HW #4

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, February 13 by 11:59pm on Gradescope.

Question 1. Let A be a Dedekind domain, and let $I, J \subset A$ be two nonzero ideals with the prime ideal factorization

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}, \quad J = \prod_{i=1}^{n} \mathfrak{p}_i^{f_i},$$

with $e_i, f_i \geq 0$ and $\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_n$ mutually distinct maximal ideals of A. Show that

$$\gcd(I, J) := I + J = \prod_{i=1}^{n} \mathfrak{p}_i^{\min(e_i, f_i)}, \quad \operatorname{lcm}(I, J) := I \cap J = \prod_{i=1}^{n} \mathfrak{p}_i^{\max(e_i, f_i)}.$$

Question 2. Let A be a Dedekind domain.

(1) Prove the **weak approxmiation theorem**:

> **Theorem.** Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be mutually distinct maximal ideals of A, and let $e_1, \cdots, e_n \in \mathbb{Z}$. Then, there exists a nonzero $b \in \operatorname{Frac}(A)$ such that the prime ideal factorization of the principal ideal (b) has $\mathfrak{p}_i$ appearing with multiplicity exactly e_i.
>
> **Hint.** It is sufficient to prove the theorem for $e_1, \cdots, e_n \geq 0$ with the extra requirement that $b \in A$. Show first that $\mathfrak{p}_i^{e_i}/\mathfrak{p}_i^{e_i+1} \subset A/\mathfrak{p}_i^{e_i+1}$ is nonzero. After that, one can use (a variant of) the Chinese Remainder Theorem, that $A \to \prod_{i=1}^{n} A/\mathfrak{p}_i^{e_i+1}$ is surjective.

(2) Prove the **strong approximation theorem**:

> **Theorem.** Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be mutually distinct maximal ideals of A, and let $e_1, \cdots, e_n \in \mathbb{Z}$. Then, there exists a nonzero $b \in \operatorname{Frac}(A)$ such that the prime ideal factorization of the principal ideal (b) has $\mathfrak{p}_i$ appearing with multiplicity exactly e_i, **and also such that all the other prime ideal factors of (b) have nonnegative multiplicities**.
>
> **Hint.** Use the version of the weak approximation for $e_1, \cdots, e_n \geq 0$ and $b \in A$ to first find a denominator, and then to find an appropriate numerator.

Question 3. Let $K = \mathbb{Q}(\sqrt{5})$ and $A = \mathbb{Z}[\sqrt{5}] \neq \mathcal{O}_K$. We already know that A is not normal, so not Dedekind. This exercise shows that the unique factorization of ideals fails to hold in A.

(1) Show that the ideal $\mathfrak{p} = (2, 1 + \sqrt{5}) \subset A$ is a maximal ideal, by showing that $A/\mathfrak{p} \cong \mathbb{F}_2$.
(2) Show that $(2) \subsetneq \mathfrak{p}$ are different ideals.
(3) Show that $\mathfrak{p}^2 = 2\mathfrak{p}$. Deduce that the unique factorization of ideals does not hold in A.

Question 4. Let $K = \mathbb{Q}(\sqrt{-26})$, and consider the two factorizations of 27 in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-26}]$:

$$27 = 3 \cdot 3 \cdot 3 = (1 + \sqrt{-26})(1 - \sqrt{-26}).$$

(1) Show that these two factorizations of 27 are factorizations into irreducibles, i.e. that 3, $1 + \sqrt{-26}$, $1 - \sqrt{-26}$ are all irreducible elements in $\mathbb{Z}[\sqrt{-26}]$. Thus, $\mathbb{Z}[\sqrt{-26}]$ is not a UFD.
Hint. Show that no element in $\mathbb{Z}[\sqrt{-26}]$ has norm 3.

(2) Find a prime ideal factorization of the ideal (27), and explain the two different prime factorizations of 27 in terms of the prime ideal factorization of the ideals (3), $(1 + \sqrt{-26})$ and $(1 - \sqrt{-26})$.

Question 5. In this exercise, we will describe the prime ideal factorization of $(p) \subset \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$, in the case of $d \equiv 1 \pmod 4$ squarefree.

(1) Show that the minimal polynomial of $\frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ over $\mathbb{Q}$ is

$$f(X) = X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X].$$

Deduce that $\mathcal{O}_K / p\mathcal{O}_K = \mathbb{F}_p[X]/(f(X))$.

(2) If $p = 2$, then show that $f(X)$ is irreducible in $\mathbb{F}_p[X]$ if and only if $\frac{1-d}{4} \equiv 1 \pmod 2$.

(3) If p is an odd prime, show that $f(X)$ is irreducible in $\mathbb{F}_p[X]$ if and only if d is not a square mod p.
Hint. $f(X) = \left(X - \frac{1}{2}\right)^2 - \frac{d}{4}$.

(4) Give a complete description of the prime ideal factorization of $(p) \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ in the case of $d \equiv 1 \pmod 4$ squarefree.