Throughout this class, we set the following notation. Let $K$ be a field with a discrete valuation $v$ and let $\hat{K}$ be the completion of $K$ with respect to $|\cdot|_v$ where

$$|x|_v = e^{-v(x)}.$$  

By convention $v(0) = \infty$. We define $B_v$ to be the set of $x \in \hat{K}$ with $v(x) \geq 0$ and let $M_v$ be the maximal ideal in $B_v$.

**Proposition 41.1.** With notation as above, let us denote as $B$ the set of all $x \in K$ such that $v(x) \geq 0$ and let us denote as $M$ the maximal ideal of $B$. For any $n \geq 1$, the inclusion $K \hookrightarrow \hat{K}$ induces an isomorphism

$$B/M \cong B_v/M_v.$$  

**Proof.** Let $(a_i)_{i=1}^\infty$ be a Cauchy sequence of $K$. Since $M_v$ consists of elements $x$ for which $v(x) \geq n$ it is clear that the kernel of the natural map

$$\phi : B/M \longrightarrow B_v/M_v$$  

consists of elements in $B$ for which $v(x) \geq t$. These are precisely the elements in $M^t$, so the map above is injective. Now, we will show that it is surjective. Take any Cauchy sequence $(a_i)_{i=1}^\infty$. Let $\epsilon = e^{-t}$. Then there exists $N_\epsilon \in \mathbb{Z}$ such that for all $m, n \geq N_\epsilon$, we have $|a_m - a_n|_v < \epsilon$. Letting $x = a_{N_\epsilon}$, we see that for all

$$|x - a_n|_v < e^{-t}$$  

so $|x - (a_i)_{i=1}^\infty| < e^{-t}$. Thus $v(x - (a_i)_{i=1}^\infty) \geq t$, so

$$x \equiv (a_i)_{i=1}^\infty \pmod{M_v^t}$$  

and $\phi(x) = (a_i)_{i=1}^\infty$. \hfill \qed

For discrete valuations $v$ on field $K$, we have an explicit way of writing out an element of $\hat{K}$. This is analogous to the decimal expansion for a real number. Here is set-up: let $B_v$ be the set of all $x \in K$ for which $v(x) \geq 0$. Then $B_v$ is a local principal ideal domain with maximal ideal $M_v$ generated by some $\pi \in B_v$. Let $U$ be complete set of residue classes for $B_v$ modulo $M_v$. When $B_v$ is $\mathbb{Z}_p$, we can take these to be $0, 1, \ldots, p - 1$ for example; in general, we just take inverse images of all the elements in $B_v/M_v$. Then any $x \in \hat{K}$ has a unique representation as a Laurent series

$$x = \sum_{i=v(x)}^\infty u_i \pi^i$$  

(1)
where $u_i \in U$, $u_i = 0$ for $u < v(a)$, and $\pi$ generates $M_v$. To see this, we first note that such a sum does indeed give rise to a Cauchy sequence in $K$ since $(\sum_{i=-v(x)}^{j} u_i \pi^i)_j$ is a Cauchy sequence since $| \cdot |$ is nonarchimedean, i.e. it is easy to see that for any $m, n > N$, we have

$$| \sum_{i=v(x)}^{n} u_i \pi^i - \sum_{i=v(x)}^{m} u_i \pi^i | < e^{-N}$$

since all the terms cancel out with up to $\pi^N$. To get an expansion of the form (1) for a nonzero $x \in \hat{K}$ (the 0 series gives us 0 of course), we proceed as follows. Let $L = v(x)$. Then $\pi^{-L}x$ is a unit and there is a unit element $u_L$ of $U$ such that

$$\pi^{-L}x \equiv u_L \pmod{M_v}.$$ 

It follows that

$$v(x - u_L \pi^L) = v(\pi^L(\pi^{-L}x - u_L)) \geq L + 1.$$ 

Applying this process to $x - u_L \pi^L$ gives us the term $u_{L+1}$ and so on recursively.

Most of the next few pages is things you’ve seen before in your $p$-adic analysis class. I include them for completeness.

**Lemma 41.2.** Let $A$ be any ring and let $I$ be an ideal of $A$. Suppose that $f(x), g(x) \in A[X]$ are monic polynomials that generate all of $A[X]$. Let $t \in IR[X]$ have degree less than $\deg f + \deg g$. Then we can write

$$af + bg = t$$

for polynomials $a, b \in IA[x]$ such that $\deg a < \deg g$ and $\deg b < \deg f$.

**Proof.** For any $v \in A[X]$, we have

$$(a + vg)f = (b - vf)g = 1$$

Since $f$ is monic, for any $z \in IA[X]$, there is some $v \in IA[X]$ for which

$$z = vf + r$$

with $\deg r < \deg f$. This is easily proved by induction on the degree of $z$. If $z$ has degree less than $f$, then we’re done. If $\deg z \geq \deg f$, then writing the lead term of $z$ as $\alpha \in I$ we see that $z - X^{\deg z - \deg f}$ has degree less than $\deg z$ and is in $IR[X]$.

Applying this when $z = b$, gives

$$\deg(b - vf) < \deg f.$$
Counting degrees shows that
\[ \deg(a + vg) < \deg g \]
and we are done. \( \square \)

**Theorem 41.3.** Let \( R \) be any ring, let \( I \) be an ideal of \( R \) and let \( h(X) \in R[X] \) be monic. Suppose that there exist monic polynomials \( f_0(X), g_0(X) \in R[X] \) such that
\[ h(X) \equiv f_0(X)g_0(X) \pmod{I} \]
and such that \((I, f_0, g_0) \) generate \( R[X] \). Then there exist monic polynomials \( f(X), g(X) \in R[X] \) such that
\[ h(X) \equiv f(X)g(X) \pmod{I^2}, \]
that \((I^2, f, g) \) generate \( R[X] \) and that \( f \equiv f_0 \pmod{I} \) and \( g \equiv g_0 \pmod{I} \).

**Proof.** Since
\[ h(X) \equiv f_0(X)g_0(X) \pmod{I}, \]
we can write
\[ h(X) = f_0(X)g_0(X) + t \]
for some \( r(X) \in R[x] \) and some \( t \in I \) with \( \deg t < \deg f + \deg f \). Since \( R[X] \) is generated by \( I \) along with \( f_0 \) and \( g_0 \), it is also generated by \( I^2 \) along with \( f_0 \) and \( g_0 \), so applying the theorem above with \( A = R/I^2 \), we can write
\[ af_0 + bg_0 = t + v \]
for \( \deg a < \deg g \), \( \deg b < \deg f \), \( a, b \in IR[X] \), and and \( v \in I^2R[X] \). Letting \( f = f_0 + b \) and \( g = g_0 + a \), we have
\[ fg = (f_0 + b)(g_0 + a) = f_0g_0 + (af_0 + bfo) + ab \equiv f_0g_0 + t + v \pmod{I^2} \equiv h(X) \pmod{I^2}. \]
Since \( f \) and \( g \) are congruent to \( f_0 \) and \( g_0 \) modulo \( I \), we see that \((f, g, I) \) generates \( R[X] \), which means that \((f, g, I^2) \) generates \( R[X] \), as desired. \( \square \)

**Corollary 41.4 (Hensel’s Lemma).** Let \( \hat{K} \) and let \( B_v \) be as usual. Let \( h(X) \in B_v[X] \). Suppose that
\[ h(X) \equiv \frac{f(X)}{g(X)} \pmod{\mathcal{M}_v} \]
for some coprime \( \overline{f(X)} \) and \( \overline{g(X)} \) in \( R/\mathcal{M}_v[X] \). Then there exist \( f, g \in B_v[X] \) such that

\[
h(X) = f(X)g(X)
\]

and

\[
f(X) \equiv \overline{f(X)} \pmod{\mathcal{M}_v}
\]

and

\[
g(X) \equiv \overline{g(X)} \pmod{\mathcal{M}_v}.
\]

**Proof.** Choose \( f(x) \) and \( g(x) \) such that

\[
f(x) \equiv \overline{f(X)} \pmod{M_v}
\]

and

\[
g(x) \equiv \overline{g(X)} \pmod{M_v}.
\]

Applying the theorem above to \( f(x) \) and \( g(x) \) with \( I = M_v \), we obtain \( f_1, g_2 \) such that

\[
h(X) \equiv f_1(X)g_1(X) \pmod{M_v^2}
\]

and \( f_1(X) \) and \( g_1(X) \) generate \( R[X] \) modulo \( M_v^2 \). We can apply the above theorem to \( f_1(X) \) and \( g_1(X) \) with \( I = M_v \) and so on, thus obtaining \( f_n, g_{n-1}, g_n, g_{n-1} \) with

\[
f_n \equiv f_{n-1} \pmod{M_v^{2n-1}}
\]

and

\[
g_n \equiv g_{n-1} \pmod{M_v^{2n-1}}
\]

and

\[
h(X) \equiv f_n(X)g_n(X) \pmod{M_v^{2n}}.
\]

This gives a Cauchy sequence of polynomials (i.e. the coefficients of the polynomials form a Cauchy sequence) \((f_n)_{n=1}^{\infty}\) and \((g_n)_{n=1}^{\infty}\) with limits \( f \) and \( g \), respectively, in \( B_v[X] \). Furthermore, we have

\[
h(X) - f(X)g(X) \equiv h(X) - f_n(X)g_n(X) \pmod{M_v^{2n}} \equiv 0 \pmod{M_v^{2n}}
\]

for any integer \( n \). Thus \( h(X) - f(X)g(X) = 0 \), so \( h(X) = f(X)g(X) \).

\[\Box\]

**Remark 41.5.** If \( h \) is monic, then we can assume that \( f \) and \( g \) are monic after multiplying by a suitable unit. In this case, we must have \( \deg f = \deg \overline{f} \) and \( \deg g = \deg \overline{g} \).

**Corollary 41.6.** Let \( h(X) \) be a monic polynomial in \( B_v[X] \) such that there exists \( \alpha \in B_v \) for which \( h(\alpha) \equiv 0 \pmod{\mathcal{M}_v} \) and \( h'(\alpha) \not\equiv 0 \pmod{\mathcal{M}_v} \). Then there exist a unique \( \beta \in B_v \) such that

\[
h(\beta) = 0
\]

and \( \beta \equiv \alpha \pmod{\mathcal{M}_v} \).
Proof. Let \( \bar{h} \) denote \( h \pmod{\mathcal{M}} \). If \( \bar{h} \) has a root \( \bar{\alpha} \) modulo \( \mathcal{M} \) and \( h'(\alpha) \not\equiv 0 \pmod{\mathcal{M}} \). Then we can write

\[
\bar{h} \equiv (X - \bar{\alpha})g(X)
\]

for some \( \overline{g(X)} \) that is prime to \( (X - \bar{\alpha}) \). By the remark above, this gives rise to a factorization \( h = f(X)g(X) \) where

\[
g \equiv \overline{g(X)} \pmod{\mathcal{M}}
\]

and

\[
f \equiv (X - \bar{\alpha}) \pmod{\mathcal{M}}
\]

and \( f \) and \( g \) are monic with degrees equal to 1 and \( \deg \overline{g(X)} \), respectively. Thus, \( f \) must be equal to \( (X - \beta) \) for some \( \beta \equiv \alpha \pmod{\mathcal{M}} \). To see that \( \beta \) must be unique, we note that if \( \beta \) were not unique, then \( \alpha \) would be a multiple root of \( \bar{h} \) and we would have \( h'(\alpha) \equiv 0 \pmod{\mathcal{M}} \). \( \square \)

Some of the results above are reminiscent of the result we prove about how primes split in extensions. Now, we will prove a result about extensions of complete fields. From now on, we’ll denote complete fields as \( K_v \) rather than as \( \hat{K} \). We will begin by showing that a nonarchimedean valuation can always be extended. First, a word on archimedean absolute values for number fields. We know that \( \mathbb{Q} \) completed at the archimedean absolute value is equal to \( \mathbb{R} \). Suppose that we have a finite extension \( L \) of \( \mathbb{Q} \) and we want to know how we extend the archimedean valuation on \( \mathbb{Q} \) to \( L \). Let \( w \) be a valuation on \( L \) extending the usual absolute value on \( \mathbb{Q} \). Thus \( L_w \) must contain \( \mathbb{R} \). We can write

\[
L \cong \mathbb{Q}[X]/f(X)
\]

for some monic polynomial \( f(X) \) irreducible over \( \mathbb{Q} \). Let \( \alpha \in L \) have the property that \( f \) is the minimal monic for \( \alpha \) over \( \mathbb{Q} \). Since \( L = \mathbb{Q}(\alpha) \), we must have \( L_w = \mathbb{R}(i(\alpha)) \) for some embedding of \( i \) of \( \alpha \) into the algebraic closure of \( \mathbb{R} \) (i.e. \( \mathbb{C} \)). Now, \( i(\alpha) \) must satisfy some polynomial irreducible over \( \mathbb{R} \) that divides \( f(X) \). So to figure out what \( L_w \) might be, we simply look at how \( f(X) \) splits into irreducible factors over \( \mathbb{R} \). This is the same thing as finding a maximal ideal in

\[
\mathbb{R}[X]/f(X) \cong L \oplus \mathbb{Q} \mathbb{R},
\]

so we can see all the completions \( L_w \) in easy manner. By exactly the same reasoning, we can see all the completions of \( L \) with respect to absolute values extending the \( p \)-adic absolute values by taking looking
at the irreducible factors of $f(X)$ over $\mathbb{Q}_p$, other words, finding the maximal ideals of $\mathbb{Q}_p[X]/f(X)$.

Since any factor of $f$ modulo $p$ lifts to a factor of $f$ in $\mathbb{Q}_p$, this set of maximal ideals looks suspiciously like the primes in $\mathcal{O}_L$ lying over $p$.

We will now see that is indeed exactly the case.

**Proposition 41.7.** Let $v$ be a discrete valuation on a field $K$ and let $L$ be a finite separable field extension of $K$. Let $B$ the set of $x$ in $K$ with $v(x) \geq 0$ and let $C$ be the integral closure of $B$ in $L$. Then the absolute values $| \cdot |_w$ on $L$ extending $| \cdot |_v$ are in one-to-one correspondence with the primes $\mathcal{P}$ in $\mathcal{O}_L$ lying over the maximal ideal $\mathcal{M}$ of $B$.

We will prove this next time.