} := \max_{i=1,\ldots,m} |c_i|.$$

(a) Prove V is a vector space norm.

(b) Prove if F is complete then V is complete with respect to $\|\cdot\|_{\sup}$. [Hint: suppose we have a cauchy sequence $(v_n)_{n\geqslant 0}$ with respect to the sup norm on V. For each n one can write $v_n := \sum_{i=1}^m c_{n,i}e_i$ for $c_{n,i} \in F$. Prove for each i the sequence $(c_{n,i})_{n\geqslant 0}$ is cauchy in F, and let c_i be the limit. Prove $(v_n)_{n\geqslant 0}$ converges to $v = \sum_{i=1}^m c_i e_i$.]

We call this norm the *sup-norm* with respect to the basis $\{e_1, \dots, e_n\}$ (note it depends highly on the basis).

Important problem 6.5. Suppose F is a complete normed field and V is a finite-dimensional F-vector space. We will prove the following statement:

$$\text{If } \|\bullet\| \text{ is a norm on } V \text{ then } \|\bullet\| \text{ is equivalent to } \|\bullet\|_{\sup}.$$

As a result, one deduces any two norms on V are equivalent, and that $(V, \|\cdot\|)$ is complete. Proceed by induction on $n = \dim(V)$ in the following steps:

(1) Prove the result when $n = 0, 1$.
(2) Suppose $n \geqslant 2$. Prove one can take $C = \sum_{i=1}^n \|e_i\|$ for $\|\cdot\| \leqslant C\|\cdot\|_{\sup}$.
(3) Suppose there does not exist C' satisfying the requirements. Conclude for each $k \in \mathbf{Z}^+$ there exists some $v_k \in V$ satisfying $\|v_k\|_{\sup} > k\|v_k\|$. Show one can find an infinite subset, hence a subsequence $(v_{k_j})_{j\geqslant 1}$, such that $\|v_{k_j}\|_{\sup}$ is equal to the norm of the e_n-coefficient of v_{k_j}.
(4) Let v'_{k_j} be v_{k_j} divided by its e_n-coefficient. Prove $\|v_{k_j}\|_{\sup} = 1$ and $\|v_{k_j}\| < 1/k_j$.
(5) Let $W = \operatorname{span}_F(e_1, \dots, e_{n-1})$. Prove $w_j := v_{k_j} - e_n \in W$. Prove $\|w_j + e_n\| \longrightarrow 0$ as $j \longrightarrow \infty$ and conclude that $(w_j)_{j\geqslant 0}$ is a cauchy sequence for $\|\cdot\|$. Thus if we consider $\|\cdot\|$ as a norm restricted to W, then $(w_j)_{j\geqslant 0}$ is a cauchy sequence in W for $\|\cdot\|$.
(6) Use the inductive hypothesis to show that $\|\cdot\|$ and $\|\cdot\|_{\sup}$ are equivalent as norms on W, and use Problem 6.4(b) to conclude that $(w_j)_{j\geqslant 0}$ has a limit $w \in W$ for the norm $\|\cdot\|$. Write $\|w + e_n\| = \|(w - w_j) + (w_j + e_n)\|$ to show that $\|w + e_n\| = 0$ and conclude $e_n \in W$, giving a contradiction.

6.2 Extending norms

Definition 6.6. Let $(F, |\cdot|)$ and $(E, \|\cdot\|)$ be normed fields with E/F a field extension. We say that E/F is an *extension of normed fields* if the norm on E extends the norm on F, i.e. if $\|x\| = |x|$ for all $x \in F$.

Notice if E/F is an extension of normed fields, then the norm on E satisfies the condition of a vector space norm, so we can consider E as a normed vector space over F.

Remark 6.7. Notice if, in the situation above, $\|\cdot\|$ and $\|\cdot\|'$ are two norms on E extending the norm on F, then a priori the notions of $\|\cdot\|$ and $\|\cdot\|'$ being equivalent as *field* norms and being equivalent as *vector space* norms are different, but in fact by virtue of Problems 4.5 and 6.3 these are equivalent. Thus we will freely talk about $\|\cdot\|$ and $\|\cdot\|'$ being *equivalent* with no further quantifier.

We will be interested in starting with a norm on F, and seeing when there is a (field) norm on E extending the norm on F. We will show when F is complete and nonarchimdedean, and when E/F is an algerbaic extension, that there is exactly one such norm on E. First let's consider the case where the norm is trivial:

Problem 6.8. Let F be a field equipped with the trivial norm. Prove if E/F is an algerbaic extension and $\|\cdot\|$ is a field norm on E extending the trivial norm on F, then $\|\cdot\|$ must be the trivial norm. [Hint: suppose there were some $\alpha \in E$ with $0 < |\alpha| < 1$; because α is algebraic over F there is some equation $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$ with $c_i \in F$. Subtract c_0 from both sides and take norms to get a contradiction.]

Thus we have a unique extension of the norm in the trivial case, and we will turn our focus to the case when the norm on F is nontrivial:

Problem 6.9. Suppose $(F, |\cdot|)$ is a complete normed field with nontrivial norm and E/F is a finite field extension. Prove that there is at most one field norm on E extending the norm on F. [Hint: suppose $\|\cdot\|$ and $\|\cdot\|'$ are both field norms on E extending the norm on F. Use a result from the previous section to conclude the two norms are equivalent, then use Problem 4.3 to write $\|\cdot\|' = \|\cdot\|^\alpha$ for some $\alpha > 0$. Evaluate this equality at some $x \in F$ with $0 < |x| < 1$ to conclude $\alpha = 1$.]

Thus we see that if there is to be a field norm on E extending the norm on F, there is at most one possibility. But we still need to prove existence. We will "discover" what the correct norm is by narrowing down our options to one possibility. Recall the notion of the *norm* of a finite separable extension:

In the following, if E/F is an extension and $\overline{F}$ is an algebraic closure of F then we will write $\mathrm{Embed}_F(E, \overline{F})$ for the set of F-linear embeddings of E into $\overline{F}$. Recall (or prove) that if E/F is finite separable then $|\mathrm{Embed}_F(E, \overline{F})| = [E : F]$. Notice if E/F is Galois and $E \subseteq \overline{F}$ then there is natural identification $\mathrm{Embed}_F(E, \overline{F}) = \mathrm{Gal}(E/F)$.

Problem 6.10. Let E/F be a finite separable field extension and fix an algebraic closure $\overline{F}$ of F containing E. The *norm* of an element $\alpha \in E$ is the quantity

$$N_{E/F}(\alpha) := \prod_{\sigma \in \mathrm{Embed}_F(E,\overline{F})} \sigma(\alpha).$$

(a) Prove $N_{E/F}(\alpha) \in F$ for any $\alpha \in E$. [Hint: let E' be a Galois closure of E/F and prove that $N_{E/F}(\alpha)$ is fixed by every element $\theta \in \mathrm{Gal}(E'/F)$.]
(b) Prove $N_{E/F}$ defines a group homomorphism $N_{E/F} : E^\times \longrightarrow F^\times$.
(c) Prove if K is an intermediate subfield of E/F then $N_{E/F} = N_{K/F} \circ N_{E/K}$.

With this definition we can greatly restrict the possibilities of the norm extension on E:

Problem 6.11. Suppose F is a complete normed field with nontrivial norm and E/F is a finite Galois extension of degree n. Suppose $\|\cdot\|$ is a field norm on E extending the norm on F. Suppose E/F is Galois. Prove for any $\sigma \in \mathrm{Gal}(E/F)$, the function $E \longrightarrow \mathbf{R}^{\geqslant 0}$, $\alpha \mapsto \|\sigma(\alpha)\|$ is also a field norm on E extending the norm on F. Conclude $\|\sigma(\alpha)\| = \|\alpha\|$ for any $\alpha \in E$, and deduce $\|\alpha\| = |N_{E/F}(\alpha)|^{1/n}$.

This result tells us that in the normal case, IF a norm $\|\cdot\|$ on E exists extending the given norm on F (complete with nontrivial norm), then the only possibility is $\|\alpha\| = |N_{E/F}(\alpha)|^{1/[E:F]}$. We will prove that this does give such a norm (regardless of whether E is normal or not), and uniqueness in the non-normal case will follow as well:

It will be convenient to have an alternative description of the norm of an element:

Problem 6.12. Let E/F be a finite separable extension with $n := [E : F]$ and let $\alpha \in E$.

(a) Suppose $E = F[\alpha]$, and let $m_{\alpha,F}(x) = \sum_{i=0}^{n} c_i x^i$ be its minimal polynomial over F. Prove in this case one has $N_{F[\alpha]/F}(\alpha) = (-1)^{[F[\alpha]:F]} c_0$. [Hint: recall/prove one has a bijection $\mathrm{Embed}_F(F[\alpha], \bar{F}) \longrightarrow \{\text{roots of } m_{\alpha,F} \text{ in } \bar{F}\}$ given by $\sigma \mapsto \sigma(\alpha)$.]
(b) Prove in general one has $N_{E/F}(\alpha) = (-1)^n c_0^r$ where $r = [E : F[\alpha]]$. [Hint: Problem 6.10(c).]

We will not use the following, but it is worth mentioning because the norm function is quite common in further topics, that there is one more common alternative characterization of the norm. In fact the following is what is most commonly used as the "official definition" of norm, it has the advantages that (1) the definition is purely internal (one does not need to consider some algebraic closure of F), and (2) it is the correct formulation for non-separable extensions.

Less important problem 6.13. Let E/F be a separable field extension. For any $\alpha \in E$, multiplication by α defines an F-vector space automorphism $E \longrightarrow E$. Prove that $N_{E/F}(\alpha)$ is equal to the determinant of this transformation. [Hint: similarly to above, first consider the case $E = F[\alpha]$ before moving on to the general case.]

We will need the following consequence of Hensel's lemma:

Problem 6.14. Let F be a complete nonarchimedean normed field. Let $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ be an irreducible polynomial in $F[x]$ (with $c_n \neq 0$). Then for each i one has $|c_i| \leqslant \max\{|c_0|, |c_n|\}$. [Hint: take i with $|c_i|$ largest and divide by a_i to reduce to the case where $\max_{i=0,\ldots,n}\{|c_i|\} = 1$. Thus you need to show that $\max\{|c_0|, |c_n|\} = 1$. Let $r \in [0, n]$ be the smallest value with $|c_r| = 1$. Use the fact that $\bar{c}_i = 0$ in k_F for $i < r$ to find a factorization of $\bar{f}$ in $k_F[x]$, and apply Hensel's lemma to conclude $r \in \{0, n\}$.]

We will need the following notion from algebra:

Definition 6.15. If $A \subseteq B$ is an extension of rings, then we say an element $b \in B$ is *integral* over A if there exists a monic polynomial $f(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n \in A[x]$ for which $f(b) = 0$.

Notice if A and B are rings then $b \in B$ being "integral" is the same as being algebraic. Thus one should consider being integral as some kind of generalization of the notion of "algebraic" to the setting of rings. For the coming results we need to take the following on faith; you should think of it as an analogue of the fact that the set of algebraic elements in a field extension form a subfield:

Theorem. The set $\{b \in B : b \text{ is integral over } A\}$ is a subring of B.

One calls this set as in the theorem the *integral closure of A in B*. We say A is *integrally closed in B* if the integral closure of A in B is A itself, i.e. the only elements of B which are integral over A are those from A.

Note: the theorem above is not incredibly difficult, one just needs the language of modules which we are not assuming here. For a proof look at Propositions 5.1 and 5.2 of Atiyah-Macdonald's Commutative Algebra. Let us not a quick application to valuation rings:

Problem 6.16. Let F be a nonarchimedean normed field. Prove that $\mathcal{O}_F$ is integrally closed in F. [Hint: one needs to show that if $x \in \mathcal{O}_F$ is integral over $\mathcal{O}_F$ then in fact $x \in {}_F$. Suppose we have an equation $c_0 + \cdots + c_{n-1}x^{n-1} + x^n = 0$ where $c_i \in \mathcal{O}_F$. Notice if $x \notin \mathcal{O}_F$ then $x^{-1} \in \mathcal{O}_F$; in this case multiply the previous equation by $x^{-(n-1)}$ and deduce that $x \in \mathcal{O}_F$ for a contradiction.]

Now we can continue to show that we actually are getting a norm on any finite (separable) extension:

Important problem 6.17. Let F be a complete nonarchimedean normed field with nontrivial norm and E/F is a finite separable extension with $n := [E : F]$.

(a) Prove $\|\alpha\| := |N_{E/F}(\alpha)|^{1/n}$ satisfies all the conditions of a field norm extending the norm on F, except the triangle inequality.
(b) Prove $\mathcal{O}_E = \{\alpha \in E : N_{E/F}(\alpha) \in \mathcal{O}_F\}$ equals the integral closure of $\mathcal{O}_F$ in E, so in particular it is a subring of E by the theorem we've cited. [Hint: for the forward direction use Problems 6.12 and 6.14. In the reverse direction, if $\alpha \in E$ is integral over $\mathcal{O}_F$, conclude that $\sigma(\alpha)$ is integral over $\mathcal{O}_F$ for each $\sigma \in \mathrm{Embed}_F(E, \overline{F})$, and then use the theorem we've recalled above to prove that $N_{E/F}(\alpha)$ is integral over $\mathcal{O}_F$. Now use that $N_{E/F}(\alpha) \in F$ and Problem 6.16 to deduce $N_{E/F}(\alpha) \in \mathcal{O}_F$.]
(c) Prove that, to get the triangle inequality, one can reduce to showing $\|\alpha\| \leqslant 1 \implies \|\alpha + 1\| \leqslant 1$. Use part (b) to prove the latter statement, so we conclude our function $\|\cdot\|$ is a (nonarchimedean) norm as desired.
(d) Use Problems 6.4 and 6.5 to prove $(E, \|\cdot\|)$ is a complete normed field.

This gives us existence on all finite separable extensions E/F, and recall uniqueness comes from 6.9. Thus overall we have proved the following: If F is a complete nonarchimedean normed field, then for any finite separable extension E/F there exists a unique field norm on E extending the given norm on F, and E is complete with respect to this norm.

In fact the separability hypothesis is not necessary, we have included it so that we don't have to think about things like "inseparable degree" or "purely inseparable extensions". If one wishes to do this, one has two options: one can define the norm $N_{E/F}$ in the non-separable case from the start (which requires one to know/introduct the definition of inseparability degree), then prove that the statements of Problems 6.10 and 6.12 still hold, and verify the same proof we gave above goes through. A more efficient approach, utilizing the already proven separable case, is given as follows;

Challenge problem 6.18. Suppose E/F is a finite extension with F a complete nonarchimedean normed field. Let's suppose we are in characteristic p, because if we are in characteristic 0 then E/F is automatically separable. Prove that the norm on F extends to E in the following steps:

(1) Show it suffices to assume that E/F is purely inseparable. [Hint: taking the separable closure of E/F one has a tower decomposition $E/S/F$ with S/F separable and E/S purely inseparable; we already know we can extend the norm uniquely to S by the separable case.]

(2) Prove $[E : F]$ is a power of p.
(3) Prove $N_{E/F}(\alpha) = \alpha^{[E:F]}$.
(4) Prove that $\|\alpha\| = |N_{E/F}(\alpha)|^{1/[E:F]}$ satisfies the triangle inequality.

The last thing we will do is "glue" these extensions together to cover the infinite case:

Problem 6.19. Prove if F is a complete nonarchimedean normed field with nontrivial norm, then the norm on F extends uniquely to any separable algebraic extension E/F (warning: you should no longer expect E to be complete with respect to this norm if E/F is infinite). [Hint: for K an intermediate subfield with K/F finite, let $|\cdot|_K$ denote the unique extension of $|\cdot|$ to K. For $\alpha \in E$ try to define $\|\alpha\| = |\alpha|_K$ for any K containing α, and use uniqueness to prove this does not depend on the choice of K.]

Note: if you believe Problem6.18, you can remove the word "separable" here.

7 Week 7

7.1 The p-adic complex numbers

Let us introduce a piece of simplifying vocabulary:

Definition 7.1. A *nonarchimedean field* is a complete nonarchimedean normed field.

In the previous chapter we've shown that if F is a nonarchimedean field then the norm on F admits a unique extension to any separable algebraic extension E/F, and in the case $[E : F] < \infty$ one has that E is complete with respect to this norm. We've also remarked at the end (Problem 6.18) that one doesn't actually need the word "separable" here, we've only done so to simplify the proof; two methods of proving this generalization have been outlined in the mentioned remark. In order to achieve maximal generality in the coming sections, we will assume the result in full. That is, we will record (and use freely) the following theorem:

Theorem 7.2. If F is a nonarchimedean field and E/F is an algebraic extension, then the norm on F admits a unique extension to E. In the case $[E : F] < \infty$, it is explicitly given by $\|\alpha\| := |N_{E/F}(\alpha)|^{1/[E:F]}$ and one has that $(E, \|\cdot\|)$ is complete in this case.

If one feels uneasy about using the fully general version of this theorem without having proved it, it is safe and reasonable to assume that we are in characteristic zero, where separability always holds (we are mainly interested in $\mathbf{Q}_p$, anyways).

To motivate the coming section, recall that $\mathbf{Q}$, equipped with the usual absolute value from $\mathbf{R}$, has property that there is an extension of normed fields $E/\mathbf{Q}$ (namely $E = \mathbf{C}$) such that $\mathbf{C}$ is complete and algebraically closed. One may ask whether we have an analogue for $\mathbf{Q}_p$. Recall that $\mathbf{C}$ is obtained by taking the completion of $\mathbf{Q}$ and then taking an algebraic closure; it so happens that $\mathbf{C}$ is still complete. Recall from the previous section we know that $|\cdot|_p$ has a unique extension to any given algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$ (let us say this algebraic closure is fixed from here on). Unfortunately $\overline{\mathbf{Q}}_p$ is not complete (we will be able to prove this next week).

Next one might try to take $\overline{\mathbf{Q}}_p$ and complete it. Then we have a normed field, but is it algebraically closed? Miraculously, yes! Let's work our way towards a proof.

For the first step, let us introduce a bit of terminology: if E/F is an algebraic extension and $a, a' \in E$, we say that a and a' are *conjugate over* F if they have the same minimal polynomial.

Problem 7.3 (Krasner's lemma)**.** Let F be a nonarchimedean field and $\overline{F}$ an algebraic closure. Suppose we are given $a, b \in \overline{F}$ such that a is separable over F, and suppose for any conjugate $a' \neq a$ of a over F one has $|b-a| < |a'-a|$. Then we claim $a \in F[b]$; proceed in the following steps:

(1) Let E be a splitting field of $m_{a,F}$ over $F[b]$; justify why $E/F[b]$ is Galois, and thus to show $a \in F[b]$ it is enough to show that $\sigma(a) = a$ for all $\sigma \in \mathrm{Gal}(E/F[b])$.
(2) For any such σ, use the fact that the norm on F extends uniquely to E to prove that $|b - \sigma(a)| = |b - a|$.
(3) Apply the triangle inequality to $|\sigma(a) - a| = |(b - a) - (b - \sigma(a))|$ and derive a contradiction if $\sigma(a) \neq a$. [Hint: take $a' = \sigma(a)$ in the main hypothesis.]

Before we continue, it will be convenient to restate (and slightly improve the statement of) the result we proved in Problem 6.17(b); this is also another opportunity to understand the proof as it is a crucial part of the theorem.

Problem 7.4. Let F be a nonarchimedean field and E/F a finite extension. Prove for $\alpha \in E$ the following are equivalent:

(i) $\alpha \in \mathcal{O}_E$,
(ii) the minimal polynomial of α over F is inside $\mathcal{O}_F[t]$,
(iii) α is integral over $\mathcal{O}_F$.

[Hint: the steps are the exact same as in Problem 6.17(b), as what one really proves in the forward inclusion is that (i) $\implies$ (ii), then (ii) $\implies$ (iii) is trivial, and (iii) $\implies$ (i) is exactly the reverse inclusion.]

Now we can show the desired result, that the completion of $\overline{\mathbb{Q}}_p$ is algebraically closed:

Important problem 7.5. Let C denote (temporarily) the completion of $\overline{\mathbb{Q}}_p$. Suppose we are given a finite extension E/C. Prove $E = C$ in the following steps:

(1) Prove there exists some $\alpha \in \mathcal{O}_E$ such that $E = C[\alpha]$. Reason that if $p(t)$ denotes the minimal polynomial over C then $p(t) \in \mathcal{O}_C[t]$.
(2) Prove for any $a \in \mathcal{O}_C$ and $\epsilon > 0$ there exists $b \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ such that $|a-b| < \epsilon$. Deduce that if we write $p(t) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$ then for any $\epsilon > 0$ there exists a polynomial $q(t) = b_0 + \cdots + b_{n-1}x^{n-1} + x^n \in \mathcal{O}_{\overline{\mathbb{Q}}_p}[t]$ such that $|a_i - b_i| < \epsilon$ for $i \in [0, n-1]$.

(3) Let A denote the set of roots of $p(t)$ in some splitting field; take some $0 < r < \min\{|a' - a| : a, a' \in A \text{ are distinct}\}$, and take $\epsilon = r^n$ to get a polynomial $q(t)$ as above. Prove $q(t)$ has at least one root inside $\mathcal{O}_{\overline{\mathbf{Q}}_p}$. [Hint: if all the roots have absolute value > 1 think about the constant term of $q(t)$.]
(4) Calculate $|p(b)|$ in two ways: first write $p(b) = p(b) - q(b)$ and deduce $|p(b)| < r^n$. On the other hand write $p(b) = \prod_{a \in A}(b - a)$ and deduce $|p(b)| \geqslant (\min\{|b - a| : a \in A\})^n$.
(5) Use this to show that, for some root a of $p(t)$, the conditions of Krasner's lemma are met. Deduce that $a \in C[b] = C$, and then deduce $\alpha \in C$ as well, proving $E = C$.

This proves that the completion of $\overline{\mathbf{Q}}_p$ is algebraically closed. One denotes this field by $\mathbf{C}_p$ and sometimes refers to it as the *p-adic complex numbers*.

7.2 Newton polygons

Next we introduce the notion of a *Newton polygon*. For this topic it is most convenient to work in the language of *valuations*. Recall we have defined valuations in Week 1; let us expand our definition a bit to allow valuations to take values in all of $\mathbf{R}$ rather than just $\mathbf{Z}$. The upshot of doing this is the following: recall that any valuation on a field induced a (nonarchimedean) norm as in Problem 1.19; if we replace $\mathbf{Z}$ by $\mathbf{R}$ in the definition of valuation, then this correspondence is actually a bijection. Let us see this:

Definition 7.6. A *valuation* on F is a function $v : F \longrightarrow \mathbf{R} \cup \{\infty\}$ satisfying, for all $x, y \in F$

(i) $v(x) = \infty \iff x = 0$,
(ii) $v(xy) = v(x) + v(y)$,
(iii) $v(x + y) \geqslant \min\{v(x), v(y)\}$.

We obtain the following:

Problem 7.7. Let F be a field. Prove that if one fixes $0 < \rho < 1$ then there is a bijection

$$\{\text{valuations on } F\} \leftrightarrow \{\text{nonarchimedean norms on } F\}.$$

In one direction, one takes a valuation $v : F \longrightarrow \mathbf{R} \cup \{0\}$ to $|x| := \rho^{v(x)}$, and in the other direction one takes a norm $|\cdot| : F \longrightarrow \mathbf{R}^{\geqslant 0}$ to $v(x) := \log_\rho(|x|)$.

In addition, properties of norms translate into analagous properties of valuations. For instance all of the following can be easily be proven by translating over the analagous property for the corresponding norm:

Problem 7.8. Let $(F, |\cdot|)$ be a normed field. Fix some $0 < \rho < 1$ and let $v : F \longrightarrow \mathbf{R} \cup \{0\}$ be the associated valuation. Prove the following:

(a) $v(-1) = v(1) = 0$ and $v(-x) = v(x)$ for any $x \in F$,
(b) $\mathcal{O}_F = \{x \in F : v(x) \geqslant 0\}$, $\mathfrak{m}_F = \{x \in F : v(x) > 0\}$, and $\mathcal{O}_F^\times = \{x \in F : v(x) = 0\}$.
(c) One has an isomorphism of groups $|F^\times| \simeq v(F^\times)$ (note one group here is multiplicative while one is additive).
(d) If $x, y \in F$ with $v(x) \neq v(y)$ then one has equality $v(x + y) = \min\{v(x), v(y)\}$.
(e) If $(F, |\cdot|)$ is complete then v has a unique extension to any algebraic extension E/F; in the case E/F is finite this is given by $w(\alpha) = \frac{1}{[E:F]} v(N_{E/F}(\alpha))$.

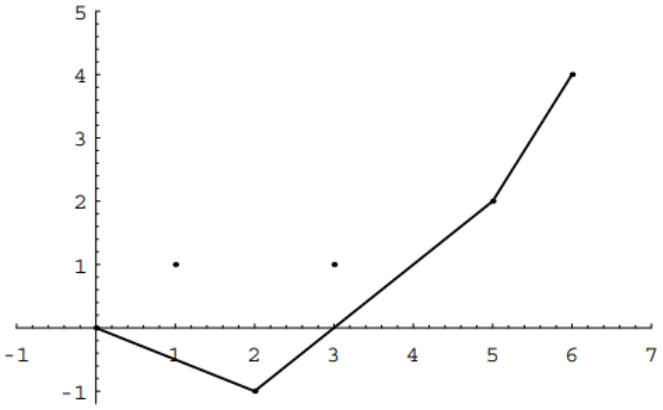
The fact that we allow flexibility with our choice of ρ is important at times: for instance one can prove the following

Problem 7.9. Suppose $(F, |\cdot|)$ is a discrete valued nonarchimedean normed field; recall this means that the norm is nontrivial and $|F^\times|$ is cyclic. Prove that there is exactly one choice of $0 < \rho < 1$ such that the associated valuation satisfies $v(F^\times) = \mathbf{Z}$. [Hint: if $|\pi|$ generates $|F^\times|$, force $v(\pi) = 1$.]

In the context of the above problem we say the valuation has been *normalized*.

Now we can talk about the Newton polygon of a polynomial. We will assume for our Newton polygons that the polynomial does not have 0 as a root; in applications if it does then one can divide by an appropriate power of t. We will also always be writing our polynomials so that the top coefficient is nonzero:

Definition 7.10. Let F be a nonarchimedean field and $v : F \longrightarrow \mathbf{R} \cup \{0\}$ be an associated valuation (i.e. corresponding to some choice of ρ). Let $f(t) = c_0 + c_1 t + \cdots + c_n t^n \in F[t]$ be a polynomial (where $c_0 c_n \neq 0$, see the remark above). We define the *Newton polygon* of f as follows: graph the points $\{(i, v(c_i))\}_{i=0}^n$ in $\mathbf{R}^2$, skipping any i such that $c_i = 0$, and take the "lower convex hull" of these points. In less fancy terms one does the following: start at the point $(0, v(c_0))$ and imagine a line extending downwards out of this point. Rotate the line counter-clockwise until a point $(i, v(c_i))$ is hit. At this point, consider the furthest point $(i_1, v(c_{i_1}))$ currently being touched by the line; we now imagine the line coming out of this point, and we keep rotating until we hit another point $(i, v(c_i))$, where we do the same. Continue until one hits $(n, v(c_n))$. Notice one then has a sequence of line segments with increasing slopes, and every point $(i, v(c_i))$ lives above (or on) this sequence of line segments.



[Image credit: *p-adic numbers: an Introduction, by Fernando Q. Gouvêa*]

Figure 1: $f(t) = 1 + 5t + \frac{1}{5}t^2 + 35t^3 + 25t^5 + 625t^6$ over $\mathbf{Q}_5$.

It is best to imagine this with a picture; here is the Newton polygon for $F = \mathbf{Q}_5$ and $f(t) = 1 + 5t + \frac{1}{5}t^2 + 35t^3 + 25t^5 + 625t^6$ (where we've taken the valuation to be normalized):

We will say that $(r, (v(c_r)) \leftrightarrow (s, v(c_s))$ is a *segment* of the Newton polygon if these points form the vertices of one segment of the Newton polygon. The *slope* is the slope of this segment, and the *length* is the horizontal length, i.e. $s - r$. It turns out that the slopes and lengths of segments of the Newton polygon gives us solid information about the roots of the polynomial in question. Also notice that if $c \in F^\times$ then the Newton polygons of f and cf are the same, only shifted up/down, so in particular the slopes and length of segments are unchanged. This allows us to make a simplifying assumption like $c_0 = 1$ or $c_n = 1$ in many proofs.

Before we prove the main statement let us introduce a quick improvement upon Problem 7.8(d):

Problem 7.11. Suppose F is a nonarchimedean normed field.

(a) Prove if we are given $a_1, \ldots, a_n \in F$ and the maximum of $\{|a_i|\}_{i=1}^n$ is achieved exactly once (i.e. there exists some i for which $|a_j| < |a_i|$ for all $j \neq i$), then one has equality $|a_1 + \cdots + a_n| = \max_{i=1,\ldots,n}\{|a_i|\}$. [Hint: you can directly use Problem 2.3.]

(b) Prove if v is a valuation on F and we are given $a_1, \ldots, a_n \in F$ such that the minimum of $\{v(a_i)\}_{i=1}^n$ is achieved exactly once, then $v(a_1 + \cdots + a_n) = \min_{i=1,\ldots,n}\{v(a_i)\}$.

Remark 7.12. The last thing we need to remark before embarking on our main proof is the following: if one has a monic polynomial $f(t) = c_0 + \cdots + c_{n-1}t^{n-1} + t^n \in F[t]$, and we write $f(t) = \prod_{i=1}^{n}(x - \alpha_i)$ for roots $\alpha_i \in \overline{F}$, then the coefficients c_i are actually symmetric functions of the α_i; for instance $c_{n-1} = -(\alpha_1 + \cdots + \alpha_n)$, $c_{n-2} = \sum_{i \neq j} \alpha_i \alpha_j$, $c_0 = \pm\alpha_1 \cdots \alpha_n$, and in general

$$c_k = \pm \sum_{i_1,\ldots,i_k} \alpha_{i_1} \cdots \alpha_{i_k}$$

where the sum is taken over distinct $i_1, \ldots, i_k \in [0, n-1]$.

Now we can continue with main theorem:

Important problem 7.13. Let F be a nonarchimedean field and v an associated valuation. We know that v has a unique extension to $\overline{F}$, and we denote this by v as well. Let $f(t) = \sum_{i=0}^{n} c_i t^i \in F[t]$ be a polynomial. If $(r, v(c_r)) \leftrightarrow (s, v(c_s))$ is a line segment in the Newton polygon on f of slope $-m$, then there are exactly $s - r$ roots of f in $\overline{F}$ satisfying $v(\alpha) = m$.

Proceed in the following steps:

(1) One can assume $c_n = 1$. Order the roots by their valuation, i.e. write $\alpha_1, \ldots, \alpha_n \in \overline{F}$ for the roots and take $1 = s_0 < s_1 < \cdots < s_t = n$ in such a way that one has by hypothesis

$$\begin{aligned} v(\alpha_1) = \cdots = v(\alpha_{s_1}) &= m_1, \\ v(\alpha_{s_1+1}) = \cdots = v(\alpha_{s_2}) &= m_2, \\ &\vdots \\ v(\alpha_{s_{t-1}+1}) = \cdots = v(\alpha_{s_t}) &= m_t. \end{aligned}$$

where $m_1 < m_2 < \cdots < m_t$ are real numbers.

(2) By the way we've listed the roots we see there are s_1 elements of valuation m_1. We will show there is a segment of the Newton polygon with length s_1 and slope $-m_1$. To do this, use the way we've listed the roots, and Remark 7.12 to prove the

following:

$$\begin{aligned} v(c_n) &= 0, \\ v(c_{n-1}) &\geqslant \min_i\{v(\alpha_i)\} = m_1, \\ v(c_{n-2}) &\geqslant \min_{i,j}\{v(\alpha_i\alpha_j)\} = 2m_1, \\ &\vdots \\ v(c_{n-s_1}) &= \min_{i_1,\dots,i_{s_1}}\{v(\alpha_{i_1}\cdots\alpha_{i_{s_1}})\} = s_1m_1, \end{aligned}$$

where the end equality comes from Problem 7.11. Use this string of (in)equalities to show that $(n - s_1, s_1m_1) \leftrightarrow (n, 0)$ is a segment of the Newton polygon of slope $-m_1$.

(3) Now use the same logic to show that $(n - s_2, s_1m_1 + (s_2 - s_1)m_2) \leftrightarrow (n - s_1, s_1m_1)$ is a segment of the Newton polygon of slope $-m_2$; for this the string of equalities you use should be the following:

$$\begin{aligned} v(c_{n-s_1-1}) &\geqslant \min_{i_1,\dots,i_{s_1+1}}\{v(\alpha_1\cdots\alpha_{i_{s_1+1}})\} = s_1m_1 + m_2, \\ v(c_{n-s_1-2}) &\geqslant \min_{i_1,\dots,i_{s_1+2}}\{v(\alpha_1\cdots\alpha_{i_{s_1+2}})\} = s_1m_1 + 2m_2, \\ &\vdots \\ v(c_{n-s_2}) &= \min_{i_1,\dots,i_{s_2}}\{v(\alpha_{i_1}\cdots\alpha_{i_{s_2}})\} = s_1m_1 + (s_2 - s_1)m_2. \end{aligned}$$

(4) Continue inductively, finding for each i a segment of the Newton polygon of length $s_i - s_{i-1}$ and slope $-m_i$. Conclude the result.

We see from the example that the Newton polygon has extreme power in determining information about the roots of a polynomial. Now we turn to look at examples:

7.3 Applications of Newton polygons

Newton polygons are often particularly useful for showing irreducibility of a polynomial. Let us set up some facts we will use multiple times:

Problem 7.14. Let F be a discretely valued nonarchimedean field and v the associated normalized valuation.

(a) Prove if $\alpha \in \overline{F}$ with $[F[\alpha] : F] = d$, one has $v(\alpha) \in \frac{1}{d}v(F^\times)$.

(b) Prove if $m \in \mathbf{Z}^+$ divides the denominator of each slope (when written in lowest terms) of $f \in F[t]$, then m divides the degree of each irreducible factor of f in $F[t]$. [Hint: if g is an irreducible factor in $F[t]$ and $\alpha \in \overline{F}$ is a root of g, then by hypothesis m divides the denominator (call it d) of $v(\alpha)$, and then using (a) deduce m divides $[F[\alpha] : F]$.]

(c) As a special case of (b) prove if $f \in F[t]$ with $\deg(f) = n$ and the Newton polygon of f has a segment of slope $\pm\frac{1}{n}$, then f is irreducible.

Problem 7.15. (a) If F is a nonarchimedean field, use the previous problem to give a proof of Eisenstein's criterion in $\mathcal{O}_F[t]$: if $\pi \in \mathcal{O}_F$ is a prime element (this is the same as being a uniformizer, so in this setting the field is discretely valued) and $f(t) = c_0 + \cdots + c_n t^n \in F[t]$ satisfies

(i) $|c_i| \leqslant |\pi|$ for $i \in [0, n-1]$,
(ii) $|c_0| = |\pi|$,
(iii) $|c_n| = 1$,

then f is irreducible.

(b) Use this to prove Eisenstein's criterion over $\mathbf{Q}$.

Remark 7.16. The above strategy should actually give a proof of Eisenstein's criterion in full generality (i.e. for all UFDs): any prime element p of a UFD D determines a valuation on the field of fractions of D in the same manner as for $\mathbf{Z}$, and then one can take the associated norm and complete.

Next let us consider another example. For motivation, recall that the *inverse Galois problem* asks the following: if one is given a finite group G, does there exist a Galois extension $K/\mathbf{Q}$ such that $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$? The problem is still open, but for many classes of groups we know the answer to be true. One of the difficulties in evaluating certain potential examples is verifying irreducibility in situation where one would like to know it. It is generally a tough thing to verify irreducibility of a polynomial; although one is given some standard techniques in a first algebra course, these can only take one so far.

Problem 7.17. Fix a prime p and consider the polynomials

$$E_n(t) = 1 + t + \frac{t^2}{2!} + \cdots + \frac{t^n}{n!}, \quad L_n(x) = \sum_{j=0}^{n} (-1)^j \binom{n}{j} \frac{x^j}{j!} \in \mathbf{Q}[t].$$

(a) Prove/read a proof of/take on faith the following two assertions:

(i) If $n \in \mathbf{Z}^+$ and we write $n = a_0 + a_1 p + \cdots + a_k p^k$ in base p (where $0 \leqslant a_i < p$), then for $s = a_1 + \cdots + a_k$ one has $v_p(n!) = \frac{n-s}{p-1}$.

(ii) (Lucas's Theorem) If $n, m \in \mathbf{Z}^+$ with $m < n$, and we write $n = a_0 + a_1 p + \cdots + a_k p^k$ and $m = b_0 + b_1 p + \cdots + b_k p^k$ are base p expansions of n and m, then one has $\binom{n}{m} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \binom{a_k}{b_k}$.

(b) Write $n = a_1 p^{n_1} + \cdots + a_k p^{n_k}$ where $0 < a_i < p$ and $n_1 > \cdots > n_k$ (i.e. reverse the order on the base p expansion and ignore the zero terms. Use (i) above to prove if one writes $x_i = a_1 p^{n_1} + \cdots + a_i p^{n_i}$ for $i = 1, \ldots, k$ and $x_0 = 0$ then the $\{x_i\}_{i=0}^k$ are exactly the x-coordinates of the Newton polygon of E_n, taken in $\mathbf{Q}_p$, with the slope between x_{i-1} and x_i given by $m_i = -\frac{p^{n_i}-1}{(p-1)p^{n_i}}$. [Hint: drawing a picture may help.]

(c) Prove if p^m divides n then $m \leqslant n_s$, and conclude p^m divides the denominator of each slope of the Newton polygon over $\mathbf{Q}_p$; conclude p^m divides the degree of each irreducible factor of E_n in $\mathbf{Q}_p[t]$. [Hint: Problem 7.14.]

(d) Conclude if $n = \prod_p p^{n_p}$ is a prime factorization of n, then p^{n_p} divides the degree of each irreducible factor of E_n in $\mathbf{Q}[t]$ for each p. Deduce E_n is irreducible in $\mathbf{Q}[t]$.

(e) Notice the Newton polygon of L_n over $\mathbf{Q}_p$ lies below the Newton polygon of E_n; use (ii) above to prove that $v_p(\binom{n}{x_i}\frac{1}{x_i!}) = v_p(\frac{1}{x_i!})$ for each $i = 1, \ldots, k$ and deduce that the Newton polygons of E_n and L_n are equal over $\mathbf{Q}_p$ for each p.

(f) Notice the argument from (c) and (d) was only dependent on the Newton polygon in $\mathbf{Q}_p$ for each p; deduce L_n is irreducible in $\mathbf{Q}[t]$ as well.

From here it's a bit of somewhat elementary algebra and number theory to prove that the Galois group of (a splitting field of) L_n over $\mathbf{Q}$ is S_n for all n, and the Galois group of E_n over $\mathbf{Q}$ is S_n when $4 \nmid n$ and A_n when $4 \mid n$. Thus one gets a solution to the inverse Galois problem for S_n, and a partial answer for A_n.

8 Week 8

8.1 Ramification

Starting now we will for some reason use the letters K and L for our nonarchimedean fields instead of F and E. In this section our nonarchimedean field will always be discretely valued; recall this means that $|K^\times|$ (or equivalently $v(K^\times)$) is infinite cyclic (the "infinite" just corresponds to the norm/valuation being nontrivial). Recall in this setting an element $\pi \in \mathfrak{m}_K$ such that $v(\pi)$ generates $v(K^\times)$ is a *uniformizer*. We will take the normalized valuation on K, which is the same as requiring $v(\pi) = 1$.

Let K be a discretely valued nonarchimedean field and L/K a finite extension. As long as L/K is understood (i.e. any problem that does not reference other extensions of K) we will fix the notation $n = [L : K]$. We have seen that the norm and valuation on K naturally extends to on L; the latter is explicitly given by $w(x) = \frac{1}{n} v(N_{L/K}(x))$. Notice that L is also discretely valued, as for instance $w(L^\times)$ is a subgroup of the cyclic group $\frac{1}{n} v(K^\times)$, Notice also $v(K^\times) \subseteq w(L^\times)$.

With respect to our norms then one has the residue fields $k_K = \mathcal{O}_K/\mathfrak{m}_K$ and $k_L = \mathcal{O}_L/\mathfrak{m}_L$; we will introduce the notation $k := k_K$ and $\ell := k_L$ and use this notation constantly without further mention. Under the inclusion map $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ one sees that $\mathfrak{m}_K \subseteq \mathfrak{m}_L$, and thus there is an induced inclusion of fields $k \hookrightarrow \ell$, i.e. ℓ is a field extension of k.

Problem 8.1. Let L/K be a finite extension.

(a) Prove that ℓ/k is a finite extension.
(b) Prove the index $[w(L^\times) : v(K^\times)]$ is finite.

Definition 8.2. One writes $e(L/K) := [w(L^\times) : v(K^\times)]$ and $f(L/K) := [\ell : k]$. We call $e(L/K)$ the *ramification index* of L/K and $f(L/K)$ the *inertia degree*. When L/K is understood from context we will just write $e = e(L/K)$ and $f = f(L/K)$.

We say that L/K is *unramified* if $e = 1$ and ℓ/k is a separable extension.

The study of ramification plays an important role in number theory. One should consider unramified extensions to be the "nicest" situation one could be in. Let us see some basic first facts about the ramification index:

Problem 8.3. Let L/K be a finite extension. Recall we have remarked above that L is also discretely valued, so L has a uniformizer $\varpi \in \mathfrak{m}_L$.

(a) Prove that $w(\varpi) = \frac{1}{e}v(\pi)$, so in particular as long as the valuation v is normalized one has $w(\varpi) = \frac{1}{e}$ and $w(L^\times) = \frac{1}{e}\mathbf{Z}$.
(b) Recall (Problem 4.16) every nonzero ideal of $\mathcal{O}_L$ has the form $\varpi^k\mathcal{O}_L$ for some (unique) $k \in \mathbf{N}$. Prove e is exactly the integer such that $\pi\mathcal{O}_L = \varpi^e\mathcal{O}_L$.
(c) Deduce $e = 1$ if and only if π is a uniformizer for L.
(d) Prove $w(1), w(\varpi), w(\varpi^2), \ldots, w(\varpi^{e-1})$ form a set of coset representatives of $w(L^\times)/v(K^\times)$.

The following is a fundamental fact about the relationship between ramification index and intertia degree:

Important problem 8.4. Let L/K be a finite extension and $n = [L : K]$. Prove that $n = ef$ in the following steps:

(1) Fix notation: let $\alpha_1, \ldots, \alpha_f \in \ell$ denote a basis of ℓ over k and let $a_1, \ldots, a_f \in \mathcal{O}_L^\times$ be lifts of these elements. We claim that $\{a_i\varpi^j \mid i \in [1, f], j \in [0, e-1]\}$ is a basis for L over K, which would give the result.
(2) Linear independence (part 1): suppose $\sum_{ij} c_{ij}a_i\varpi^j = 0$ for $c_{ij} \in K$, and suppose for a contradiction not all c_{ij} are zero. Write $s_j = \sum_{i=1}^{f} cija_i$. Because not all $c_{ij} \neq 0$, there exists at least one j for which there exists $c_{ij} \neq 0$. Fix any such j and let i_0 be such that $v(c_{i_0j})$ is minimal. Divide s_j by c_{i_0j} to obtain a linear combination of the a_i with coefficients in $\mathcal{O}_K$ and at least one coefficient equal to 1. View the combination in ℓ and use linear independence of the α_i to deduce that $s_j/c_{i_0j} \in \mathcal{O}_L^\times$, and deduce $w(s_j) = v(c_{i_0j}) \in v(K^\times)$ (also notice $s_j \neq 0$ necessarily).
(3) Linear independence (part 2): by hypothesis $\sum_{j=0}^{e-1} s_j\varpi^j = 0$. We know there exist nonzero summands (the final conclusion of (2)); conclude that there must exist some $j \neq k$ with $w(s_j\varpi^j) = w(s_k\varpi^k)$ (Hint: Problem 7.11). Apply (2) to both s_j and s_k to deduce $w(\varpi^j) - w(\varpi^k) \in v(K^\times)$ and get a contradiction using Problem 8.3(d). From the contradiction deduce linear independence.
(4) Spanning (part 1): prove that it suffices to show that any $x \in \mathcal{O}_L$ can be written as a $\mathcal{O}_K$-linear combination of the $\{a_i\varpi^j\}$.
(5) Spanning (part 2): for $x \in \mathcal{O}_L$, use the fact that the α_i span ℓ as a k-vector space to prove there exist some $c_{01}, \ldots, c_{0f} \in \mathcal{O}_K$ such that $x = c_{01}a_1 + \cdots + c_{0f}a_f + \varpi z$ for $c_{ij} \in \mathcal{O}_K$ and $z \in \mathcal{O}_L$. Apply the same logic to z, and continue inductively; eventually you will have a ϖ^e term, and then remember that $\varpi^e = \pi u$ for some $u \in \mathcal{O}_L^\times$ (see Problem

8.3(b)), and see then that x can be written as a sum

$$\begin{aligned} x = {} & c_{01}^{(1)} a_1 + \cdots + c_{0f}^{(1)} a_f \\ & + \varpi(c_{11}^{(1)} a_1 + \cdots + c_{1f}^{(1)} a_f) \\ & + \cdots \\ & + \varpi^{e-1}(c_{e-1,1}^{(1)} a_1 + \cdots + c_{e-1,f}^{(1)} a_f) \\ & + \pi x_1 \end{aligned}$$

for some $x_1 \in \mathcal{O}_L$.

(6) Spanning (part 3): Repeat the same process for x_1 and upgrade the previous equality to (for some $c_{ij}^{(1)} \in \mathcal{O}_K$)

$$\begin{aligned} x = {} & (c_{01}^{(0)} + \pi c_{01}^{(1)}) a_1 + \cdots + (c_{0f}^{(1)} + \pi c_{0f}^{(2)}) a_f \\ & + \varpi((c_{11}^{(1)} + \pi c_{11}^{(2)}) a_1 + \cdots + (c_{1f}^{(1)} + \pi c_{1f}^{(2)}) a_f) \\ & + \cdots \\ & + \varpi^{e-1}((c_{e-1,1}^{(1)} + \pi c_{e-1,1}^{(2)}) a_1 + \cdots + (c_{e-1,f}^{(1)} + \pi c_{e-1,f}^{(2)}) a_f) \\ & + \pi^2 x_2 \end{aligned}$$

for some $x_2 \in \mathcal{O}_L$.

(7) Spanning (part 4): Continue this process to obtain a sequence $(c_{ij}^{(k)})_{k \geqslant 0}$ for each fixed i, j; let $c_{ij} := \sum_{k \geqslant 0} c_{ij}^{(k)} \pi^k$. Justify why this sum converges to give a value $c_{ij} \in \mathcal{O}_K$ and find $x = \sum_{i,j} c_{ij} a_i \pi^j$, giving the conclusion we wanted.

Remark 8.5. Notice what we actually proved is slightly stronger, we prove that the $\{a_i \varpi^j\}$ is a basis for $\mathcal{O}_L$ as an $\mathcal{O}_K$-module. We probably will not need this but I am giving it as a remark here just in case.

Notice as a result of this proposition we in fact have that $e = 1$ if and only if $[L : K] = f$, and also $[L : K]$ is the largest possible value of e; when the latter happens we say that L/K is *totally ramified*. One can easily see that being "totally ramified" is well behaved in towers, i.e. if $E/L/K$ then E/K is totally ramified if and only if both E/L and L/K are totally ramified.

In the next section we will have a nice classification of unramified extensions of K (at least when we have our running hypothesis that K is discretely valued), and we will be able to say very explicitly what they are in the case $K = \mathbf{Q}_p$. For now let us give some examples of totally ramified extensions:

Problem 8.6. Let $p^{1/n}$ be an n-th root of p in some algebraic closure of $\mathbf{Q}_p$ and consider $L = \mathbf{Q}_p[p^{1/n}]$. Let $e = e(L/\mathbf{Q}_p)$.

(a) Prove $[L : \mathbf{Q}_p] = n$. [Hint: Eisenstein.]
(b) Prove one has $v(p^{1/n}) = 1/n$. From this conclude $e \geqslant n$, and deduce $e = n$, so $L/\mathbf{Q}_p$ is totally ramified and $p^{1/n}$ is a uniformizer for L.

Problem 8.7. Fix some $m \in \mathbf{Z}^+$ and let ζ be a primitive p^m-th root of unity in some algebraic closure of $\mathbf{Q}_p$. Let $L = \mathbf{Q}_p[\zeta]$ and $e = e(L/\mathbf{Q}_p)$.

(a) Notice $\zeta^{p^{m-1}}$ is primitive p-th root of unity; use this to prove that ζ is a root of $f(t) = t^{(p-1)p^{m-1}} + t^{(p-2)p^{m-1}} + \cdots + 1$.
(b) Use Eisenstein's criterion to show that $f(t+1)$ is irreducible, and conclude this is the minimal polynomial of $\zeta - 1$. Deduce $[L : \mathbf{Q}_p] = (p-1)p^{m-1} = \varphi(p^m)$.
(c) Recall from basic field theory that $L/\mathbf{Q}_p$ is Galois (for example it is the splitting field of f over $\mathbf{Q}_p$, and we are in characteristic zero). Also recall one has a natural homomorphism $\mathrm{Gal}(L/\mathbf{Q}_p) \longrightarrow (\mathbf{Z}/p^m\mathbf{Z})^\times$; show this is an isomorphism.
(d) Use Problem 6.12 to show that $N_{L/\mathbf{Q}_p}(\zeta - 1) = p$. Deduce that $v(\zeta - 1) = \frac{1}{(p-1)p^{m-1}}$, and conclude that $L/\mathbf{Q}_p$ is totally ramified and $\zeta - 1$ is a uniformizer for L.

8.2 Unramified extensions

Problem 8.8. Let L/K be a finite unramified extension. Prove that L/K is separable. In fact, prove if $\ell = k[\alpha]$ (such α exists by primitive element theorem), then $L = K[a]$ for any lift $a \in \mathcal{O}_L$ of α, and a is separable over K. [Hint: choose a as in the theorem and let $m_{a,K}$ denote the minimal polynomial over K. Recall $m_{a,K} \in \mathcal{O}_K[t]$ by 7.4, so one can consider $\overline{m}_{a,K} \in k[t]$. Prove that $m_{\alpha,k} | \overline{m}_{a,K}$ and use a degree argument (recalling $[L : K] = [\ell : k]$ by the unramified hypothesis) to show that $L = K[a]$. You should deduce along the way that $m_{\alpha,k} = \overline{m}_{a,K}$, and use this to prove that $m_{a,K}$ is a separable polynomial.]

Let us analyze some basics about how unramified extensions behave in towers and under "change of base":

Problem 8.9. Let $E/L/K$ be a tower of finite extensions (let ε denote the residue field of E when working the problem, since we are already using the letter e), and suppose all these extensions are occuring within some fixed algebraic extension Ω/K (you can imagine $\Omega = \overline{K}$ if you like; we are making this hypothesis so that we can talk about compositum in parts (c) and (d)).

(a) Prove $e(E/K) = e(E/L)e(L/K)$ and $f(E/K) = f(E/L)f(L/K)$.
(b) Conclude E/K is unramified if and only if both E/L and L/K are unramified. [Hint: don't forget to think about the separability condition on the residue fields!]
(c) Prove if K'/K is a finite extension inside Ω and L/K is unramified, then LK'/K' is unramified; proceed in the following steps:
    (1) Fix notation: let $L' = LK'$ and let k', ℓ' denote the residue fields of K, L. Choose $\alpha \in \ell$ such that $\ell = k[\alpha]$, and choose a lift $a \in \mathcal{O}_L$ so that a is separable over K and $L = K[a]$ as in the previous problem. Notice then $L' = K'[a]$. Let m, m' be the minimal polynomial of a over K, K' respectively. Recall from the proof of the previous problem one has $m \in \mathcal{O}_K[t]$ and $\overline{m} = m_{\alpha,k}$.
    (2) Prove $m' \mid m$ in $K'[t]$; use the fact that all roots of m are integral (i.e. they satisfy $|b| \leqslant 1$, see Problem 7.4) or Gauss's lemma to deduce that in fact $m' \mid m$ in $\mathcal{O}_{K'}[t]$ and then $\overline{m}' \mid \overline{m}$ in $k'[t]$. In particular $\overline{m}'$ is separable in $k'[t]$.
    (3) Use Hensel's lemma (and the fact $\overline{m}'$ is separable) to prove that $\overline{m}'$ is irreducible, and conclude $\overline{m}' = m_{\alpha,k'}$; in particular α is separable over k'.
    (4) Prove $[\ell' : k'] \leqslant [L' : K'] = [k'[\alpha] : k'] \leqslant [\ell' : k']$ and conclude the result.
(d) Use (b) and (c) to deduce that if L, K' are both unramified over K then the compositum LK' is unramified over K as well.

This proposition gives us quite a bit about unramified extensions: first it tells us that we can make the following definition: a (possibly infinite) algebraic extension E/K is *unramified* if every finite subextension L/K is unramified. By virtue of part (b) above this does not clash with our original definition of unramified when E/K is finite. One can also use (d) to get the following:

Problem 8.10. Let Ω/K be an algebraic extension. Prove that the union of all finite unramified subextensions L/K inside Ω is a field, and furthermore an unramified extension of K. We call this the *maximal unramified subextension* of Ω/K. When $\Omega = \overline{K}$ we also denote this by K^{nr} and call this a *maximal unramified extension of* K.

Next we show a beautiful result, that unramified extensions of K correspond perfectly to finite separable extensions of k.

Important problem 8.11. Let K be a discretely valued nonarchimedean field. Fix an algebraic closure $\overline{K}$ of K and let $\overline{k}$ denote its residue field.

(a) Prove that $\overline{k}$ is an algebraic closure of k. [Hint: it suffices to check that a monic irreducible polynomial $\overline{f} \in k[t]$ decomposes into linear factors inside $\overline{k}[t]$. To do

this lift $\overline{f}$ to a monic polynomial $f \in \mathcal{O}_K[t]$; if one takes $L \subseteq \overline{K}$ to be a splitting field for f over K, then use Problem 7.4 to show each root of f in L is actually inside $\mathcal{O}_L$, and then conclude f splits into linear factors in $\ell[t]$.]

(b) From the definition of unramified extension we know taking residue fields, i.e. mapping $L \mapsto k_L$, defines a map

$$\left\{\begin{array}{c}\text{finite unramified extensions} \\ \text{of } K \text{ inside } \overline{K}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{finite separable extensions} \\ \text{of } k \text{ inside } \overline{k}\end{array}\right\}.$$

Prove this map is in fact a bijection in the following steps:

(1) Define an inverse map: if ℓ/k is finite separable and $\ell \subseteq \overline{k}$, let $f \in \mathcal{O}_K[t]$ be a monic lift of $m_{\alpha,k}$ and E be a splitting field of f over K inside $\overline{K}$. Use Hensel's lemma to show that there is a lift $a \in \mathcal{O}_E$ of α which is a zero of f, and take $L = K[a]$.

(2) Notice $\ell \subseteq k_L$. Prove the (in)equalities $[k_L : k] \leqslant [K[a] : K] = \deg(f) = \deg(m_{\alpha,k}) = [\ell : k]$ and use this to conclude that $\ell = k_L$ and L/K is unramified.

(3) Use Problem 8.8 to show if one had $\ell = k[\alpha']$ for some other α', and one takes a corresponding lift a' instead, then $K[a] = K[a']$, which shows the construction we've made is independent of α. This together with (2) tell us the function we've written is well-defined.

(4) Show this gives us the inverse we want.

(c) Prove if L/K is unramified and ℓ is the residue field of L then L/K is Galois if and only if ℓ/k is Galois.

(d) If L/K is finite, recall/prove that the uniqueness of the extension of the norm to L implies that $|\sigma(x)| = |x|$ for any $x \in L$ and $\sigma \in \mathrm{Aut}_K(L)$. Conclude that any such σ defines a corresponding element of $\mathrm{Aut}_k(\ell)$, and that the resulting map $\mathrm{Aut}_K(L) \longrightarrow \mathrm{Aut}_k(\ell)$ is a group homomorphism.

(e) Prove when the conditions of (c) hold the map $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(\ell/k)$ from (d) is an isomorphism. [Hint: because the two extensions have equal degree one just needs to show injectivity. Choosing α, a as in Problem 8.8, if $\sigma \mapsto \mathrm{id}_\ell$ under our map then this means that $\sigma(a) \equiv a \bmod \mathfrak{m}_L$; use uniqueness from Hensel's lemma to deduce in fact that $\sigma(a) = a$, so $\sigma = \mathrm{id}_L$.]

Using this result we can completely classify the unramified extensions of $\mathbf{Q}_p$: there is one (up to isomorphism, or exactly one inside a fixed algebraic closure) of degree n for each $n \in \mathbf{N}$, corresponding to the unique extension $\mathbf{F}_{p^n}/\mathbf{F}_p$ of degree n. One often denotes this by $\mathbf{Q}_{p^n}$; let us try to describe it more explicitly.

Problem 8.12. Fix some algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$.

(a) Prove if $K/\mathbf{Q}_p$ is a finite extension, then K contains a primitive $(p^f - 1)$-th root of unity, where $f = f(K/\mathbf{Q}_p)$. [Hint: because the group of $(p^f - 1)$-th roots of unity in K must be cyclic, it suffices to prove K has $p^f - 1$ such roots of unity; to do this apply Hensel's lemma repeatedly to $t^{p^f-1} - 1$ (which splits in k), obtaining one root at a time.]
(b) Let $\mathbf{Q}_{p^n}$ be the degree n unramified extension of $\mathbf{Q}_p$ inside $\overline{\mathbf{Q}}_p$. Use (a) to show $\mathbf{Q}_{p^n}$ contains a primtive $(p^n - 1)$-th root of unity; let's call it ζ and let $K = \mathbf{Q}_p[\zeta]$.
(c) Use the uniqueness in Hensel's lemma to prove $\overline{\zeta} \in k$ is also a primitive $(p^n - 1)$-th root of unity; conclude $f(K/\mathbf{Q}_p) \geqslant n$ and use this to show that $\mathbf{Q}_{p^n} = K = \mathbf{Q}_p[\zeta]$.

This problem actually lets us describe the maximal unramified extension of $\mathbf{Q}_p$:

Problem 8.13. Prove the maximal unramfied of $\mathbf{Q}_p$ is given by $\mathbf{Q}_p^{\mathrm{nr}} = \bigcup_{(m,p)=1} \mathbf{Q}_p[\zeta_m]$ where ζ_m is a primitive m-th root of unity for each m. [Hint: on one hand, any finite unramified extension of $\mathbf{Q}_p$ is equal to $\mathbf{Q}_p[\zeta_m]$ for some $m = p^n - 1$, and on the other hand if $(m, p) = 1$ one can find some n such that $m | p^n - 1$.]

Remark 8.14. Let us note one more interesting consequence of Theorem 8.11, particularly part (e), is the following: if $\mathrm{char}(k) = p$ (so for instance if K is a finite extension of $\mathbf{Q}_p$ this holds), and L/K is finite Galois, then there is a natural isomorphism $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(\ell/k)$, and the right side has a distinguished element one often considers: the Frobenius element. The inverse of the Frobenius element under this isomorphism gives an element $\mathrm{Fr}_{L/K} \in \mathrm{Gal}(L/K)$, which we call the *Frobenius* of L/K. Note that, when $\mathrm{char}(K) = 0$, this cannot possibly be Frobenius in the sense of $x \mapsto x^p$ because this would never give a homomorphism. But what is true is that it satisfies $\mathrm{Fr}_{L/K}(x) \equiv x^p \bmod \mathfrak{m}_K$ for all $x \in \mathcal{O}_L$.

In addition, one can see that if $L \subseteq E$ and L, E are both unramified Galois extensions of K then from commutativity of the diagram

$$\begin{array}{ccc} \mathrm{Gal}(E/K) & \xrightarrow{\simeq} & \mathrm{Gal}(\varepsilon/k) \\ \big\downarrow{\scriptstyle \mathrm{res}} & & \big\downarrow{\scriptstyle \mathrm{res}} \\ \mathrm{Gal}(L/K) & \xrightarrow{\simeq} & \mathrm{Gal}(\ell/k) \end{array}$$

one has $\mathrm{Fr}_{E/K}|_L = \mathrm{Fr}_{L/K}$. As a result, the Frobenius elements "glue" to a single Frobenius $\mathrm{Fr}_K \in \mathrm{Gal}(K^{nr}/K)$. The Frobenius elements play an important role when one does class field theory, and we will see a bit of this next week.

References

[AM16] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra*. Westview Press, 2016.

[Cona] K. Conrad. Equivalent Norms. https://kconrad.math.uconn.edu/blurbs/gradnumthy/equivnorms.pdf.

[Conb] K. Conrad. Ostrowski's Theorem for Q. https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskiQ.pdf.

[Gou03] F. Gouvêa. *p-adic Numbers: an Introduction*. Springer-Verlag, 2003.

[Neu92] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1992.

[Rob00] J. Roberts. *A Course in p-adic Analysis*. Springer, 2000.

[Sta] The Stacks project authors. The Stacks project. https://stacks.math.columbia.edu.