18.785 Number Theory **Fall 2015**

Problem Set #2

Description

These problems are related to the material covered in Lectures 3-5. 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 via e-mail to the instructor by 5pm on the due date.
Collaboration is permitted, 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 any combination of problems 1–5 that sums to 99 points and write up your answers in latex. Finally, be sure to complete the survey problem 6.

Problem 0.

These are warm up problems that do not need to be written up or turned in. These should not take long and are simply provided to help you check your understanding.

(a) Let A be a Dedekind domain and I a nonzero ideal of A. Prove that every ideal in A/I is principal and use this to give an alternative proof of the fact that every ideal in A can be generated by at most two elements (Theorem 3.32).

(b) Let k be a field. Prove that an irreducible polynomial $f \in k[x]$ is inseparable if and only if it is of the form $f(x) = g(x^p)$ for some $g \in k[x]$ with $p = \mathrm{char}(k) \neq 0$.

(c) Let B be an A-algebra that is free of rank n as an A-module. Prove $\mathrm{N}_{B/A}(a) = a^n$ and $\mathrm{T}_{B/A}(a) = na$ for all $a \in A$.

(d) Let $K = \mathbb{Q}(\zeta_5)$ be the number field generated by a primitive 5th root of unity ζ_5. Show that $K \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathbb{R}^4$ as an $\mathbb{R}$-vector space but as an $\mathbb{R}$-algebra it is isomorphic to $\mathbb{C}^2 \not\cong \mathbb{R}^4$.

Problem 1. Dedekind domains (33 points)

(a) Let A be a local domain whose maximal ideal is nonzero. Prove that if every nonzero ideal of A is invertible then A is a DVR (and therefore a Dedekind domain).

(b) Let A be a noetherian domain in which every nonzero ideal I is invertible. Prove that A is a Dedekind domain.

(c) Let A be a noetherian domain in which every nonzero ideal $I \neq A$ can be uniquely factored into prime ideals. Prove that A is a Dedekind domain.

(d) Show that the noetherian hypothesis in (b) and (c) is unnecessary.

(e) Show that the uniqueness hypothesis in (c) is unnecessary.

(f) Let A be a noetherian domain in which "to contain is to divide" holds, that is, a prime ideal $\mathfrak{p}$ contains an ideal I if and only if $I = \mathfrak{p}J$ for some ideal J. Must A be a Dedekind domain? If not, what additional hypotheses on A are necessary?

Problem 2. Factoring primes in quadratic fields (33 points)

This is a follow-up to Problem 3 on Problem Set 1. Let $p, q \in \mathbb{Z}$ denote primes.

(a) Let K be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$, and let

$$(q) = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$$

be the unique factorization of the principal ideal (q) in $\mathcal{O}_K$. Show that

$$[\mathcal{O}_K : q\mathcal{O}_K] = q^2 = \sum_{i=1}^{n} e_i [\mathcal{O}_K : \mathfrak{q}_i],$$

and conclude that there are three possibilities: (q) is prime, $(q) = \mathfrak{q}_1\mathfrak{q}_2$, or $(q) = \mathfrak{q}_1^2$.

(b) For $K := \mathbb{Q}(\sqrt{p})$ determine the unique factorization of (q) in $\mathcal{O}_K$ explicitly; that is, determine which of the three possibilities admitted by (a) occurs and when applicable, write $\mathfrak{q}_i$ in the form (q, α_i) for some explicitly described $\alpha \in \mathcal{O}_K$. Be sure to address the cases $q = 2$ and $q = p$ which may require special treatment.

(c) Do the same for $K := \mathbb{Q}(\sqrt{-p})$.

Problem 3. Weak approximation (33 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 $|\cdot|_1, \ldots, |\cdot|_n$ 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 $|\cdot|_1, \ldots, |\cdot|_n$ on k, there is a sequence $(x_1, x_2, \ldots)$ of elements $x_j \in k$ that converges to 1 with respect to $|\cdot|_1$ and to 0 with respect to $|\cdot|_i$ for $1 < i \leq n$.*

(a) Prove S_2 (hint: consider the set $\{(\log|x|_1, \log|x|_2) : x \in k^\times\} \subseteq \mathbb{R}^2$).

(b) Prove that S_n implies W_n.

(c) For each $n \geq 2$ prove that S_2 and S_n imply S_{n+1}.

(d) Prove that S_n and W_n hold for all n.

(e) Prove the Weak Approximation Theorem:

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

Problem 4. Norm and trace in inseparable extensions (33 points)

Let L be a finite extension of a field K. Let Ω be an algebraically closed field containing K and let $\Sigma = \mathrm{Hom}_K(L, \Omega)$. Recall that the degree $[L:K]$ of the extension L/K can be written as

$$[L:K] = [L:K]_s[L:K]_i,$$

where $[L:K]_s := \#\Sigma$ and $[L:K]_i$ denote the separable and inseparable degrees of L/K.

(a) Prove that for all $b \in L$ we have

$$N_{L/K}(b) = \left(\prod_{\sigma\in\Sigma} \sigma(b)\right)^{[L:K]_i}.$$

(b) Prove that for all $b \in L$ we have

$$T_{L/K}(b) = [L:K]_i \left(\sum_{\sigma\in\Sigma} \sigma(b)\right).$$

(c) Prove that $T_{L/K} = 0$ (as a linear map) if and only if L/K is inseparable.

Problem 5. Fermat's last theorem (66 points)[1]

Recall that Fermat's Last Theorem (FLT) states that

$$x^n + y^n = z^n$$

has no integer solutions with $xyz \neq 0$ for $n > 2$. By removing common factors we may assume $\gcd(x, y, z) = 1$, and we may assume that $n = p$ is a prime greater than 5, since the cases $n = 3$ and $n = 4$ were proved by Euler and Fermat (respectively), and we can easily reduce to the case where either $n = p$ is prime or $n = 4$ (every solution with $n = ab$ also gives a solution with $n = a$ and $n = b$).

So let $p \geq 5$ be prime and suppose x, y, z are relatively prime integers for which

$$x^p + y^p = z^p$$

with $xyz \neq 0$, and let $\zeta_p \in \overline{\mathbb{Q}}$ denote a primitive pth root of unity (so $\zeta_p^p = 1$ but $\zeta_p \neq 1$). In order to simplify matters, we will make two further assumptions

(1) $xyz \neq 0 \bmod p$;

(2) the ring $\mathbb{Z}[\zeta_p]$ is a UFD.

You will prove below that under these assumptions, no such x, y, z can exist.

The first assumption is not necessary, your proof can be extended to remove this assumption. This was the basis of Lamé's "proof" of FLT in 1847, which relied on (2); unfortunately (2) holds only for $p \leq 19$. Kummer later generalized Lamé's argument to many cases where $\mathbb{Z}[\zeta_p]$ is not a UFD; Kummer's argument applies whenever the order of ideal class group of the ring of integers of $\mathbb{Q}(\zeta_p)$ is not divisible by p, which is expected to hold for infinitely many p (the set of so-called *regular* primes is believed to be infinite but this is not known).

For any $z \in \mathbb{Q}(\zeta_p)$, let $\bar{z}$ denote its complex conjugate. If S is a set, then $a \equiv b \bmod S$ means $a - b \in S$.

[1] This problem is adapted from [1, I, Ex.17-27]

(a) Show that $\zeta_p^i - \zeta_p^j$ properly divides p in the ring $\mathbb{Z}[\zeta_p]$ for any $i \neq j$.

(b) Show that if a non-unit $\alpha \in \mathbb{Z}[\zeta_p]$ divides $x + y\zeta_p^i$ then it does not divide $x + y\zeta_p^j$ for any $j \neq i$.

(c) Show that $x + y\zeta_p^i = u_i \alpha_i^p$ for some $\alpha_i \in \mathbb{Z}[\zeta_p]$ and $u_i \in \mathbb{Z}[\zeta_p]^\times$.

(d) Prove that $1 + t + \cdots + t^{p-1}$ is irreducible in $\mathbb{Q}[t]$; conclude that $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ is a basis for $\mathbb{Z}[\zeta_p]$ as a $\mathbb{Z}$-module.

(e) Show that in any commutative ring A we have $\alpha^p + \beta^p \equiv (\alpha + \beta)^p \bmod pA$ for all $\alpha, \beta \in A$.

(f) Let $\alpha \in \mathbb{Z}[\zeta_p]$. Show (1) $\alpha^p \equiv a \bmod p\mathbb{Z}[\zeta_p]$ for some $a \in \mathbb{Z}$, (2) $\alpha^p \equiv \bar{\alpha}^p \bmod p\mathbb{Z}[\zeta_p]$, (3) $p \notin \mathbb{Z}[\zeta_p]^\times$, and (4) if $u \in \mathbb{Z}[\zeta_p]^\times$ then $u/\bar{u} \neq -\zeta_p^i$ for any i.

(g) Show that if $\alpha \in \overline{\mathbb{Q}}^\times$ is an algebraic integer whose Galois conjugates all lie in the unit disk in $\mathbb{C}$ then α is a root of unity.

(h) Show that if $u \in \mathbb{Z}[\zeta_p]^\times$ then $u/\bar{u} = \zeta_p^i$ for some i.

(i) Show that if $x + y\zeta_p \equiv u\alpha^p \bmod p\mathbb{Z}[\zeta_p]$ with $u \in \mathbb{Z}[\zeta_p]^\times$, then for some $0 \leq j \leq p-1$ we must have $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \bmod p\mathbb{Z}[\zeta_p]$.

(j) Show that $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \bmod p\mathbb{Z}[\zeta_p]$ only if $j = 1$.

(k) Show that if $x + y\zeta_p \equiv x\zeta_p + y \bmod p\mathbb{Z}[\zeta_p]$ then $x \equiv y \bmod p$.

(l) Assuming $\mathbb{Z}[\zeta_p]$ is a UFD, show $x^p + y^p = z^p$ has no solutions with $xyz \neq 0 \bmod p$.

Problem 6. Survey (1 point)

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
9/22	Norm and trace				
9/24	Factoring primes				

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.

References

[1] Dino Lorenzini, *An invitation to arithmetic geometry*, Graduate Studies in Mathematics **9**, American Mathematical Society, 1996.

18.785 Number Theory I
Fall 2015