Math 203B (Number Theory), UCSD, winter 2015
Notes on Hensel's lemma

Let K be a field complete with respect to a (not necessarily discrete) nonarchimedean absolute value. Let $\mathfrak{o}_K$ denote the valuation ring of K. Let $\mathfrak{p}_K$ denote the maximal ideal of $\mathfrak{o}_K$. Let k denote the residue field of $\mathfrak{o}_K$.

In class, we proved *Hensel's lemma* in the following form (following Neukirch II.4.6).

Theorem 1. *For any polynomial $f(T) \in \mathfrak{o}_K[T]$ which is primitive (its reduction $\overline{f}(T) \in k[T]$ is nonzero) and any factorization*

$$\overline{f}(T) = \overline{g}(T)\overline{h}(T)$$

in $k[T]$ such that $\overline{g}, \overline{h}$ are coprime, there is a unique lift of this factorization to a factorization

$$f(T) = g(T)h(T)$$

such that $\deg(g) = \deg(\overline{g})$.

This is most commonly applied as follows.

Corollary 2. *Let $f(T) \in \mathfrak{o}_K[T]$ be a polynomial. Then any simple root of $\overline{f}(T)$ in k lifts uniquely to a root of $f(T)$ in $\mathfrak{o}_K$.*

Proof. Apply Theorem 1 with $\overline{g} = T - \overline{x}$ where $\overline{x}$ is a simple root of $\overline{f}$. □

It turns out that one can recover Theorem 1 from Corollary 2 using some trickery involving symmetric polynomials, but we will not need to do this. Instead, we describe a stronger version of Corollary 2.

Theorem 3. *Suppose $f(T) \in \mathfrak{o}_K[T]$ and $t_0 \in \mathfrak{o}_K$ satisfy*

$$|f(t_0)| < |f'(t_0)|^2 .$$

Then there exists a unique root t of f satisfying

$$|t - t_0| < |f'(t_0)| ,$$

and this root actually satisfies

$$|t - t_0| \leq \frac{|f(t_0)|}{|f'(t_0)|}.$$

Note that we recover Corollary 2 by taking $t_0 \in \mathfrak{o}_K$ to be a lift of a simple root of $\overline{f}$; in this case, $|f(t_0)| < 1$ while $|f'(t_0)| = 1$.

To prove Theorem 3, we use the Banach contraction mapping theorem.

Lemma 4. *Let X be a complete metric space with distance function d. Let $g : X \to X$ be a map such that for some $\epsilon \in [0, 1)$, we have*

$$d(g(x), g(y)) \leq \epsilon d(x, y) \qquad (x, y \in X). \tag{1}$$

Then there exists a unique $x \in X$ such that $g(x) = x$.

Proof. We first check uniqueness. If $x, y \in X$ satisfy $g(x) = x$, $g(y) = y$, then (1) implies

$$d(x, y) = d(g(x), g(y)) \leq \epsilon d(x, y),$$

so $d(x, y) = 0$ and hence $x = y$.

We next check existence. Choose any $x_0 \in X$ and define

$$x_1 = g(x_0), x_2 = g(x_1), \dots.$$

By (1) again,

$$d(x_{n+2}, x_{n+1}) \leq \epsilon d(x_{n+1}, x_n),$$

from which it follows immediately that $x_0, x_1, \dots$ is a Cauchy sequence. Since X is complete, this Cauchy sequence admits a unique limit x. By (1) again, g is continuous for the metric topology, so $x_1, x_2, \dots$ is a Cauchy sequence with limit $g(x)$. By the uniqueness of limits in a metric topology, this forces $g(x) = x$, proving existence of a fixed point. $\square$

Proof of Theorem 3. Pick any real number c satisfying

$$\frac{|f(t_0)|}{|f'(t_0)|} \leq c < |f'(t_0)|.$$

Let X be the set of $t \in K$ satisfying $|t - t_0| \leq c$, equipped with the metric topology. Since f has coefficients in $\mathfrak{o}_K$, so does f'; consequently,

$$|f'(t) - f'(t_0)| \leq |t - t_0| \leq c < |f'(t_0)| \qquad (t \in X),$$

so $|f'(t)| = |f'(t_0)| \neq 0$ for all $t \in X$. We may thus define the function $g : X \to K$ by the formula

$$g(t) = t - \frac{f(t)}{f'(t)}.$$

Since f has coefficients in $\mathfrak{o}_K$, from the definitions of c and X we have

$$|f(t)| \leq \max\{|f(t_0)|, |f'(t_0)||t - t_0|, |t - t_0|^2\} \leq c|f'(t_0)| \qquad (t \in X).$$

Since we already computed that $|f'(t)| = |f'(t_0)|$, this implies

$$|f(t)| \leq c|f'(t)| \qquad (t \in X),$$

so $|g(t) - t| \leq c$ and so $|g(t) - t_0| \leq c$. In other words, g maps X into itself.

Now choose $t, u \in X$ and expand $f(u), f'(u)$ as polynomials in $u - t$:

$$f(u) = f(t) + f'(t)(u-t) + \cdots$$
$$f'(u) = f'(t) + f''(t)(u-t) + \cdots .$$

We then compute that as a formal (and also convergent) power series in $u - t$,

$$g(u) - g(t) = \frac{f(t)f''(t)}{f'(t)^2}(u-t) + \cdots ,$$

from which we see that

$$|g(u) - g(t)| \leq \frac{c}{|f'(t_0)|}|u-t|.$$

We may thus apply Lemma 4 to deduce that there is a unique $t \in X$ such that $g(t) = t$, and hence $f(t) = 0$.

This proves that there is a unique root t of f satisfying $|t - t_0| \leq c$. On one hand, since we could have taken $c = |f(t_0)|/|f'(t_0)|$, we deduce that

$$|t - t_0| \leq \frac{|f(t_0)|}{|f'(t_0)|}.$$

On the other hand, since c can be taken arbitrarily close to $|f'(t_0)|$, we deduce that t is the unique root of f for which $|t - t_0| < |f'(t_0)|$. (Note that Lemma 4 does not directly apply to the set of $t \in K$ for which $|t - t_0| < |f'(t_0)|$, because the value of ϵ cannot be chosen uniformly.)

$\square$