Math 254A. Hensel’s Lemma

Proposition. Let $K$ be a field, complete with respect to a non-archimedean absolute value $|\cdot|$, let $A$ be its valuation ring $\{a \in K \mid |a| \leq 1\}$, and let $f(x) \in A[x]$. Assume that $\alpha_0 \in A$ satisfies

$$|f(\alpha_0)| < |f'(\alpha_0)|^2$$

(1)

(where $f'$ is the derivative taken formally). Then the sequence defined by

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}, \quad i \in \mathbb{N}$$

converges to a root $\alpha$ of $f$ satisfying

$$|\alpha - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < 1.$$ (2)

This root is the only root of $f$ satisfying (2); more generally it is the only root of $f$ satisfying

$$|\alpha - \alpha_0| < |f'(\alpha_0)|.$$ (3)

Proof. First we claim that if $|\alpha - \alpha_0| < |f'(\alpha_0)|$ then $|f'(\alpha)| = |f'(\alpha_0)|$. To see this, we first note that since $\alpha_0 \in A$ and $f'(x) \in A[x]$, $f'(\alpha_0) \in A$ and therefore also $\alpha \in A$. By Taylor’s formula (for polynomials) there exists $\beta \in A$ such that

$$f'(\alpha) = f'(\alpha_0) + \beta(\alpha - \alpha_0).$$

Thus

$$|f'(\alpha) - f'(\alpha_0)| \leq |\alpha - \alpha_0| < |f'\alpha_0|$$

and therefore $|f'(\alpha)| = |f'(\alpha_0)|$ by the non-archimedean property of the valuation. In particular, by (1), this holds for all $\alpha$ satisfying (2).

Now let $c = |f(\alpha_0)|/|f'(\alpha_0)|^2 < 1$. By induction we will show that, for all $i \geq 0$,

(i). $|\alpha_i - \alpha_0| \leq |f(\alpha_0)|/|f'(\alpha_0)| < 1$,
(ii). $|f'(\alpha_i)| = |f'(\alpha_0)|$, and
(iii). $|f(\alpha_i)| \leq c^2|f'(\alpha_0)|^2$.

The base case $i = 0$ holds trivially. By (ii) and (iii) (by induction), we have

$$|\alpha_{i+1} - \alpha_i| = \frac{|f(\alpha_i)|}{|f'(\alpha_i)|} \leq c|f'(\alpha_0)| = \frac{|f(\alpha_0)|}{|f'(\alpha_0)|}$$
and therefore (i) holds for $i + 1$. The claim then implies that (ii) holds for $i + 1$. Finally, we show (iii). By Taylor’s formula, there exists $\beta \in A$ such that

$$
\begin{align*}
f(\alpha_{i+1}) &= f(\alpha_i) + f'(\alpha_i)(\alpha_{i+1} - \alpha_i) + \beta(\alpha_{i+1} - \alpha_i)^2 \\
&= f(\alpha_i) + f'(\alpha_i)\left(-\frac{f(\alpha_i)}{f'(\alpha_i)}\right) + \beta(\alpha_{i+1} - \alpha_i)^2 \\
&= \beta(\alpha_{i+1} - \alpha_i)^2.
\end{align*}
$$

Taking absolute values gives

$$
|f(\alpha_{i+1})| \leq |\alpha_{i+1} - \alpha_i|^2 = \left(\frac{|f(\alpha_i)|}{|f'(\alpha_i)|}\right)^2 = \left(\frac{|f(\alpha_i)|}{|f'(\alpha_0)|}\right)^2 \leq (c^2|f'(\alpha_0)|)^2 = c^{2i+1}|f'(\alpha_0)|^2.
$$

This proves (iii).

The sequence $(\alpha_i)$ therefore is a Cauchy sequence; by continuity, its limit $\alpha$ is a root of $f$.

Finally, we prove the uniqueness statement. Suppose $\alpha$ and $\alpha'$ are distinct roots of $f$ satisfying (3). We then have $|\alpha - \alpha'| < |f'(\alpha_0)|$. But by Taylor’s formula,

$$
f(\alpha') = f(\alpha) + f'(\alpha)(\alpha' - \alpha) + \beta(\alpha' - \alpha)^2
$$

for some $\beta \in A$. Since $f(\alpha) = f(\alpha') = 0$ and $\alpha \neq \alpha'$, this gives

$$
\begin{align*}
f'(\alpha) &= -\beta(\alpha' - \alpha); \\
|f'(\alpha)| &\leq |\alpha' - \alpha| < |f'(\alpha_0)|.
\end{align*}
$$

This is a contradiction since the claim at the beginning of the proof implies that $|f'(\alpha)| = |f'(\alpha_0)|$. \qed