18.785 Number Theory **Fall 2019**

Problem Set #2

Description

These problems are related to the material covered in Lectures 3–4. 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 typo/error in any of the problem sets or lecture notes will receive 1–5 points of extra credit.

Instructions: Solve Problem 0 (take the time to at least convince yourself that you know how to solve each part; come to office hours if you do not), then pick one of Problems 1-2 and one of Problems 3-4 to solve. Finally, complete the survey, Problem 5.

Problem 0. Warmup (0 points)

These warmup exercises do not need to be written up. I urge you to at least think through these problems (they should not take long).

(a) Let I, J, K be nonzero ideals in a noetherian (not necessarily Dedekind) domain. Show that $(I : J + K) = (I : J) \cap (I : K)$.

(b) Let K be the field $\mathbb{F}_p(x, y)$ and consider the field $L := K[t]/(t^{p^2} + t^p x + y)$. Show that L/K can be decomposed as a purely inseparable extension of a separable extension, but not as a separable extension of a purely inseparable extension.

(c) Let K and L be two number fields. Describe the finite ètale K-algebra $L \otimes_{\mathbb{Q}} K$ when $L \subseteq K$, $K \subseteq L$, $K = L$, $K \cap L = \mathbb{Q}$, and then in general.

(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 not as an $\mathbb{R}$-algebra.

(e) Let p be a prime. Prove that there are exactly four (unital) commutative rings of cardinality p^2, two of which are finite ètale $\mathbb{F}_p$-algebras. Of these four, which arise as A/I for some discrete valuation ring A and ideal I?

Problem 1. Characterizing Dedekind domains (64 points)

Recall that we defined a Dedekind domain to be an integrally closed noetherian domain of dimension at most one, or equivalently, a noetherian domain whose localizations at nonzero prime ideals are discrete valuation rings (see Proposition 2.9); let (D) denote either of these equivalent conditions. In Lecture 3 we proved that every Dedekind domain A enjoys the following properties:

(a) Each nonzero prime ideal of A is invertible.

(b) Each nonzero ideal of A is a (finite) product of prime ideals.

(c) A is noetherian and *to contain is to divide*: $J \supseteq I \Rightarrow J|I$ for all ideals I, J.

(d) For each ideal I in A there exists a nonzero ideal J such that IJ is principal.

(e) The quotient A/I of A by any nonzero ideal I is a principal ideal ring.

(f) If a is a nonzero element of an ideal I then $I = (a, b)$ for some $b \in I$.

In this problem you will prove that for any integral domain A, each of the conditions above implies (D). You may prove these implications any order (e.g. it suffices to just prove (a)⇒(b) in your answer for part **(a)** so long as you eventually prove (b)⇒(D)). You may want to first consider the case where A is a noetherian local domain.

(a) Prove (a)⇒(D).

(b) Prove (b)⇒(D).

(c) Prove (c)⇒(D).

(d) Prove (d)⇒(D).

(e) Prove (e)⇒(D).

(f) Prove (f)⇒(D).

(g) Show that the noetherian integral domain $A = \mathbb{Z}[\sqrt{-3}]$ of dimension one is *not* a Dedekind domain in two ways: show that it is not integrally closed and exhibit a nonzero prime ideal $\mathfrak{p}$ for which $A_{\mathfrak{p}}$ is not a DVR. Then give similarly explicit demonstrations that A does not satisfy each of the properties (a)-(f) above.

Problem 2. Fermat's last theorem (64 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 is a prime $p \geq 5$, 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.

[1] This problem is adapted from [**?**, I, Ex.17-27] but corrects/clarifies a number of minor issues there.

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 the sake of concreteness, let us fix an embedding of $\mathbb{Q}(\zeta_p)$ in $\mathbb{C}$ by defining $\zeta_p := e^{2\pi i/p}$, and for any $z \in \mathbb{Q}(\zeta_p) \subseteq \mathbb{C}$, let $\bar{z}$ denote its complex conjugate. If S is a set, then $a \equiv b \bmod S$ means $a - b \in S$.

(a) Show that $\zeta_p^i - \zeta_p^j$ properly divides p in the ring $\mathbb{Z}[\zeta_p]$ for any $i \not\equiv j \bmod p$.

(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 $j \not\equiv i \bmod p$.

(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 $j \equiv 1 \bmod p$.

(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 $xyz \not\equiv 0 \bmod p$.

Problem 3. Factoring primes in quadratic fields (32 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

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

(where $[B : A]$ denotes the index of A in B as an additive abelian group), 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 $K := \mathbb{Q}(\sqrt{-p})$.

(d) For primes $p, q \neq 2$, let $K := \mathbb{Q}(\sqrt{\pm p})$ and relate the factorization of (q) in $\mathcal{O}_K$ you determined in parts (b) and (c) to the factorization of $x^2 \mp p$ in $\mathbb{F}_q[x]$.

Problem 4. Computing the norm and trace (32 points)

Let L/K be a finite extension of fields, let $\overline{K}$ be an algebraic closure of K containing L, and define $\Sigma := \mathrm{Hom}_K(L, \overline{K})$.

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

$$N_{L/K}(\alpha) = \left(\prod_{\sigma\in\Sigma} \sigma(\alpha)\right)^{[L:K]_i} \qquad \text{and} \qquad T_{L/K}(\alpha) = [L:K]_i \left(\sum_{\sigma\in\Sigma} \sigma(\alpha)\right).$$

Fix $\alpha \in L^\times$ with minimal polynomial $f(x) = \sum a_i x^i$ over K, and let $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ be the factorization of f in $\overline{K}[x]$. Define $n := [L : K]$ and $e := [L : K(\alpha)]$ (so $de = n$).

(b) Prove that

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{d} \alpha_i^e = (-1)^n a_0^e \qquad \text{and} \qquad \mathrm{T}_{L/K}(\alpha) = \sum_{i=1}^{d} e\alpha_i = -e a_{d-1}.$$

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

Problem 5. 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			

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
9/11	Properties of Dedekind domains				
9/16	Étale algebras, norm and trace				

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 2019