18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 7, due Thursday, April 13

Reminder: the detached part of the midterm is also due on April 13; no extensions on that!

1. Leftover from last time: here is Kummer's original motivation for developing the theory of ideals and the like. Let $p > 3$ be a rational prime which does not divide the class number of $\mathbb{Q}(\zeta_p)$; such a prime p is said to be *regular*. (Optional: web search to find out more about regular and irregular primes.) Suppose that we had a counterexample $x^p + y^p + z^p = 0$ to the Fermat conjecture with $p \not| xyz$.

   (a) Prove that for $i = 0, \dots, p-1$, $x + \zeta^i y$ is equal to a p-th power times a unit in $\mathbb{Z}[\zeta_p]$. (Hint: check that the ideals $(x + \zeta^i y)$ are pairwise coprime.)

   (b) Prove that for some integer m,
   $$x\zeta_p^m + y\zeta_p^{m-1} \equiv x\zeta_p^{-m} + y\zeta_p^{1-m} \pmod{p}.$$
   (Hint: use a problem from the previous pset.)

   (a) Prove that in (b), we must have $2m \equiv 1 \pmod{p}$ and deduce that $x \equiv y \pmod{p}$. Since the same argument yields $x \equiv z \pmod{p}$, this yields a contradiction.

2. Prove that the 10-adic completion of $\mathbb{Z}$ is not a domain. Optional (not to be turned in): prove that the N-adic completion of $\mathbb{Z}$ is isomorphic to the product of $\mathbb{Z}_p$ over all p dividing N (in particular, it only depends on the squarefree part of N). Also optional (also not to be turned in): generalize to any Dedekind domain.

3. Prove that an element of $\mathbb{Q}_p$ is rational if and only if its base p expansion is terminating or periodic (to the *left*, that is).

4. Janusz p. 99, exercise 3.

5. Janusz p. 99, exercise 7.

6. Let $P(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$, and suppose $r \in \mathbb{Z}_p$ satisfies $|P(r)| < |P'(r)|^2$. Prove that starting from r, the Newton iteration $z \mapsto z - P(z)/P'(z)$ converges to a root of P; deduce as a corollary that such a root exists. This leads to a proof of Hensel's Lemma, as well as a good algorithm for computing roots of p-adic polynomials.

7. (Optional) A DVR satisfying the conclusion of Hensel's lemma (say, in the formulation given in the previous exercise) is said to be *henselian*; such a DVR satisfies most of the interesting properties of complete DVRs, like the theorems about extending absolute values.

   (a) Let R be the integral closure of $\mathbb{Z}_{(p)}$ in $\mathbb{Z}_p$. Prove that R is a henselian DVR which is not complete.

(b) Let R be the ring of formal power series over $\mathbb{C}$ which converge on some disc around the origin. Prove that R is a henselian DVR which is not complete.

8. Let R be a complete DVR whose fraction field is of characteristic 0 and whose residue field κ is perfect of characteristic $p > 0$ (e.g., $R = \mathbb{Z}_p$). Prove that for each $x \in \kappa$, there exists a unique lift of x into R which has a p^n-th root in R for all positive integers n. (Hint: define a sequence whose n-th term is obtained by choosing some lift of x^{1/p^n} and raising it to the p^n-th power. Show that this sequence converges.) This lift, usually denoted $[x]$, is called the *Teichmüller lift* of x.

9. (a) Prove that the field $\mathbb{Q}_p$ has no nontrivial automorphisms *as a field*, even if you don't ask for continuity. (Hint: use the previous exercise, but beware that you aren't given that the automorphism carries $\mathbb{Z}_p$ into itself.)

   (b) Prove that for p and q distinct primes, the fields $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic. (Hint: which elements of $\mathbb{Q}_q$ have p-th roots?)

10. If you postponed PS 4 problem 8, solve it now as follows. (Parts (a) and (b) are related to the hint from PS 4.) Throughout, let R'/R be a finite extension of DVRs such that the residue field extension is separable.

   (a) Suppose R is complete (as then is R'). Prove that there exists a unique intermediate DVR R'' such that R''/R is unramified and R'/R'' is totally ramified. (Hint: apply the primitive element theorem to the residue field, then lift the resulting polynomial and apply Hensel's lemma to it.)

   (b) In the situation of (a), prove that R' is monogenic over R. (Hint: add a uniformizer to an element generating the unramified subextension.) extension.)

   (c) In the situation of (a), choose x such that $R' = R[x]$. Prove that there exists an integer n such that if $x - y \in \mathfrak{m}_{R'}^n$, then also $R' = R[y]$. (That is, any sufficiently good approximation to a generator is again a generator.)

   (d) Now let R be arbitrary, and let $\widehat{R}$ and $\widehat{R'}$ denote the respective completions. Prove that $[\widehat{R'} : \widehat{R}] = [R' : R]$, or equivalently, that the natural map $\widehat{R} \otimes_R R' \to \widehat{R'}$ is a bijection. (Hint: you can prove the latter by viewing the map as a morphism of $\widehat{R}$-modules and use Nakayama's lemma.)

   (e) Show that R'/R is monogenic. (Hint: use (a)-(c) to produce an element $x \in R'$ with $\widehat{R'} = \widehat{R}[x]$. Then use (d) to show that also $R' = R[x]$.)

11. The ring $\mathbb{Z}_{(5)}[x]/(x^2 + 1)$ is finite integral over the DVR $\mathbb{Z}_{(5)}$ but injects into the completion $\mathbb{Z}_5$. Why doesn't that contradict part (d) of the previous problem?