HW #8

ALGEBRAIC NUMBER THEORY, GU4043; INSTRUCTOR: GYUJIN OH

Due Tuesday, March 19 by 11:59pm on Gradescope.

Question 1. For a rational prime $p \in \mathbb{Z}$, let $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ be the map defined as follows.

– For $n \in \mathbb{Z}$, $v_p(n) \geq 0$ is such that $p^{v_p(n)} \mid n$ but $p^{v_p(n)+1} \nmid n$.

– For $\dfrac{n}{m} \in \mathbb{Q}$, $n, m \in \mathbb{Z}$, define $v_p\left(\dfrac{n}{m}\right) = v_p(n) - v_p(m)$.

(1) Show that v_p is a normalized discrete valuation on $\mathbb{Q}$.
(2) Show conversely that any normalized discrete valuation v on $\mathbb{Q}$ is equal to v_p for some rational prime p.

Hint. Show that $v(1) = 0$, and $v(n) \geq 0$ for all $n \in \mathbb{Z}$. Then, show that $I = \{n \in \mathbb{Z} \mid v(n) > 0\}$ is a prime ideal of $\mathbb{Z}$.

Question 2. Let A be an integral domain, and let $S \subset A - \{0\}$ be a multiplicative set. Let B be a commutative ring, and let $f : A \to B$ be a ring homomorphism, such that $f(s)$ is a unit in B for every $s \in S$. Show that there exists a **unique** ring homomorphism $g : S^{-1}A \to B$ where the composition of g with the natural map $A \to S^{-1}A$, $a \mapsto \frac{a}{1}$, recovers $f : A \to B$.[1]

Question 3. Let $\mathbb{Z}_p$ (the p-**adic integers**) be the set defined as follows.

$$\mathbb{Z}_p := \{(a_1, a_2, \cdots) \mid a_n \in \mathbb{Z}/p^n\mathbb{Z},\ a_{n+1} \pmod{p^n} = a_n\}.$$

Namely, $\mathbb{Z}_p$ is the collection of compatible sequences of mod p^n congruence classes.

(1) Endow $\mathbb{Z}_p$ with a commutative ring structure, where the addition and the multiplication are defined entrywise (e.g. $(a_1, a_2, \cdots) + (b_1, b_2, \cdots) = (a_1 + b_1, a_2 + b_2, \cdots)$). Show that $\mathbb{Z}_p$ is a discrete valuation ring.
(2) Consider the natural ring homomorphism $\mathbb{Z} \to \mathbb{Z}_p$, $n \mapsto [n] := (n, n, \cdots)$. Show that, for any $n \in \mathbb{Z}$ coprime to p, $[n]$ is a unit in $\mathbb{Z}_p$. Deduce that this gives rise to a natural injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$.
(3) Show that the natural injection $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ is not surjective. Deduce that $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p)$ is strictly bigger than $\mathbb{Q}$.

Hint. Show that $\mathbb{Z}_p$ is uncountable.

[1] In general, this kind of a statement is called the **universal property**.

Question 4. Let $p \neq q$ be two different rational primes such that $p, q \equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, and $L = \mathbb{Q}(\sqrt{pq})$, so that $L \subset K$. Show that **every prime ideal of** $\mathcal{O}_L$ is unramified in K.[2]

Hint. One can see K as an extension of L in two different ways, $K = L(\sqrt{p}) = L(\sqrt{q})$.

Question 5.

(1) Let $f(X) \in \mathbb{Z}[X]$ be any nonconstant polynomial. Show that $f(X)$ has a root mod p for infinitely many rational primes p.

  Hint. If all prime factors of $f(n)$ are less than N, then show that, for large enough M, $\frac{f(M!f(0))}{f(0)}$ must have a prime factor bigger than N.

(2) Let K be a number field. Show that there are infinitely many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ such that the residue degree of $\mathfrak{p}$ is 1.

(3) Let K/L be an extension of number fields. Show that there are infinitely many prime ideals of L that split completely in K.

  Hint. Apply (2) to the Galois closure of K over $\mathbb{Q}$.

[2]In this situation, we call that K/L is an **unramified extension**.