18.785 Number Theory **Fall 2021**

Problem Set #6

Description

These problems are related to the material covered in Lectures 11–14. Your solutions should be written in latex and submitted as a pdf-file to by midnight on the date due.

Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on, as well any references you consulted that are not listed in the course syllabus. If there are none write "**Sources consulted: none**" at the top of your solution. Note that each student is expected to write their own solutions; it is fine to discuss the problems with others, but your work must be your own.

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, depending on the severity of the error

Instructions: First do the warm up problem, then pick problems that sum to 96 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 is always a square mod 4.

(b) Compute the different ideals of the quadratic fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$.

(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 (64 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 α, with degree $n = [L : K]$.

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

$$\mathrm{T}_{L/K}\left(\frac{\alpha^i}{f'(\alpha)}\right) = \begin{cases} 0 & \text{if } 0 \le i \le n-2; \\ 1 & \text{if } i = n-1; \\ \in A & \text{if } i \ge n. \end{cases}$$

(b) Suppose $B = A[\alpha]$. Prove that $B^* := \{x \in L : \mathrm{T}_{L/K}(xb) \in A \text{ for all } b \in B\}$ is the principal fractional B-ideal $(1/f'(\alpha))$. Conclude that $\mathcal{D}_{B/A} = (f'(\alpha))$.

(c) Prove that if g is the minimal polynomial of an element $\beta \in B$ for which $L = K(\beta)$ then $\mathrm{N}_{L/K}(g'(\beta)) = \pm\mathrm{disc}(g)$.

(d) By Proposition 12.25 we have $\mathcal{D}_{B/A} = (\delta_{B/A}(\beta)\colon \beta \in B)$, where $\delta_{B/A}(\beta)$ is $g'(\beta)$ if the minimal polynomial g of β has degree n and zero otherwise. Prove or disprove:

$$D_{B/A} \stackrel{?}{=} (\mathrm{N}_{L/K}(\delta_{B/A}(\beta)) : \beta \in B).$$

(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 $D_{C/A} = \mathrm{N}_{B/A}(\mathfrak{c})D_{B/A}$, so that $D_{C/A} = \mathrm{N}_{B/A}(\mathcal{D}_{C/A})$.

(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

$$e_{\mathfrak{q}} - 1 \le v_{\mathfrak{q}}(\mathcal{D}_{B/A}) \le e_{\mathfrak{q}} - 1 + v_{\mathfrak{q}}(e_{\mathfrak{q}}),$$

and that the lower bound is an equality only when it coincides with the upper bound (in which case B/A is tamely ramified at $\mathfrak{q}$).

(g) Show that the upper bound in (f) is essentially the best possible by exhibiting a wildly ramified degree-p extension of $\mathbb{Q}_p$ for which the upper bound is achieved, and showing that in the family of wildly ramified degree-p extensions of $\mathbb{F}_p((t))$ obtained by adjoining a root of $x^p + t^n x + t$ the valuation of the different ideal is unbounded as n increases (note that in this case $v_{\mathfrak{q}}(e_{\mathfrak{q}}) = v_{\mathfrak{q}}(p) = v_{\mathfrak{q}}(0) = \infty$, since we are in characteristic p, so (f) holds but imposes no upper bound).

(h) 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 (64 points)

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

$$\begin{array}{cccc} a \le b \le a & \Longrightarrow & a = b & \text{(antisymmetry)} \\ a \le b \le c & \Longrightarrow & a \le c & \text{(transitivity)} \\ a \not\le b & \Longrightarrow & b \le a & \text{(totality)} \\ a \le b & \Longrightarrow & a + c \le b + c & \text{(compatibility)} \end{array}$$

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

A *valuation* v on a field K is a surjective homomorphism $v\colon K^\times \to \Gamma$ to an ordered abelian group Γ that satisfies $v(x + y) \ge \min(v(x), v(y))$ for all $x, y \in K^\times$. The group Γ 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 ∞ is defined to be strictly greater than any element of Γ.

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 $v\colon K^\times \to K^\times/A^\times = \Gamma$ be the quotient map. Show that the relation $\le$ on Γ defined by

$$v(x) \le v(y) \Longleftrightarrow y/x \in A,$$

makes Γ an ordered abelian group and that v is a valuation on K.

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

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

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

Let Γ be an ordered abelian group and let k be a field. Let A be the set of functions $f\colon \Gamma \to k$ whose *support* $\operatorname{supp}(f) := \{a \in \Gamma : f(a) \ne 0$ is a *well ordered* subset of $\Gamma_{\ge 0}$, meaning that every nonempty subset of $\operatorname{supp}(z)$ has a minimal element.

(c) Prove that $S \subseteq \Gamma$ is well ordered is if and only if every infinite sequence of elements in S contains an infinite non-decreasing subsequence and use this to prove that if $S, T \subseteq \Gamma$ are well-ordered, so are $S + T := \{s + t : s \in S, t \in T\}$ and $S \cup T$.

(d) Prove that an ordered set is finite if and only if every subset has both a minimal and maximal element and use this to prove that for all well-ordered $S, T \subseteq \Gamma$ and every $a \in \Gamma$ the set $\{a + b : b \in S\} + \{a - b : b \in T\}$ is finite.

We now define addition and multiplication of elements of A by $(f + g)(a) := f(a) + g(a)$ and $(fg)(a) := \sum_{b\in\Gamma} f(a - b)g(a + b)$.

(e) Show addition and multiplication are well defined and make A an integral domain.

(f) Let K be the fraction field of A and define $v\colon K^\times \to \Gamma$ by

$$v(f/g) = \min \operatorname{supp}(f) - \min \operatorname{supp}(g).$$

Show that v is well defined and is a valuation on K with value group Γ. Thus every ordered abelian group arises as the value group of a field.

Remark. The field K is known as the field of *Hahn series* [1] (or *Hahn-Mal'cev-Neumann* series) with residue field k and value group Γ, and is typically denoted $k[[z^\Gamma]]$, since its elements can be viewed as formal power series $f = \sum f_a z^a$ with coefficients in k and exponents in Γ, corresponding to functions $a \mapsto f_a$ with well-ordered support. One can show that A is the valuation ring of K by showing that $A^\times = \{x \in K : v(x) = 0\}$. The key to proving this is showing that $(1 - z)^{-1} = 1 + z + z^2 + \cdots$ is a well-defined element of A; there are several approaches that work [2, 3, 4], but none of them are particularly simple. Your proof that v is a valuation on K with value group Γ should not depend on the fact that A is the valuation ring.

(g) Let $v\colon K^\times \to \Gamma_v$ and $w\colon K^\times \to \Gamma_w$ 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 $\rho\colon \Gamma_v \to \Gamma_w$ 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.

(h) 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 $R_1 \le R_2$ 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.

(i) 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.

(j) 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 (32 points)

Let A be the valuation ring of a nonarchimedean local field K, let L be a tamely ramified finite abelian 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, $\mathrm{N}_{L/K}(B^\times) = A^\times$. Let $\mathfrak{p}$ and $\mathfrak{q}$ be the maximal ideals of A and B and $k := A/\mathfrak{p}$ and $l := B/\mathfrak{q}$ the residue fields.

(a) Prove that we always have $\mathrm{N}_{L/K}(B^\times) \subseteq A^\times$ and $\mathrm{N}_{l/k}(l^\times) = k^\times$ and $\mathrm{T}_{l/k}(l) = k$.

(b) For $i \ge 0$ 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 totally ramified then the norm of every $b \in B^\times$ lies in a coset of U_1 of the form $u^n U_1$, where $n = [L : K]$. Show that for $n > 1$ the norms of these cosets do not cover $A^\times$. Conclude that if $\mathrm{N}_{L/K}(B^\times) = A^\times$ then L/K must be unramified.

(d) Assume L/K is unramified. Show that for every $u \in A^\times$ there exists $\alpha_0 \in B^\times$ with $\mathrm{N}_{L/K}(\alpha_0) \equiv u \bmod \mathfrak{p}$. Then construct $\alpha_1 \in B^\times$ with $\mathrm{N}_{L/K}(\alpha_0\alpha_1) \equiv u \bmod \mathfrak{p}^2$. Continuing in this fashion, construct $\alpha \in B^\times$ such that $\mathrm{N}_{L/K}(\alpha) = u$.

Problem 4. Minkowski's lemma and sums of four squares (32 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 $\mu(S) \ge 2^n$ (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 (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
10/25	Haar measure, product formula				
10/27	The geometry of numbers				

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] Hans Hahn, *Über die nichtarchimedischen Grössensysteme*, Sitzungsberichte der K. Akademie der Wissenschaften, Vienna **116** (1907), 601–655.

[2] Crispin St. J. A. Nash-Williams, *On well-quasi-ordering finite trees*, Proc. Cambridge Philos. Soc. **59** (1963), 833–835.

[3] Bernhard H. Neumann, *On ordered division rings*, Trans. Amer. Math. Soc. **66** (1949), 202–252.

[4] Donald S. Passman, *The algebraic structure of group rings*, Wiley, 1977.

18.785 Number Theory I
Fall 2021