18.782 Introduction to Arithmetic Geometry **Fall 2020**
Problem Set #3 **Due: 9/25/2020**

These problems are related to the material covered in Lectures 5-7. I have made every effort to proof-read them, but there are may be errors that I have missed. The first person to spot each error will receive 1-5 points of extra credit.

The problem set is due by 5pm on 9/25/2020 and should be submitted electronically as a pdf-file e-mailed to zzyzhang@mit.edu and roed@mit.edu. You can use the latex source for this problem set as a template for writing up your solutions; be sure to include your name in your solutions and remember to identify all collaborators and any sources that you consulted that are not listed in the syllabus.

Problem 1. Non-archimedean topology. (35 points)

Let k be a field with a non-archimedean absolute value $\| \ \|$. The metric $d(x, y) = \|x - y\|$ makes k a metric space whose topology is defined by the basis of open sets consisting of all *open balls* $B(x, r) = \{y : d(x, y) < r\}$ with $x \in k$ and $r \in \mathbb{R}_{>0}$.

Non-archimedean topology can be very counterintuitive, so be sure to keep in mind the following definitions, which apply to any topological space.

1. The collection of open sets is closed under arbitrary unions (including infinite unions) and finite intersections, and always includes the empty set and the whole space.
2. A set is closed if and only if its complement is open.
3. The *interior* of a set S is the union of all the open sets S contains, and the *closure* of S is the intersection of all the closed sets that contain S.

(a) Prove that every triangle in k is either equilateral, or acute isosceles. More precisely, for any $x, y, z \in k$ prove that the three distances $d(x, y), d(y, z), d(z, x)$ are either all equal, or two of them are equal and the third is smaller.

(b) Prove that every point in an open ball $B(x, r)$ is "at the center" by showing that $y \in B(x, r)$ implies $B(x, r) = B(y, r)$. Conclude that two balls are either disjoint or concentric (this means they have a common center).

(c) Prove that every open ball is closed (and therefore equal to its closure).

(d) Consider a *closed ball* $C(x, r) = \{y : d(x, y) \le r\}$. Prove that every point in $C(x, r)$ is at the center, and that every closed ball is open (and therefore equal to its interior).

(e) Consider a *sphere* $S(x, r) = \{y : d(x, y) = r\}$. Prove that every sphere is both open and closed.

(f) Prove that k is totally disconnected. This means that for all distinct $x, y \in k$ there are disjoint open sets X and Y containing x and y respectively, such that $k = X \bigcup Y$.

(g) For $k = \mathbb{Q}_p$ with the p-adic absolute value, prove that the closure of the open $B(x, r)$ is not necessarily the closed ball $C(x, r)$, but sometimes is (give examples of both). Prove that the total number of open balls is countable and that every open ball has uncountably many distinct radii (that is, $B(x, r) = B(x, r')$ for uncountably many r').

Problem 2. ***n*-adic rings (35 points)**

For any integer $n > 1$ define the *n-adic valuation* $v_n(x)$ of nonzero $x \in \mathbb{Q}$ to be the unique integer k for which $x = \frac{a}{b}n^k$, with $n \nmid a$, $\gcd(a,b) = 1$ and $\gcd(b,n) = 1$, and let $v_n(0) = \infty$. Now define the function $|\ |_n \colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ by

$$|x|_n = n^{-v_n(x)},$$

where $|0|_n = n^{-\infty}$ is understood to be 0.

(a) Prove that $|\ |_n$ is an absolute value if and only if n is prime, but that $|\ |_n$ always satisfies the non-archimedean triangle inequality $|x+y|_n \leq \max(|x|_n, |y|_n)$.

Let $A_k = \mathbb{Z}/n^k\mathbb{Z}$ and consider the inverse system of rings (A_k) with morphisms $A_{k+1} \to A_k$ given by reduction modulo n^k. Define the *ring of n-adic integers* as the inverse limit $\mathbb{Z}_n = \varprojlim A_k$ (this generalizes our definition of $\mathbb{Z}_p$).

(b) Prove that if n is not a prime power then $\mathbb{Z}_n$ is not an integral domain.

In view of (b), we cannot define $\mathbb{Q}_n$ as the fraction field of $\mathbb{Z}_n$ in general. But we can define $\mathbb{Q}_n$ as the completion of $\mathbb{Q}$ with respect to $|\ |_n$, in the same way that we constructed $\mathbb{Q}_p$ as the p-adic completion of $\mathbb{Q}$ (giving us an alternative definition of $\mathbb{Q}_p$).

(c) Formalize this definition of $\mathbb{Q}_n$ and show that it is a ring. Make it clear what the elements of $\mathbb{Q}_n$ are, define the ring operations, and extend the definition of $|\ |_n$ to $\mathbb{Q}_n$.

(d) Which of parts (a) to (g) in Problem 1 still apply if we replace k with $\mathbb{Q}_n$ and use the metric $d(x,y) = |x-y|_n$?

(e) Prove that for all prime powers p^e we have $\mathbb{Q}_{p^e} = \mathbb{Q}_p$.

(f) Prove that if $p_1, \ldots p_r$ are the distinct prime divisors of n then $\mathbb{Q}_n$ is isomorphic to the direct product of rings $\mathbb{Q}_{p_1} \oplus \cdots \oplus \mathbb{Q}_{p_r}$ and is not a field unless $r = 1$.

Problem 3. Quadratic extensions of $\mathbb{Q}_p$ (30 points)

Let p be a prime congruent to 3 mod 4.

(a) Prove that -1 does not have a square-root in $\mathbb{Q}_p$ and that the ideal $\mathfrak{p} = (p)$ is prime in $\mathbb{Z}[i]$, the ring of integers of $\mathbb{Q}(i)$.

(b) Consider the quadratic extension $\mathbb{Q}_p(i) = \mathbb{Q}_p[x]/(x^2+1)$ and extend the p-adic absolute value $|\ |_p$ from $\mathbb{Q}_p$ to $\mathbb{Q}_p(i)$ by defining for each $\alpha = a + bi \in \mathbb{Q}_p(i)$:

$$|\alpha|_p = |N_{\mathbb{Q}_p(i)/\mathbb{Q}_p}(\alpha)|_p^{1/[\mathbb{Q}_p(i):\mathbb{Q}_p]} = \sqrt{|a^2+b^2|_p}.$$

Prove that $|\ |_p$ is an absolute value on $\mathbb{Q}_p(i)$, and that $\mathbb{Q}_p(i)$ is complete with respect to this absolute value.

(c) For $\alpha \in \mathbb{Q}(i)$ define

$$|\alpha|_{\mathfrak{p}} = N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} = p^{-2v_{\mathfrak{p}}(\alpha)},$$

where $v_{\mathfrak{p}}(\alpha)$ is the $\mathfrak{p}$-adic valuation of α. Recall that the $\mathfrak{p}$-adic valuation of $\beta \in \mathbb{Z}[i]$ is the exponent of $\mathfrak{p}$ in the prime factorization of the $\mathbb{Z}[i]$-ideal (β), and this extends to $\mathbb{Q}(i)$ via $v_{\mathfrak{p}}(\beta/\gamma) = v_{\mathfrak{p}}(\beta) - v_{\mathfrak{p}}(\gamma)$ (note that $\mathbb{Q}(i)$ is the fraction field of its ring of integers $\mathbb{Z}[i]$). Let $\mathbb{Q}(i)_{\mathfrak{p}}$ denote the completion of $\mathbb{Q}(i)$ with respect to $|\ |_{\mathfrak{p}}$. Prove that $\mathbb{Q}_p(i)$ and $\mathbb{Q}(i)_{\mathfrak{p}}$ are isomorphic fields with equivalent (but not equal) absolute values.

(d) Prove that p does not have a square root in $\mathbb{Q}_p(i)$, thus the quadratic extensions $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(i)$ are distinct. Conclude that $\mathbb{Q}_p(\sqrt{-p})$ is also a quadratic extension of $\mathbb{Q}_p$, and it is distinct from both $\mathbb{Q}_p(i)$ and $\mathbb{Q}_p(\sqrt{p})$.

We will see that up to isomorphism, $\mathbb{Q}_p(i)$, $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{-p})$ are the only quadratic extensions of $\mathbb{Q}_p$, and that a similar statement holds for primes that are congruent to $1 \bmod 4$. This is in contrast to $\mathbb{Q}$, which has infinitely many non-isomorphic quadratic extensions, and to $\mathbb{Q}_\infty = \mathbb{R}$, which has only one.

(e) Recall that every field K with a nonarchimedean absolute value has an associated residue field, defined by $\mathcal{O}_K/\mathfrak{m}_K$, where

$$\mathcal{O}_K = \{x \in K : |x| \leq 1\}$$
$$\mathfrak{m}_K = \{x \in K : |x| < 1\}.$$

Compute the residue fields of $\mathbb{Q}_p(i)$ and $\mathbb{Q}_p(\sqrt{p})$.

Problem 4. Survey

Complete the following survey by rating each problem on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.