

## Description

These problems are related to the material covered in Lectures 10-12. 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 `SurnamePset6.pdf` via e-mail to `drew@math.mit.edu` by **5pm** 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 problem, then pick problems that sum to 99 points to solve and write up your answers in latex. Finally, complete the survey problem 5.

## Problem 0.

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

- (a) Prove that the absolute discriminant of a number field must be a square mod 4.
- (b) Compute the different ideal of the quadratic extensions  $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$  and  $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ .
- (c) Determine all the primes that ramify in the cubic fields  $\mathbb{Q}[x]/(x^3 - x - 1)$  and  $\mathbb{Q}[x]/(x^3 + x + 1)$  and compute their ramification indices.
- (d) Let  $p$  be an odd prime. Compute the different ideal and absolute discriminant of the cyclotomic extension  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ .

## Problem 1 The different ideal (66 points)

Let  $A$  be a Dedekind domain with fraction field  $K$ , let  $L/K$  be a finite separable extension, and let  $B$  be the integral closure of  $A$  in  $L$ . Write  $L = K(\alpha)$  with  $\alpha \in B$  and let  $f \in A[x]$  be the minimal polynomial of  $\alpha$ , with degree  $n = [L : K]$ .

- (a) By comparing the Laurent series expansion of  $1/f(x)$  with its partial fraction decomposition over the splitting field of  $f$  (the Galois closure of  $L$ ), prove that

$$T_{L/K} \left( \frac{\alpha^i}{f'(\alpha)} \right) = \begin{cases} 0 & \text{if } 0 \leq i \leq n-2; \\ 1 & \text{if } i = n-1; \\ \in A & \text{if } i \geq n. \end{cases}$$

- (b) Suppose  $B = A[\alpha]$ . Prove that  $B^* := \{x \in L : T_{L/K}(xb) \in A \text{ for all } b \in B\}$  is the principal fractional  $B$ -ideal  $(1/f'(\alpha))$ . Conclude that  $\mathcal{D}_{B/A} = (f'(\alpha))$ .
- (c) For any  $\beta \in B$  with minimal polynomial  $g \in A[x]$  define

$$\delta_{B/A}(\beta) = \begin{cases} g'(\beta) & \text{if } L = K(\beta); \\ 0 & \text{otherwise.} \end{cases}$$

One can show that  $\mathcal{D}_{B/A}$  is the  $B$ -ideal generated by  $\{\delta_{B/A}(\beta) : \beta \in B\}$  (you are not required to prove this). Prove that if  $g$  is the minimal polynomial of  $\beta \in B$  for which  $L = K(\beta)$  then  $N_{B/A}(g'(\beta)) = \pm \text{disc}(g)$ .

- (d) Prove or disprove:  $D_{B/A}$  is the  $A$ -ideal generated by  $\{N_{B/A}(\delta_{B/A}(\beta)) : \beta \in B\}$ .  
 (e) Let  $\mathfrak{c}$  be the conductor of the order  $C = A[\alpha]$ . Prove that

$$\mathfrak{c} = (B^* : C^*) := \{x \in L : xC^* \subseteq B^*\}.$$

Conclude that if we define  $\mathcal{D}_{C/A} := (B : C^*)$  and  $D_{C/A} := D(C)$  then we have  $\mathcal{D}_{C/A} = \mathfrak{c}\mathcal{D}_{B/A}$  and  $D_{C/A} = N_{B/A}(\mathfrak{c})D_{B/A}$ , so that  $D_{C/A} = N_{B/A}(\mathcal{D}_{C/A})$ .

- (f) Let  $\mathfrak{q}$  be a prime of  $B$  lying above a prime  $\mathfrak{p}$  of  $A$  and suppose the corresponding residue field extension is separable. Prove that  $v_{\mathfrak{q}}(\mathcal{D}_{B/A}) \geq e_{\mathfrak{q}} - 1$  with equality if and only if  $B/A$  is tamely ramified at  $\mathfrak{q}$ .  
 (g) Let  $p$  and  $q$  be distinct primes congruent to 1 mod 4, let  $K := \mathbb{Q}(\sqrt{pq})$ , and let  $L := \mathbb{Q}(\sqrt{p}, \sqrt{q})$ . Prove that  $\mathcal{D}_{L/K}$  is the unit ideal (so  $L/K$  is unramified).

## Problem 2. Valuation rings (66 points)

An *ordered abelian group* is an abelian group  $\Gamma$  with a total order  $\leq$  that is compatible with the group operation. This means that for all  $a, b, c \in \Gamma$  the following hold:

$$\begin{aligned} a \leq b \leq a &\implies a = b && \text{(antisymmetry)} \\ a \leq b \leq c &\implies a \leq c && \text{(transitivity)} \\ a \not\leq b &\implies b \leq a && \text{(totality)} \\ a \leq b &\implies a + c \leq b + c && \text{(compatibility)} \end{aligned}$$

Note that totality implies reflexivity ( $a \leq a$ ). Given an ordered abelian group  $\Gamma$ , we define the relations  $\geq, <, >$  and the sets  $\Gamma_{\leq 0}, \Gamma_{\geq 0}, \Gamma_{< 0}$ , and  $\Gamma_{> 0}$  in the obvious way.

A *valuation*  $v$  on a field  $K$  is a surjective homomorphism  $v: K^\times \rightarrow \Gamma$  to an ordered abelian group  $\Gamma$  that satisfies  $v(x + y) \geq \min(v(x), v(y))$  for all  $x, y \in K^\times$ . The group  $\Gamma$  is called the *value group* of  $v$ , and when  $\Gamma = \{0\}$  we say that  $v$  is the *trivial valuation*. We may extend  $v$  to  $K$  by defining  $v(0) = \infty$ , where  $\infty$  is defined to be strictly greater than any element of  $\Gamma$ .

Recall that a *valuation ring* is an integral domain  $A$  with fraction field  $K$  such that for all  $x \in K^\times$  either  $x \in A$  or  $x^{-1} \in A$  (possibly both).

- (a) Let  $A$  be a valuation ring with fraction field  $K$ , and let  $v: K^\times \rightarrow K^\times/A^\times = \Gamma$  be the quotient map. Show that the relation  $\leq$  on  $\Gamma$  defined by

$$v(x) \leq v(y) \iff y/x \in A,$$

makes  $\Gamma$  an ordered abelian group and that  $v$  is a valuation on  $K$ .

- (b) Let  $K$  be a field with a non-trivial valuation  $v: K^\times \rightarrow \Gamma$ . Prove that the set

$$A := \{x \in K : v(x) \geq 0\}$$

is a valuation ring with fraction field  $K$  and that  $v(x) \leq v(y) \iff y/x \in A$ .

- (c) Let  $\Gamma$  be an ordered abelian group and let  $k$  be a field. For each  $a \in \Gamma_{\geq 0}$ , let  $x^a$  be a formal symbol, and define multiplication of these symbols via  $x^a x^b := x^{a+b}$ . Let  $A$  be the  $k$ -algebra whose elements are formal sums  $\sum_{a \in I} c_a x^a$ , where  $c_a \in k$  and the index set  $I \subseteq \Gamma_{\geq 0}$  is *well ordered* (every subset has a minimal element).<sup>1</sup> Let  $K$  be the fraction field of  $A$  and define  $v: K^\times \rightarrow \Gamma$  by

$$v\left(\frac{\sum c_a x^a}{\sum d_a x^a}\right) = \min\{a : c_a \neq 0\} - \min\{a : d_a \neq 0\}.$$

Prove that  $v$  is a valuation on  $K$  with value group  $\Gamma$  and valuation ring  $A$ .

- (d) Let  $v: K^\times \rightarrow \Gamma_v$  and  $w: K^\times \rightarrow \Gamma_w$  be two valuations on a field  $K$ , and let  $A_v$  and  $A_w$  be the corresponding valuation rings. Prove that  $A_v = A_w$  if and only if there is an order preserving isomorphism  $\rho: \Gamma_v \rightarrow \Gamma_w$  for which  $\rho \circ v = w$ , in which case we say that  $v$  and  $w$  are *equivalent*. Thus there is a 1-to-1 correspondence between valuation rings with fraction field  $K$  and equivalence classes of valuations on  $K$ .
- (e) Let  $A$  be an integral domain properly contained in its fraction field  $K$ , and let  $\mathcal{R}$  be the set of local rings that contain  $A$  and are properly contained in  $K$ . Partially order  $\mathcal{R}$  by writing  $R_1 \leq R_2$  if  $R_1 \subseteq R_2$  and the maximal ideal of  $R_1$  is contained in the maximal ideal of  $R_2$  (this is known as the *dominance ordering*). Prove that  $\mathcal{R}$  contains a maximal element  $R$  and that every such  $R$  is a valuation ring.
- (f) Prove that every valuation ring is local and integrally closed, and that the intersection of all valuation rings that contain an integral domain  $A$  and lie in its fraction field is equal to the integral closure of  $A$ .
- (g) Prove that a valuation ring that is not a field is a discrete valuation ring if and only if it is noetherian.

### Problem 3. Norm maps of local fields (33 points)

Let  $A$  be the valuation ring of a nonarchimedean local field  $K$ , let  $L$  be a tamely ramified extension of  $K$ , and let  $B$  be the integral closure of  $A$  in  $L$ . The goal of this problem is to prove that the extension  $L/K$  is unramified if and only if the norm map restricts to a surjective map of unit groups, equivalently,  $N_{L/K}(B^\times) = A^\times$ . Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be the maximal ideals of  $A$  and  $B$  and let  $k := A/\mathfrak{p}$  and  $l := B/\mathfrak{q}$  be the residue fields.

- (a) Prove that we always have  $N_{L/K}(B^\times) \subseteq A^\times$  and  $N_{l/k}(l^\times) = k^\times$  and  $T_{L/K}(l) = k$ .
- (b) For  $i \geq 0$  define  $U_i := 1 + \mathfrak{p}^i := \{1 + a : a \in \mathfrak{p}^i\}$ . Show that the  $U_i$  are distinct closed subgroups of  $A^\times$  that form a base of neighborhoods  $1 \in A^\times$  (this means every open neighborhood of 1 in the topological group  $A^\times$  contains some  $U_i$ ).
- (c) Prove that if  $L/K$  is not unramified then the norm of every  $b \in B^\times$  lies in a coset of  $U_1$  of the form  $u^n + U_1$  with  $n := [L : K] > 1$ . Show that these cosets do not cover  $A^\times$  and therefore  $N_{L/K}(B^\times) = A^\times$  can hold only if  $L/K$  is unramified.
- (d) Assume  $L/K$  is unramified. Show that for every  $u \in A^\times$  there exists  $\alpha_0 \in B^\times$  with  $N_{L/K}(\alpha_0) \equiv u \pmod{\mathfrak{p}}$ . Then construct  $\alpha_1 \in B^\times$  with  $N_{L/K}(\alpha_0 \alpha_1) \equiv u \pmod{\mathfrak{p}^2}$ . Continuing in this fashion, construct  $\alpha \in B^\times$  such that  $N_{L/K}(\alpha) = u$ .

<sup>1</sup>If  $\Gamma$  is well ordered you may fix  $I = \Gamma$  but in general  $I$  will vary from sum to sum; alternatively, index by  $\Gamma$  but require the indices of the nonzero coefficients to form a well-ordered subset of  $\Gamma$ .

**Problem 4. Minkowski’s lemma and sums of four squares (33 points)**

Minkowski’s lemma (for  $\mathbb{Z}^n$ ) states that if  $S \subseteq \mathbb{R}^n$  is a symmetric convex set of volume  $\mu(S) > 2^n$  then  $S$  contains a nonzero element of  $\mathbb{Z}^n$ .

Here *symmetric* means that  $S$  is closed under negation, and *convex* means that for all  $x, y \in S$  the set  $\{tx + (1 - t)y : t \in [0, 1]\}$  lies in  $S$ .

- (a) Prove that for any measurable  $S \subseteq \mathbb{R}^n$  with measure  $\mu(S) > 1$  there exist distinct  $s, t \in S$  such that  $s - t \in \mathbb{Z}^n$ , then prove Minkowski’s lemma.
- (b) Prove that Minkowski’s lemma is tight in the following sense: show that it is false if either of the words “symmetric” or “convex” is removed, or if the strict inequality  $\mu(S) > 2^n$  is weakened to  $\mu(S) \geq 2^n$  (give three explicit counter examples).
- (c) Prove that one can weaken the inequality  $\mu(S) > 2^n$  in Minkowski’s lemma to  $\mu(S) \geq 2^n$  if  $S$  is assumed to be compact.

You will now use Minkowski’s lemma to prove a theorem of Lagrange, which states that every positive integer is a sum of four integer squares. Let  $p$  be an odd prime.

- (d) Show that  $x^2 + y^2 = a$  has a solution  $(m, n)$  in  $\mathbb{F}_p^2$  for every  $a \in \mathbb{F}_p$ .
- (e) Let  $V$  be the  $\mathbb{F}_p$ -span of  $\{(m, n, 1, 0), (-n, m, 0, 1)\}$  in  $\mathbb{F}_p^4$ , where  $m^2 + n^2 = -1$ . Prove that  $V$  is *isotropic*, meaning that  $v_1^2 + v_2^2 + v_3^2 + v_4^2 = 0$  for all  $v \in V$ .
- (f) Use Minkowski’s lemma to prove that  $p$  is a sum of four squares.
- (g) Prove that every positive integer is the sum of four squares.

**Problem 5. 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			
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
10/20	Different and discriminant ideals				
10/25	Haar measure, product formula				

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.