18.786: Topics in Algebraic Number Theory (spring 2006)
Problem Set 8, due Thursday, April 20

This problem set uses heavily the fact that if K is the fraction field of a discrete valuation ring, then the absolute value on K extends uniquely to any finite extension of K; I should get to this by the end of class on the 13th.

I marked a number of things "Optional" on here; to make up for it, please make sure to do at least one "Optional" part. (That is, the parts are all optional individually but not collectively.)

1. Let U_i be the group of $x \in \mathbb{Z}_p$ with $x \equiv 1 \pmod{p^i}$. Prove that if $p \neq 2$ and $i \geq 1$, or $p = 2$ and $i \geq 2$, then U_i is torsion-free. (Hint: use exp and log.)

2. Determine the radius of convergence of the Taylor series for $\sin x$ over $\mathbb{Q}_p$.

3. Prove that a formal power series $\sum_{n=0}^{\infty} a_n x^n$ and its formal derivative $\sum_{n=1}^{\infty} n a_n x^{n-1}$ have the same radius of convergence over $\mathbb{Q}_p$.

4. (a) Prove that the infinite extension $\mathbb{Q}_p(p, p^{1/p}, p^{1/p^2}, \dots)$ of $\mathbb{Q}_p$ is not complete (under the unique extension of the p-adic absolute value).
   (b) Prove that the maximal unramified extension of $\mathbb{Q}_p$ is not complete either.
   (c) Optional: prove that *any* infinite algebraic extension of $\mathbb{Q}_p$ is not complete.

5. (Optional, possibly tricky) Let $\mathbb{C}_p$ be the completion of an algebraic closure of $\mathbb{Q}_p$ for the unique extension of the p-adic absolute value. Prove that $\mathbb{C}_p$ is again algebraically closed; the field $\mathbb{C}_p$ is loosely analogous to the usual complex numbers in ordinary analysis.

6. In this exercise, you will check some of the basic properties of Newton polygons I outlined in class. Let K be the fraction field of a DVR R. For $P(x) = a_n x^n + \cdots + a_0 \in K[x]$ with $a_n, a_0 \neq 0$, consider the set of points $\{(-i, v(a_i)) : i = 0, \dots, n\}$ in $\mathbb{R}^2$. Their lower convex hull is the *Newton polygon* of P; I'll think of this polygon as consisting of n separate segments of horizontal width 1.
   (a) Let $r_1, \dots, r_n$ be the roots of P in some finite extension K' of K. Assume that v extends uniquely to K' (we'll prove this in class; note that v is normalized with respect to K, not K'). Prove that the slopes of the Newton polygon are precisely $v(r_1), \dots, v(r_n)$. (Hint: sort the r_i so that $v(r_1) \leq \cdots \leq v(r_n)$. Then check $v(a_{n-i}/a_n) \geq v(r_1) + \cdots + v(r_i)$. Then check that equality holds if $v(r_i) < v(r_{i+1})$, or if $i = n$.)
   (b) Prove that the Newton polygon of PQ is obtained by "merging" the Newton polygons of P and Q: that is, the number of segments of the Newton polygon of PQ of any given slope is the sum of the corresponding numbers for P and Q. (Hint: this can be done directly, but use (a) instead.)

(c) As an example, compute the p-adic absolute values of the roots of $x^5 - 2x^2 + 16$ in an algebraic closure of $\mathbb{Q}_2$. (I suspect SAGE can verify this by approximating the roots numerically.)

7. (a) Let K be a finite *unramified* extension of $\mathbb{Q}_p$. Prove that there is a unique automorphism of K over $\mathbb{Q}_p$ lifting the p-power Frobenius map on the residue field. (Optional: state and prove a generalization to an arbitrary finite unramified extension between the fraction fields of two complete DVRs.)

   (b) (Optional) Exhibit examples to show that neither the existence nor the uniqueness in (a) need hold if K is ramified. (Hint: for the non-existence you must use a non-Galois extension.)

8. Let R be a discrete valuation ring with fraction field K, and let $|\cdot|$ be a nonarchimedean absolute value on K with valuation ring R. Prove that for *any* extension L of K, not necessarily finite, there exists an extension of $|\cdot|$ to a nonarchimedean absolute value of L. (Hint: use Zorn's lemma to reduce to considering a single algebraic extension, which we treated in class, and a single purely transcendental extension.)

9. Here is a surprising application of the p-adic absolute value due to Paul Monsky. It is to prove that in Euclidean geometry, you cannot dissect a square into an odd number of triangles of equal area!

   (a) Apply the previous exercise to show that there exists a nonarchimedean absolute value $|\cdot|_2$ on $\mathbb{R}$ for which $|2|_2 < 1$.

   (b) Define the following subsets of $\mathbb{R}^2$:

$$\begin{aligned} A &= \{(x, y) \in \mathbb{R}^2 : |x|_2 < 1, |y|_2 < 1\} \\ B &= \{(x, y) \in \mathbb{R}^2 : |x|_2 \geq 1, |x|_2 \geq |y|_2\} \\ C &= \{(x, y) \in \mathbb{R}^2 : |y|_2 \geq 1, |y|_2 > |x|_2\}. \end{aligned}$$

   Verify that A, B, C form a partition of $\mathbb{R}^2$.

   (c) Prove that no line in $\mathbb{R}^2$ meets all of A, B, C. (Hint: note that A, B, C are all stable under translation by A, then reduce to the case where the line passes through the origin.)

   (d) Let R be the interior of a convex polygon of the plane, dissected into finitely many triangles. Suppose that the number of edges of R which ahave one vertex in A and one in B is odd. Prove that there is a triangle in the dissection with one vertex in each of A, B, C. (Hint: once you incorporate (c), this is a purely combinatorial parity argument.)

   (e) Prove that if T is a triangle with one vertex in each of A, B, C, and T has area K, then $|K|_2 > 1$. (Hint: see (c).)

   (f) Deduce Monsky's theorem by applying (d) to an appropriate unit square and then using (e).