18.785 Number Theory **Fall 2018**

Problem Set #4 **Due: 10/10/2018**

Description

These problems are related to the material covered in Lectures 7–9. Your solutions are to be written in latex and submitted as a pdf-file named `SurnamePset4.pdf` (replace `Surname` with your surname) via e-mail to `drew@math.mit.edu` by noon on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references consulted other than the lecture notes. If there are none, write **Sources consulted: none** at the top of your problem set. The first person to spot each typo/error in the problem set or lecture notes will receive 1-5 points of extra credit.

Instructions: First do the warm up problems (especially if you have not seen p-adic fields before!), then pick any combination of problems 1–5 that sum to 96 points. Finally, complete the survey problem 6 (worth 4 points).

Problem 0.

These are warm up problems that do not need to be turned in.

(a) Give an example of a metric on a field that is not induced by an absolute value.

(b) Prove that the completion $\hat{k}$ of a field k at one of its absolute values $|\ |$ satisfies the following universal property: every topological field embedding of k into a complete field k' extends uniquely to an embedding of $\hat{k}$ into k' that is an isomorphism if and only if k is dense in k'.

(c) Compute the 3-adic expansions of $1/4$, $-5/6$ and $\sqrt{7}$ in $\mathbb{Q}_3$.

(d) Let X be a metric space defined by a nonarchimedean absolute value. Verify that (1) every point in an open ball is a center, (2) two open balls are either disjoint or concentric, (3) every open ball is closed and every closed ball is open, (4) all triangles are isosceles, (5) X is totally disconnected.

(e) Show that every $\alpha \in \mathbb{Q}_p^\times$ can be written uniquely in the form $\alpha = p^r u$ for some $r \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$.

Problem 1. Quadratic reciprocity (32 points)

Recall that for an odd prime p the *Legendre symbol* $\left(\frac{\cdot}{p}\right)\colon \mathbb{Z} \to \{-1, 0, 1\}$ defined by

$$\left(\frac{n}{p}\right) := \begin{cases} -1 & \text{if } n \text{ is not a square modulo } p; \\ 0 & \text{if } n \text{ is divisible by } p; \\ 1 & \text{if } n \text{ is a nonzero square module } p. \end{cases}$$

Gauss's theorem of quadratic reciprocity states that for odd primes $p \neq q$:

$$(1)\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}; \quad (2)\quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}; \quad (3)\quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

For any integer $n > 1$, let ζ_n denote a primitive nth root of unity.

(a) Prove that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

(b) Let $n > 1$ be an integer, let p a prime that does not divide n, and let $[p]$ denote the residue class of p in $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Prove that

$$\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{(p)}\right) = [p],$$

and conclude that for the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, the Artin map is surjective.

(c) Let p be an odd prime, and define $p^* := (-1)^{(p-1)/2}p$. Prove that $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$.

(d) By comparing values of the Artin map for suitably chosen cyclotomic and quadratic extensions of $\mathbb{Q}$, prove (1), (2), (3) (you may prove these in any order you wish).

Of the more than 200 proofs of quadratic reciprocity that are known, this one is certainly not the most elementary, but it is arguably the one that Gauss was looking for.

Problem 2. Weak approximation (32 points)

Let k be a field and for $n \in \mathbb{Z}_{\geq 1}$ let S_n and W_n denote the following statements:

S_n : *Given inequivalent nontrivial absolute values* $|\ |_1, \ldots, |\ |_n$ *on* k*, there is an* $x \in k^\times$ *for which* $|x|_1 > 1$ *and* $|x|_i < 1$ *for* $1 < i \leq n$.

W_n : *Given inequivalent nontrivial absolute values* $|\ |_1, \ldots, |\ |_n$ *on* k*, there is a sequence* $(x_1, x_2, \ldots)$ *of elements* $x_j \in k$ *that converges to* 1 *with respect to* $|\ |_1$ *and to* 0 *with respect to* $|\ |_i$ *for* $1 < i \leq n$.

(a) Prove that S_n implies W_n.

(b) Prove that S_n holds for all $n \geq 1$.

(c) Prove the Weak Approximation Theorem:

Given inequivalent nontrivial absolute values $|\ |_1, \ldots, |\ |_n$ *on* k*,* $a_1, \ldots, a_n \in k$*, and* $\epsilon_1, \ldots, \epsilon_n \in \mathbb{R}_{>0}$ *there exists* $x \in k$ *such that* $|x - a_i|_i < \epsilon_i$ *for* $i = 1, \ldots, n$.

(d) Let $|\ |_1$ and $|\ |_2$ be absolute values on k. Prove that the topologies on k induced by $|\ |_1$ and $|\ |_2$ coincide if and only if $|\ |_1 \sim |\ |_2$.

Problem 3. n-adic rings (64 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 nonarchimedean triangle inequality $|x+y|_n \leq \max(|x|_n, |y|_n)$; in particular, $d_n(x,y) := |x-y|_n$ is a nonarchimedean metric.

Let $A_k = \mathbb{Z}/n^k\mathbb{Z}$ and consider the inverse system consisting of the sequence 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 $\mathbb{Z}_n := \varprojlim A_k$.

(b) Compute the first three terms of the 10-adic expansions of -7, $1/3$, and $\sqrt[3]{3}$ in $\mathbb{Z}_{10}$ (as with the p-adic expansion defined in Lecture 8, each term is a decimal digit).

(c) For $n = p$ prime prove the fraction field of $\mathbb{Z}_p$ is (canonically isomorphic to) $\mathbb{Q}_p$, the completion of $\mathbb{Q}$ with respect to $|\ |_p$, and that $\mathbb{Z}_p$ is its valuation ring.

(d) Prove that $\mathbb{Z}_n$ is an integral domain if and only if n is a prime power.

In view of (d), we cannot construct the fraction field of $\mathbb{Z}_n$ in general, but we can still define $\mathbb{Q}_n$ as the completion $\mathbb{Q}_n$ of $\mathbb{Q}$ with respect to the metric $d_n(x,y) := |x-y|_n$.

(e) Prove that $\mathbb{Q}_n$ is a ring containing (subrings canonically isomorphic to) $\mathbb{Q}$ and $\mathbb{Z}_n$.

(f) Extend $|\ |_n$ to $\mathbb{Q}_n$, show that $d(x,y) := |x-y|_n$ is a metric on $\mathbb{Q}_n$.
Is $\mathbb{Q}_n$ a topological ring?

(g) For $n = p^e$ a prime power, prove that $\mathbb{Q}_n \simeq \mathbb{Q}_p$ (as topological fields).

(h) Prove that in general we have a ring isomorphism $\mathbb{Q}_n \simeq \prod_{p|n} \mathbb{Q}_p$.
If you answered yes to (f), do we also have an isomorphism of topological rings?

Problem 4. Quadratic extensions of $\mathbb{Q}_p$ (32 points)

(a) Let $p \equiv 3 \bmod 4$ be prime, and let $\mathfrak{p}$ be the prime of $\mathbb{Q}(i)$ lying above p. Let $\mathbb{Q}_p(i)$ denote the extension of $\mathbb{Q}_p$ obtained by adjoining a square-root of -1, and let $\mathbb{Q}(i)_\mathfrak{p}$ denote the completion of $\mathbb{Q}(i)$ at the absolute value $|\cdot|_\mathfrak{p}$. Show that $\mathbb{Q}_p(i)$ has a unique absolute value extending the p-adic absolute value $|x|_p := p^{-v_p(x)}$, and that $\mathbb{Q}_p(i)$ and $\mathbb{Q}(i)_\mathfrak{p}$ are isomorphic local fields. Are their absolute values the same?

(b) Let p be an odd prime. Prove that $\mathbb{Q}_p$ has exactly 3 distinct quadratic extensions; describe them explicitly, determine which are ramified, and compute their residue fields (the quotient of the ring of integers by its unique maximal ideal).

(c) Prove that $\mathbb{Q}_2$ has exactly 7 distinct quadratic extensions; describe them explicitly, determine which are ramified, and compute their residue fields.

(d) Prove that for every positive integer n there exists a global number field (finite extension of $\mathbb{Q}$) with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$, but that for local number fields (finite extensions of $\mathbb{Q}_p$ for some prime p) this occurs only for $n \le 3$.

Problem 5. Roots of unity in $\mathbb{Q}_p$ (32 points)

Let $\mathbb{Q}_p^{\times n} = \{x^n : x \in \mathbb{Q}_p^\times\}$ denote the set of nth powers in $\mathbb{Q}_p^\times$.

(a) Prove that $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ when p is odd, and $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
(hint: use Hensel's lemmas).

(b) Determine the structure of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$ for all primes p and odd primes n.

Let $\mu_{n,p} = \{x \in \mathbb{Q}_p^\times : x^n = 1\}$ denote the set of nth roots of unity in $\mathbb{Q}_p$.

(c) Prove that $\mu_{n,p}$ is a cyclic group of order $\gcd(n, p-1)$ whenever $p \nmid n$, and that $\mu_{p,p}$ is trivial when p is odd.

(d) Prove that the roots of unity in $\mathbb{Q}_p$ form a cyclic subgroup of $\mathbb{Z}_p^\times$ that has order $p-1$ when p is odd, and order 2 when $p = 2$.

Problem 6. Survey (4 points)

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

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			
Problem 5			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
10/1	Completions and valuation rings				
10/3	Local fields, Hensel's lemmas				

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.