

---

## 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 on the due date. 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:** First do problem 0, then pick *one* of problems 1 and 2 and *one* of problems 3 and 4 to solve. Then complete the survey problem 5.

## Problem 0.

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

- (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  $K$  and  $L$  be two number fields. Describe the finite étale  $K$ -algebra  $L \otimes_{\mathbb{Q}} K$  when  $L \subseteq K$ ,  $K \subseteq L$ ,  $K = L$ ,  $K \cap L = \mathbb{Q}$ , and then in general.
- (c) Let  $B$  be an  $A$ -algebra that is free of rank  $n$  as an  $A$ -module. Prove  $N_{B/A}(a) = a^n$  and  $T_{B/A}(a) = na$  for all  $a \in A$ .
- (d) Let  $K = \mathbb{Q}(\zeta_5)$  be the number field generated by a primitive 5th root of unity  $\zeta_5$ . 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.

## Problem 1. Characterizing Dedekind domains (66 points)

Recall that we defined a Dedekind domain to be an integrally closed noetherian domain of dimension at most one, equivalently, a noetherian domain whose localizations at nonzero prime ideals are discrete valuation rings; let (D) denote either of these equivalent conditions. In Lecture 3 we proved that every integral domain  $A$  that satisfies (D) also 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 an integral domain  $A$  each of these implies (D). You may prove these implications any order (e.g. it suffices to just prove (a) $\Rightarrow$ (b) in your answer for part (a) so long as you eventually prove (b) $\Rightarrow$ (D)).

- (a) Prove (a) $\Rightarrow$ (D).
- (b) Prove (b) $\Rightarrow$ (D).
- (c) Prove (c) $\Rightarrow$ (D).
- (d) Prove (d) $\Rightarrow$ (D).
- (e) Prove (e) $\Rightarrow$ (D).
- (f) Prove (f) $\Rightarrow$ (D).
- (g) Show that the noetherian integral domain  $A = \mathbb{Z}[\sqrt{-3}]$  is *not* a Dedekind domain by exhibiting a prime ideal  $\mathfrak{p} \neq (0)$  for which  $A_{\mathfrak{p}}$  is not a DVR. Then give similarly explicit counterexamples for each of the properties (a)-(f) above.

## Problem 2. Fermat's last theorem (66 points)<sup>1</sup>

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  $p$ th 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)  $xyz \not\equiv 0 \pmod{p}$ ;
- (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 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  $a \equiv b \pmod{S}$  means  $a - b \in S$ .

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

- (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  $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$  is a basis for  $\mathbb{Z}[\zeta_p]$  as a  $\mathbb{Z}$ -module.
- (e) Show that in any commutative ring  $A$  we have  $\alpha^p + \beta^p \equiv (\alpha + \beta)^p \pmod{pA}$  for all  $\alpha, \beta \in A$ .
- (f) Let  $\alpha \in \mathbb{Z}[\zeta_p]$ . Show (1)  $\alpha^p \equiv a \pmod{p\mathbb{Z}[\zeta_p]}$  for some  $a \in \mathbb{Z}$ , (2)  $\alpha^p \equiv \bar{\alpha}^p \pmod{p\mathbb{Z}[\zeta_p]}$ , (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  $\alpha$  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  $x + y\zeta_p \equiv u\alpha^p \pmod{p\mathbb{Z}[\zeta_p]}$  with  $u \in \mathbb{Z}[\zeta_p]^\times$ , then for some  $0 \leq j \leq p-1$  we must have  $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \pmod{p\mathbb{Z}[\zeta_p]}$ .
- (j) Show that  $x + y\zeta_p \equiv (x + y\zeta_p^{-1})\zeta_p^j \pmod{p\mathbb{Z}[\zeta_p]}$  only if  $j = 1$ .
- (k) Show that if  $x + y\zeta_p \equiv x\zeta_p + y \pmod{p\mathbb{Z}[\zeta_p]}$  then  $x \equiv y \pmod{p}$ .
- (l) Assuming  $\mathbb{Z}[\zeta_p]$  is a UFD, show  $x^p + y^p = z^p$  has no solutions with  $xyz \neq 0 \pmod{p}$ .

### Problem 3. 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

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

(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  $(q, \alpha_i)$  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  $K := \mathbb{Q}(\sqrt{\mp p})$  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 (33 points)**

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

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

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

Now fix  $\alpha \in L$  with minimal polynomial  $f(x) = \sum a_i x^i$  over  $K$ , and let  $f(x) = \prod_1^d (x - \alpha_i)$  be the factorization of  $f$  in  $\bar{K}[x]$ . Define  $n := [L:K]$  and  $e := [L:K(\alpha)]$  (so  $de = n$ ).

(b) Prove that

$$N_{L/K}(\alpha) = \prod_{i=1}^d \alpha_i^e = (-1)^n a_0^e \quad \text{and} \quad T_{L/K}(\alpha) = \sum_{i=1}^d e \alpha_i = -e a_{d-1}.$$

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

**Problem 5. Survey (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 |          |            |            |

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 |
|------|------------------|----------|--------------|------|---------|
| 9/20 | Norm and trace   |          |              |      |         |
| 9/22 | 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.

MIT OpenCourseWare  
<https://ocw.mit.edu>

18.785 Number Theory I  
Fall 2016

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.