18.786 Problem Set 6 (due Thursday Mar 18 in class)

1. Let A be a ring, S a multiplicatively closed subet of A, and $\mathfrak{p}$ an ideal of A such that $S \cap \mathfrak{p} = \phi$. Show that localization commutes with quotients: letting $A' = S^{-1}A$, $\mathfrak{p}' = \mathfrak{p}A'$ and $\bar{S} = S \bmod \mathfrak{p}$, show that

$$A'/\mathfrak{p}' \cong \bar{S}^{-1}(A/\mathfrak{p})$$

2. Let α be a root of $f(x) = x^4 + x^3 + x^2 + 1$. Figure out the decomposition of the primes $2, 19$ and 61 in the ring of integers of $\mathbb{Q}(\alpha)$. Which primes ramify?

3. Let K be a finite extension of $\mathbb{Q}_p$ and L be totally ramified over K of degree n. Let π_L be a uniformizer of L. Show that π_L satisfies an Eisenstein equation

$$X^n + a_{n-1}X^{n-1} + \ldots a_0 = 0$$

with $a_i \in \mathfrak{p}_K$ for all i, and $a_0 \notin \mathfrak{p}_K^2$. Conversely, any root of such an equation generates a totally ramified extension of degree n.

4. Show that any extension of non-archimedean local fields $K \subset L$ can be written as a tower $K \subset M \subset L$ of an unramified extension $K \subset M$ and a totally ramified extension $M \subset L$.

5. Show that any finite extension of p-adic fields is monogenic. [Hint: show this first separately for unramified and totally ramified extensions]

6. Let K be a non-archimedean local field, i.e. a finite extension of $\mathbb{Q}_p$. Let $\mathfrak{o}$ be its valuation ring, and $\mathfrak{p} = (\pi)$ the maximal ideal, with π being the uniformizer. Let $U_0 = U = \mathfrak{o}^*$ be the multiplicative group of units of $\mathfrak{o}$, and define, for $i \geq 1$, $U_i = 1 + \mathfrak{p}^i$. Show that U/U_1 is cyclic, $U \cong U_1 \times (U/U_1)$, and also that $\mathfrak{p}^i/\mathfrak{p}^{\mathfrak{i}+1} \cong U_i/U_{i+1}$ under the map $x \mapsto 1 + x$, is an isomorphism from the additive group on the left to the multiplicative group on the right, for $i \geq 1$. Can you define an isomorphism from $\mathfrak{p}$ to U_1?

7. Show that there are only finitely many extensions of $\mathbb{Q}_p$ of any fixed degree n.

8. Let L, M be finite, linearly disjoint extensions of a number field K, i.e. if $e_1, \ldots, e_m$ is a basis for L over K and $f_1, \ldots, f_n$ is a basis for M over K, then $\{e_i f_j\}$ is a basis for the compositum LM over K. Assume that the discriminants $d_{L/K}, d_{M/K}$ are coprime. Then show that $\mathcal{O}_{LM} = \mathcal{O}_L\mathcal{O}_M$.

9. Compute the ring of integers of $\mathbb{Q}(\zeta_n)$ for an arbitrary positive integer n.

18.786 Topics in Algebraic Number Theory
Spring 2010