Problem Set 11.

Here is a summary of results which have been discussed in class on Newton polygons and extensions of fields K with a discrete nonarchimedean absolute value $|\ |_K$. They may be useful in analyzing the problems in this assignment.

A1. There is an element π_K of maximal possible absolute value less than 1, and every nonzero element $x \in K$ is of the form $\pi_K^n u$ for some integer $n = ord(x)$ and some u with $|u|_K = 1$. Those elements which are so expressible with $n \geq 0$ form a discrete valuation ring O_K. The residue field is the quotient of O_K by the principal ideal $\pi_K O_K$ of all elements of absolute value strictly less than 1.

A2. If L/K is a finite degree extension of K that has an absolute value discrete nonarchimedean absolute value $|\ |_L$ extending $|\ |_K$ then there exist positive integers e, f such that π_K/π_L^e has absolute value 1 and $N\pi_L/\pi_K^f$ has absolute value 1. Further f is the degree of the residue field extension $O_L/(\pi_L)$ over the field $O_K/(\pi_K)$ and the product ef equals the degree of L/K. It is convenient to normalize the order of an element in L by the definition $|\pi_K|_K^{ord(w)} = |w|_L$, so that $ord(w)$ is not an integer, but $ord(w)e \in \mathbf{Z}$, so that we can recognize elements with non integer order as not being in K.

A3. A discrete nonarchimedean absolute value on a field K can be extended to a discrete nonarchimedean absolute value on a separable finite extension L/K.

A4. When K is complete with respect to $|\ |_K$ then the formula $|x|_L = |N_{L/L}(x)|_K^{1/[L:K]}$ gives an extension of $|\ |_K$ to a discrete nonarchimedean absolute value of L and L is complete with respect to this absolute value.

A5. The Newton polygon of a monic separable polynomial $f(x) \in K[x]$ with roots α_i in a splitting field L can be described in terms of the absolute values of the roots of the polynomial . When the roots are ordered by increasing order the Newton polygon is the union of line segments joining $(k, ord(\alpha_1) + \cdots ord(\alpha_{n-k}))$ in order as k ranges from 0 to the degree of $f(x)$. The slopes of the line segments are the negatives of the order of the various roots.

A6. For a complete field K the extended absolute value to the splitting field L of $f(x)$ over K described in A4 above takes the same value on all Galois conjugates of a root of $f(x)$.

A7. The slope factorization of $f(x) \in K[x]$: By A6, the Galois group of the splitting field of $f(x)$ over K acts on roots preserving absolute values. Then the product

$f_{\mu_i}(x) = \prod_{ord(\alpha_i)=\mu_i}$ is a polynomial in $K[x]$ and there is a constant $a \in K$ such that $f(x) = a \prod f_{\mu_i}(x)$. Let the distinct slopes of the segments of the boundary of the Newton polygon be $-\mu_i$, and the length of projection of the segment to the x-axis be λ_i. Then $f_{\mu_i}(x)$ has degree λ_i.

A8. If $f_{\mu_i}(x)$ factors in $K[x]$ as a product of polynomials of degree l, k then the segment of slope $-\mu_i$ on the boundary of the Newton polygon has an integral point with first coordinate l. Hence if the segment of slope μ_i has integral points only at the endpoints then f_{μ_i} is irreducible over K.

A9. If the slope of the segment corresponding to f_{μ_i} of degree λ_i is of the form a/λ_i with a, λ_i relatively prime, then a root of $f_i(x)$ generates a totally ramified extension of K of degree λ_i so that $f_i(x)$ is irreducible in $K[x]$.

Problem Set 11

1. Consider the discrete nonarchimedean absolute value on the rational field $\mathbf{Q}$ given by $|x|_5 = 5^{-ord_5(x)}$ where $ord_5(x)$ is the power of 5 in the expression of x as a ratio of two integers. Show that there at least 2 distinct extensions of this absolute value to the Gaussian field $\mathbf{Q}(i)$ (corresponding to the two prime ideals in $\mathbf{Z}[i]$ which contain 5). Show that the function $F(a+bi) = |N_{\mathbf{Q}(i)/Q}(a+bi)|_K = |a^2+b^2|_5$ satisfies all properties of an absolute value on $\mathbf{Q}(i)$ except the triangle inequality, and exhibit $x, y \in \mathbf{Q}(i)$ such that $F(x+y) > F(x) + F(y)$.
2. Use the version of Newton's method appearing in Hensel's Lemma to find the first 5 terms of a Cauchy sequence converging to a square root of 2 in the 7-adic field Q_7 which is congruent to 4 modulo 7.
3. (Newton-Puiseux Theorem) Let K be an algebraically closed field of characteristic 0. Let $K[[t]]$ be the ring of formal power series.
   a) Show that the set of power series with nonzero constant term are units in this ring and the fraction field of this ring is the field of formal Laurent series $K((t)) = \{\sum_k^\infty a_i t^i | k \in \mathbf{Z}, a_i \in K\}$.
   b) Show that the function $|\sum_{i=k}^\infty a_i t^i| = (1/2)^k$ when $a_k \neq 0$ is a nonarchimedean discrete absolute value on $K((t))$, and the field is complete with respect to this absolute value.
   c) Suppose that $L/K((t))$ is a finite degree extension of degree n (which is automatically separable since K was assumed to be a characteristic 0 field). There is an extension of the absolute value of part b) to an absolute value $||_L$ on L, and then L contains an element π_L and there are integers e, f such that $t = \pi_L^e u$ and $N_{L/K} * \pi_L = \pi^f v$ with $|u|_L = |v|_L = 1$. Show that $f = 1$, and then that $e = n$, so that L/K is totally ramified.
   d) From b) there exists an element u in L, $t = u\pi_L^n$. Show using Hensel's lemma that u is the n-th power of an element in L (or use the binomial theorem)) so that $L = K((t))(z)$ for some z satisfying $z^n = t$, so that L is isomorphic to $K((t^{1/n}))$.
   e) Show using the parts above that when K is algebraically closed of characteristic 0 then $\cup_l K((t^{1/l}))$ is an algebraically closed field (Theorem of Newton-Puiseux).

4. Let K be the number field $\mathbf{Q}(\alpha)$ where α is a root of $f(x) = x^4 - 2x^3 - 2 * 3 * x^2 + 2 * 3^3 * x + 2 * 3^6$. Show using Newton polygons that the degree of $K/\mathbf{Q}$ is 4 and that the prime 3 is contained in 4 distinct primes in $\mathcal{O}_K$. Show that if $\beta \in O_K$ then 3 divides the index $[O_K : \mathbf{Z}[\beta]]$. Explain how to make examples for any square free integer m to show that there exist number fields $K/\mathbf{Q}$ for which m divides the index of any order of form $\mathbf{Z}[\beta]$ inside $\mathcal{O}_K$.

5. Consider the n-th truncated exponential polynomial $f_n(x) = 1+x+x^2/2!+\cdots+x^n/n!$. The goal of this problem is to show that any polynomial with the same Newton polygon as $f_n(x)$ is irreducible.

   a) Show that the exact power of a prime p dividing $n!$ is the sum $ord_p(n!) = \sum_{n=1} \lfloor n/p^n \rfloor$. Show that when n is expressed in base $p = \sum b_i p^i$ with $0 \leq b_i \leq p-1$ then $(p-1)ord_p(n!) = n - \sum b_i$.

   b) Show that the Newton polygon for $f_n(x) \in \mathbf{Q}_p[x]$ has vertices at points of discontinuity of $g(x) = n - \sum_{0 \leq j \leq x} p^j$ and the set of slopes is the set of $\frac{-(p^j-1)}{(p^{b_j}(p-1))}$ as j runs over all indices such that $b_j \neq 0$.

   c) Suppose that p is a prime integer, and $ord_p(n) = m$. Show that the slopes in the Newton diagram for $f_n(x)$ over Q_p in lowest terms have p^m dividing the denominator and that every irreducible factor of $f_n(x) \in \mathbf{Q}_p[x]$ defines an extension of K with ramification degree divisible by p^m.

   d) Show that $f_n(x)$ is irreducible over $\mathbf{Q}$ by considering the degree of an irreducible factor.

   e) Remark: Schur proved that the Galois group of $f_n(x)$ is the symmetric group on n letters or the alternating group according to 4 not dividing n or dividing n.