18.785 Number Theory **Fall 2018**

Problem Set #3 **Due: 10/1/2018**

Description

These problems are related to the material in Lectures 5–7. Your solutions should be written up in late and submitted as a pdf-file named `SurnamePset3.pdf` (replace `Surname` with your surname) via e-mail to `drew@math.mit.edu` by **noon** on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators, and any references consulted other than the lecture notes. If there are none, write **Sources consulted: none** at the top of your problem set. The first person to spot each typo/error in the problem set or lecture notes will receive 1–5 points of extra credit.

Instructions: First do the warm up problems, then pick any combination of problems 1–6 that sums to 96 points and write up your answers in latex. Finally, be sure to complete the survey problem 7.

Problem 0. Warmup (0 points)

These warmup exercises do not need to be written up or turned in.

(a) Show that odd primes p split over $\mathbb{Q}(\sqrt{d})$ if and only if $x^2 - d$ splits in $\mathbb{F}_p[x]$, but that this holds for $p = 2$ only when $d \not\equiv 1 \bmod 4$. Then show that for $d \equiv 1 \bmod 4$ using $x^2 - x + (1-d)/4$ instead of $x^2 - d$ works for every prime p.

(b) Let $\mathcal{O}_K$ be the ring of integers of an imaginary quadratic field K and let c be a positive integer. Prove that $\mathcal{O} := \mathbb{Z} + c\mathcal{O}_K$ is an order with conductor $c\mathcal{O}_K$ and that $c = [\mathcal{O}_K : \mathcal{O}]$ (the index of $\mathcal{O}$ in $\mathcal{O}_K$ as additive abelian groups).

(c) Let L/K be a finite Galois extension of number fields. Prove that if K has any inert primes then $\mathrm{Gal}(L/K)$ is cyclic (as we shall prove later, the converse holds).

(d) Let L/K be a finite extension of number fields. Show that a prime of K splits completely in L if and only if it splits completely in the normal closure of L/K.

Problem 1. Factoring primes in cubic fields (32 points)

Let $K = \mathbb{Q}(\sqrt[3]{5})$.

(a) Prove that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$.

(b) Factor the primes $p = 2, 3, 5, 7, 11, 13$ in $\mathbb{Q}(\sqrt[3]{5})$. Write the prime ideals $\mathfrak{q}$ appearing in your factorizations in the form $(p, f(\sqrt[3]{5}))$ where $f \in \mathbb{Z}[x]$ has degree at most 2.

(c) Prove that the factorization patterns you found in (b) represent every possible case; that is, every possible sum $[K : \mathbb{Q}] = \sum_{\mathfrak{q}|(p)} e_\mathfrak{q} f_\mathfrak{q}$ that can arise for this particular field K. You should find that there is one numerically possible case that does not occur for $p \leq 13$; you need to prove that it cannot occur for any prime p.

(d) Find a different cubic field of the form $K = \mathbb{Q}(\sqrt[3]{n})$ for which the one factorization pattern missing from (c) does occur (demonstrate this explicitly).

Problem 2. Factoring primes in cyclotomic fields (32 points)

Let ℓ be a prime and let ζ_ℓ denote a primitive ℓth root of unity.

(a) Prove that $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ is a Galois extension.

(b) Prove that $\mathbb{Z}[\zeta_\ell]$ is the ring of integers of $\mathbb{Q}(\zeta_\ell)$.

(c) For each prime $p \neq \ell$, determine the number g_p of primes $\mathfrak{q}$ of $\mathbb{Q}(\zeta_\ell)$ lying above (p), the ramification index e_p and the residue field degree f_p (as a function of p and ℓ).

(d) Do the same for $p = \ell$.

Problem 3. Non-monogenic fields (32 points)

Recall that a number field K is said to be monogenic if its ring of integers $\mathcal{O}_K$ is of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Every number field of degree 2 is monogenic; indeed, for $K = \mathbb{Q}(\sqrt{-d})$ we can take $\alpha = (d \pm \sqrt{-d})/2$. In this problem you will prove that infinitely many number fields of degrees 3 and 4 are not monogenic.

(a) Let K be a number field of degree $n > 2$ in which the prime 2 splits completely (so $2\mathcal{O}_K$ is the product of n distinct prime ideals). Prove that K is not monogenic.

(b) Prove that if 2 splits completely in number fields K_1 and K_2 then it also splits completely in their compositum (the smallest number field containing K_1 and K_2).

(c) Show that if $p \equiv \pm 1 \bmod 8$ is prime, then 2 splits completely in $\mathbb{Q}(\sqrt{\pm p})$ (with the same sign in both $\pm$). Conclude that for each $k \geq 2$, infinitely many number fields of degree 2^k are not monogenic and give a quartic example.[1]

(d) Consider $K = \mathbb{Q}(\sqrt[3]{ab^2})$, with $a, b \in \mathbb{Z}$ coprime, squarefree, and $a^2 \not\equiv b^2 \bmod 9$. Dedekind showed that $(1, \sqrt[3]{ab^2}, \sqrt[3]{a^2b})$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$. Show that for every $\alpha \in \mathcal{O}_K - \mathbb{Z}$, the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ has the form $ar^3 - bs^3$, with $r, s \in \mathbb{Z}$. Show that infinitely many cubic number fields are not monogenic and give an example.

Problem 4. Orders in Dedekind domains (32 points)

Let $\mathcal{O}$ be an order (noetherian domain of dimension one with nonzero conductor) with integral closure B (a Dedekind domain) and conductor $\mathfrak{c}$ (largest B-ideal in $\mathcal{O}$).

(a) Prove that for a prime $\mathfrak{p}$ of $\mathcal{O}$ the following are equivalent:

(1) $\mathfrak{p}$ does not contain $\mathfrak{c}$;

(2) $\mathcal{O} = \{x \in B : x\mathfrak{p} \subseteq \mathfrak{p}\}$;

(3) $\mathfrak{p}$ is invertible (as a fractional $\mathcal{O}$-ideal);

(4) $\mathcal{O}_\mathfrak{p}$ is a DVR;

(5) $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a principal $\mathcal{O}_\mathfrak{p}$-ideal.

Then show that these equivalent conditions all imply that $\mathfrak{p}B$ is a prime B-ideal.

[1] You may assume Dirichlet's theorem on primes in arithmetic progressions, which we will prove later in the course: for any coprime $a, m \in \mathbb{Z}$ there are infinitely many primes $p \equiv a \bmod m$.

(b) Prove that nonzero fractional ideals I of $\mathcal{O}$ prime to $\mathfrak{c}$ are invertible, but the converse need not hold (give an explicit counterexample).

(c) Let $K \neq \mathbb{Q}$ be a number field with ring of integers $\mathcal{O}_K$, let $c \in \mathbb{Z}_{>1}$, and let

$$\mathcal{O} := \mathbb{Z} + c\mathcal{O}_K = \{a + b : a \in \mathbb{Z}, b \in c\mathcal{O}_K\}.$$

Prove that $\mathcal{O}$ is an order with integral closure $\mathcal{O}_K$ and conductor $c\mathcal{O}_K$, and that $c\mathcal{O}_K$ is not principal as an $\mathcal{O}$-ideal.

(d) Let $K := \mathbb{Q}(i)$ with $\mathcal{O}_K = \mathbb{Z}[i]$, let p be any prime, and let $\mathcal{O} := \mathbb{Z} + pi\mathbb{Z}$. Show that the conductor of $\mathcal{O}$ is $\mathfrak{p} := p\mathbb{Z} + pi\mathbb{Z}$, that $\mathfrak{p}$ is a prime $\mathcal{O}$-ideal, and that $\mathfrak{a} := p^2\mathbb{Z} + pi\mathbb{Z}$ is an $\mathcal{O}$-ideal contained in $\mathfrak{p}$ but not divisible by $\mathfrak{p}$.

Problem 5. A relative extension without an integral basis (32 points)

Let K be the quadratic field $\mathbb{Q}(\sqrt{-6})$ with ring of integers $A = \mathbb{Z}[\sqrt{-6}]$, let $L := K(\sqrt{-3})$ be a quadratic extension, and let B be the integral closure of A in L (so $AKLB$ holds).

(a) Let $\zeta_3 := \frac{-1+\sqrt{-3}}{2}$. Show that $\{1, \sqrt{2}, \zeta_3\}$ generates B as an A-module. Conclude that B is a torsion free A-module, and that if it is a free A-module, it has rank 2.

(b) Show that if $B \simeq A^2$, then $\{1, \zeta_3\}$ is an A-module basis for B (hint: show that if $\{\beta_1, \beta_2\}$ is any A-module basis for B, then the matrix that expresses $\{1, \zeta_3\}$ in terms of this basis is invertible; to do so you may also want to write $\{1, \sigma(\zeta_3)\}$ in terms of $\{\sigma(\beta_1), \sigma(\beta_2)\}$ with $\sigma \in \mathrm{Gal}(L/K)$).

(d) Show that $\{1, \zeta_3\}$ is *not* an A-module basis for B by showing that you cannot write $\sqrt{2}$ in terms of this basis. Conclude that B is not a free A-module and that the ideal class group $\mathrm{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$ is non-trivial.

(d) Show that the A-module B is isomorphic to the A-module $I_1 \oplus I_2$, where $I_1, I_2 \in \mathcal{I}_A$ are the fractional A-ideals $I_1 := (\zeta_3)$ and $I_2 := \frac{1}{\sqrt{-3}}(3, \sqrt{-6})$.

Problem 6. Modules over Dedekind domains (64 points)

Let us recall some terminology from commutative algebra. Let A be a ring and let M be an A-module. A *splitting* of a surjective A-module homomorphism $\psi \colon N \to M$ is an A-module homomorphism $\phi \colon M \to N$ such that $\psi \circ \phi$ is the identity map; we then have

$$N = \phi(M) \oplus \ker(\psi) \simeq M \oplus \ker(\psi).$$

We say that M is *projective* if every surjective A-module homomorphism $\psi \colon N \to M$ admits a splitting $\phi \colon M \to N$. A *torsion* element $m \in M$ satisfies $am = 0$ for some nonzero $a \in A$. If M consists entirely of torsion elements then it is a *torsion module.* If M has no nonzero torsion elements then it is *torsion free.* Note that the zero module is a torsion-free torsion module.

Now let A be a Dedekind domain with fraction field K.

(a) Prove that every finitely generated torsion A-module M is isomorphic to

$$A/I_1 \oplus \cdots \oplus A/I_n,$$

for some nonzero A-ideals $I_1, \ldots, I_n$ (you may use the structure theorem for modules over PIDs).

(b) Prove that every fractional ideal of A is a projective A-module.

(c) Prove that every finitely generated torsion-free A-module M is isomorphic to a finite direct sum of nonzero fractional ideals of A (elements of $\mathcal{I}_A$).

(d) Prove that every finitely generated A-module is isomorphic to the direct sum of a finitely generated torsion module and a finitely generated torsion-free module.

(e) Show that if M is a finitely generated A-module then $M \otimes_A K \simeq K^r$ for some $r \in \mathbb{Z}_{\geq 0}$, and that for $M \in \mathcal{I}_A$ we must have $r = 1$.

(f) Let M be a finitely generated torsion-free A-module, and let us fix an isomorphism $\iota\colon M \otimes_A K \xrightarrow{\sim} K^n$ that embeds M in K^n via $m \mapsto \iota(m \otimes 1)$. Let N be the A-submodule of K generated by the determinants of all $n \times n$ matrices whose columns lie in M. Prove that $N \in \mathcal{I}_A$ and that its ideal class (its image in the ideal class group $\mathrm{cl}(A) := \mathcal{I}_A/\mathcal{P}_A$) is independent of ι; this is the *Steinitz class* of M.

(g) Prove that for any $I_1, \ldots, I_n \in \mathcal{I}_A$ the Steinitz class of $I_1 \oplus \cdots \oplus I_n$ is the ideal class of the product $I_1 \cdots I_n$.

(h) Prove that two finite direct sums $I_1 \oplus \cdots \oplus I_m$ and $J_1 \oplus \cdots \oplus J_n$ of elements of $\mathcal{I}_A$ are isomorphic as A-modules if and only if $m = n$ and the ideal classes of $I_1 \cdots I_m$ and $J_1 \cdots J_n$ are equal.

(i) Prove that infinite direct sums $\bigoplus_{i=1}^{\infty} I_i$ and $\bigoplus_{j=1}^{\infty} J_j$ of elements of $\mathcal{I}_A$ are always isomorphic as A-modules.

Problem 7. 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			
Problem 5			
Problem 6			

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
9/25	Ideal norms, Dedekind-Kummer				
9/27	Primes in Galois extensions				

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.