18.785 Number Theory **Fall 2015**

Problem Set #4

Description

These problems are related to the material covered in Lectures 7-9. Your solutions are to be written up in latex (you can use the latex source for the problem set as a template) and submitted as a pdf-file with a filename of the form `SurnamePset4.pdf` via e-mail to the instructor by **2pm** on the date due. Collaboration is permitted/ encouraged, but you must identify your collaborators, and any references you consulted. If there are none, write "**Sources consulted: none**" at the top of your problem set. The first person to spot each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit.

Instructions: First do the warm up problems, then pick two of problems 1-3 to solve and write up your answers in latex. Finally, be sure to complete the survey problem 4.

Problem 0.

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

(a) Let $\mathcal{O}_K$ be the ring of integers of an imaginary quadratic field K and let c be a positive integer. Prove that $\mathbb{Z} + c\mathcal{O}_K$ is an order with conductor $c\mathcal{O}_K$ and that $c = [\mathcal{O}_K : \mathcal{O}]$ is the index of $\mathcal{O}$ in $\mathcal{O}_K$ (as additive abelian groups).

(b) Prove that the completion $\hat{k}$ of a field k at one of its absolute values is complete, and that up to a canonical isomorphism it is uniquely determined by the following universal property: every embedding of k into a complete field k' extends to an embedding of $\hat{k}$ into 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) X is totally disconnected.

Problem 1. Orders in Dedekind domains (50 points)

Let $\mathcal{O}$ be an order (noetherian domain of dimension one with nonzero conductor) with integral closure B (a Dedekind domain) and conductor $\mathfrak{c}$ (largest B-ideal in $\mathcal{O}$).

(a) Prove that for a prime $\mathfrak{p}$ of $\mathcal{O}$ the following are equivalent:

(a) $\mathfrak{p}$ does not contain $\mathfrak{c}$;

(b) $\mathcal{O} = \{x \in B : x\mathfrak{p} \subseteq \mathfrak{p}\}$;

(c) $\mathfrak{p}$ is invertible (as a fractional $\mathcal{O}$-ideal);

(d) $\mathcal{O}_\mathfrak{p}$ is a DVR;

(e) $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a principal $\mathcal{O}_\mathfrak{p}$-ideal.

Then show that these equivalent conditions all imply that $\mathfrak{p}B$ is a prime of B.

(b) Prove that nonzero fractional ideals I of $\mathcal{O}$ prime to $\mathfrak{c}$ are invertible, but that the converse need not hold (give an explicit counterexample).

(c) Let K be a number field with ring of integers $\mathcal{O}_K$, let $c > 1$ be an integer, and let

$$\mathcal{O} := \mathbb{Z} + c\mathcal{O}_K = \{a + b : a \in \mathbb{Z}, b \in c\mathcal{O}_K\}.$$

Prove $\mathcal{O}$ is an order with integral closure $\mathcal{O}_K$ and conductor $c\mathcal{O}_K$, and that $c\mathcal{O}_K$ is not principal as an $\mathcal{O}$-ideal.

(d) Let $K = \mathbb{Q}(i)$ with $\mathcal{O}_K = \mathbb{Z}[i]$, let p be prime, and let $\mathcal{O} = \mathbb{Z} + p\mathbb{Z}[i]$. Then $\mathcal{O}$ is an order with integral closure $\mathcal{O}_K$, by part (c). Show that its conductor $\mathfrak{p} := p\mathbb{Z}[i]$ is prime as an $\mathcal{O}$-ideal (but need not be prime as an $\mathcal{O}_K$-ideal). Let $\mathfrak{a} := p^2\mathbb{Z} + pi\mathbb{Z}$. Prove $\mathfrak{a}$ is an $\mathcal{O}$-ideal contained in $\mathfrak{p}$ but not divisible by $\mathfrak{p}$.

Problem 2. Quadratic reciprocity (50 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. In this problem you may assume Dirichlet's theorem on primes in arithmetic progressions, which we will prove later in the course.

(a) Prove that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ (so $\mathbb{Q}(\zeta_n)$ is an abelian extension of $\mathbb{Q}$).

(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 $p^* := \left(\frac{-1}{p}\right)p$. 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 extension of $\mathbb{Q}$, prove (1).

(e) Similarly prove (2) and (3).

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 3. Quadratic extensions of $\mathbb{Q}_p$ (50 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 $\mathbb{Q}_p(i)$ and $\mathbb{Q}(i)_\mathfrak{p}$ are isomorphic local fields with equivalent absolute values, but that these absolute values differ by a power (give the power).

(b) Let p be an odd prime. Prove that $\mathbb{Q}_p$ has exactly 3 distinct quadratic extensions; describe them explicitly and determine which are ramified.

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

Problem 4. Survey

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			

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
10/6	Artin map, local fields				
10/8	Hensel's lemma, complete DVRs				

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.

18.785 Number Theory I
Fall 2015