Math 254A. Hensel's Lemma

Proposition. *Let* $K = (K, |\cdot|)$ *be a complete non-archimedean valued field, let* A *be its valuation ring* $\{a \in K \mid |a| \le 1\}$, *and let* $f(x) \in A[x]$. *Assume that* $\alpha_0 \in A$ *satisfies*

$$|f(\alpha_0)| < |f'(\alpha_0)|^2 \tag{1}$$

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

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

converges to a root α *of* f *satisfying*

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

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

$$|\alpha - \alpha_0| < |f'(\alpha_0)|\,. \tag{3}$$

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

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

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

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

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

The base case $i = 0$ holds trivially.

For the inductive step, assume that (i)–(iii) hold for some value of i.

First, by (ii) and (iii) for i, we have

$$|\alpha_{i+1} - \alpha_i| = \frac{|f(\alpha_i)|}{|f'(\alpha_i)|} \le \frac{c^{2^i}|f'(\alpha_0)|^2}{|f'(\alpha_0)|} = c^{2^i}|f'(\alpha_0)|\,. \tag{4}$$

Now we show (i) for $i+1$. By (4), the inequality $c < 1$, and the definition of c,

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

Combining this with (i) for i then gives (i) for $i+1$.

To show (ii), we have

$$|\alpha_{i+1}-\alpha_0| \le \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < |f'(\alpha_0)| \, .$$

by (i) and (1). Therefore the claim applies, which gives (ii) for $i+1$.

Finally, we show (iii). By Taylor's formula, there exists $\beta \in A$ such that

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

Taking absolute values and applying (4) gives

$$|f(\alpha_{i+1})| \le |\alpha_{i+1}-\alpha_i|^2 \le (c^{2^i}|f'(\alpha_0)|)^2 = c^{2^{i+1}}|f'(\alpha_0)|^2 \, .$$

This proves (iii) for $i+1$.

The sequence (α_i) therefore is a Cauchy sequence by (4). By continuity and (iii), its limit α is a root of f.

Finally, we prove the uniqueness statement. Suppose α and α' 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 $\alpha \ne \alpha'$, this gives

$$\begin{gathered} f'(\alpha) = -\beta(\alpha'-\alpha); \\ |f'(\alpha)| \le |\alpha'-\alpha| < |f'(\alpha_0)| \, . \end{gathered}$$

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