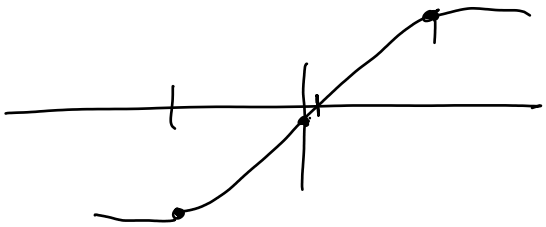
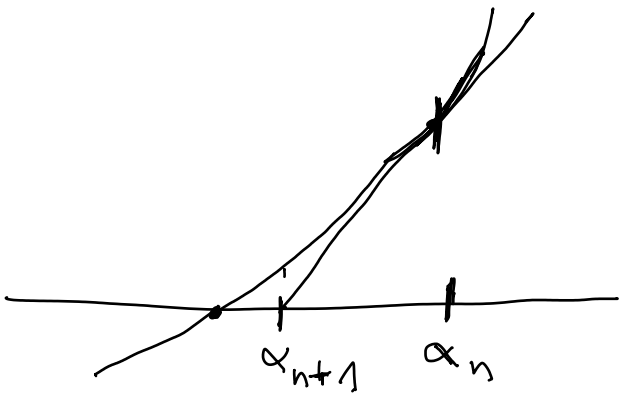
Finding roots over $\mathbb{R}$

- Intermediate value theorem



Doesn't work over $\mathbb{C}$, $\mathbb{Q}_p$ because there's no good ordering.

- Newton's method



Applies over $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$, ...

Hensel's lemma (V 2)

Hensel's lemma (V2)

Let $f(X) \in \mathcal{O}_v[X]$ and assume $\alpha \in \mathcal{O}_v$ satisfies

$$v(f(\alpha)) > 2v(f'(\alpha)) \qquad (I)$$

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

Then, there is exactly one root $\beta \in \mathcal{O}_v$ of $f(X)$ such that $v(\beta - \alpha) > v(f'(\alpha))$.

$$|\beta - \alpha| < |f'(\alpha)|$$

It actually satisfies $v(\beta-\alpha) \geq v(f(\alpha)) - v(f'(\alpha)) \underset{(I)}{>} v(f(\alpha))$.

$$|\beta - \alpha| \leq \left| \frac{f(\alpha)}{f'(\alpha)} \right|.$$

Ex $\sqrt{9} \in \mathbb{Z}_2$ (Okay, $\sqrt{9}$ is a little silly. :)

Pf (assuming V2)

$f(X) = X^2 - 9 + 7$

$v_2(f(1)) = v_2(8) = 3$

$v_2(f'(1)) = v_2(2) = 1.$ □

Pf that V2 $\Rightarrow$ V1

α root mod $\mathfrak{p} \Rightarrow v(f(\alpha)) \geq 1$

α simple root mod $\mathfrak{p} \Rightarrow v(f'(\alpha)) = 0.$ □

Pf of V2

Existence

Let $\alpha_0 = \alpha$.

Let $\alpha_1 = \alpha_0 + t_1$ for some $t_1 \in \mathcal{O}_v$.

["$f(\alpha_1) = f(\alpha_0 + t_1) = f(\alpha_0) + t \cdot f'(\alpha_0) + \mathcal{O}(t^2)$"]

Write $f(X) = \sum c_i X^i$.

$$\Rightarrow f(\alpha_1) = f(\alpha_0 + t_1) = \sum c_i (\alpha_0 + t_1)^i$$

$$= \sum c_i \left(\alpha_0^i + i\alpha_0^{i-1} \cdot t_1 + \dots t_1^2 + \dots\right)$$

$$\equiv \sum c_i \left(\alpha_0^i + i\alpha_0^{i-1} \cdot t_1\right) \equiv \sum c_i \alpha_0^i + \sum i c_i \alpha_0^{i-1} t_1$$

$$\equiv f(\alpha_0) + t_1 \cdot f'(\alpha_0) \mod t_1^2$$

Picks $t_1 = -\dfrac{f(\alpha_0)}{f'(\alpha_0)} \in \mathcal{O}_v$.

$$\Rightarrow f(\alpha_1) \equiv 0 \mod t_1^2.$$

$$\Rightarrow v(f(\alpha_1)) \geq 2v(t_1) = 2v(f(\alpha_0)) - 2v(f'(\alpha_0))$$

$$\overset{(I)}{>} v(f(\alpha_0))$$

$$f'(\alpha_1) = f'(\alpha_0 + t_1) \equiv f'(\alpha_0) \mod t_1.$$

$\Rightarrow v(f'(\alpha_1)) \geq \min(v(f'(\alpha_0)), v(t_1))$ with equality if $v(f'(\alpha_0)) < v(t_1)$.

Indeed, $v(t_1) = v(f(\alpha_0)) - v(f'(\alpha_0)) \underset{(I)}{\geq} v(f'(\alpha_0))$.

$\Rightarrow v(f'(\alpha_1)) = v(f'(\alpha_0))$.

$\Rightarrow \alpha_1$ still satisfies (I) and we can continue:

$$\alpha_2 = \alpha_1 + t_2, \quad \alpha_3 = \alpha_2 + t_3, \dots$$

We have shown that

$$v(f(\alpha_0)) < v(f(\alpha_1)) < \dots \Rightarrow f(\alpha_n) \xrightarrow{n\to\infty} 0$$

$$v(f'(\alpha_0)) = v(f'(\alpha_1)) = \dots$$

$$v(t_1) < v(t_2) < \dots \Rightarrow t_n \xrightarrow{n\to\infty} 0$$

We have $\alpha_n = \alpha_0 + t_1 + \dots + t_n$.

$\Rightarrow \beta = \lim_{n\to\infty} \alpha_n = \alpha_0 + \sum_{n=0}^{\infty} t_n$ exists in $\mathcal{O}_v$.
($t_n \to 0$)

$$f(\beta) = f(\lim \alpha_n) = \lim f(\alpha_n) = 0.$$

Also $v(\beta - \alpha_0) = v(\sum t_n) \geq v(t_1)$

$$= v(f(\alpha_0)) - v(f'(\alpha_0)).$$

Uniqueness Let $\beta_1 \neq \beta_2 \in \mathcal{O}_v$ be roots of $f(x)$ such that $v(\beta_i - \alpha) > v(f'(\alpha))$ for $i = 1, 2$.

As in the proof of existence, it follows that

$$v(f'(\beta_i)) = v(f'(\alpha)).$$

Write $\beta_2 = \beta_1 + t$.

$$\Rightarrow v(t) = v(\beta_1 - \beta_2) \geq \min(v(\beta_1 - \alpha), v(\beta_2 - \alpha))$$

$$> v(f'(\alpha)) = v(f'(\beta_1)).$$

As before, $\underbrace{f(\beta_2)}_{0} \equiv \underbrace{f(\beta_1)}_{0} + t \cdot f'(\beta_1) \bmod t^2$.

$$\Rightarrow f'(\beta_1) \equiv 0 \bmod t.$$

$$\Rightarrow v(t) \leq v(f'(\beta_1)). \quad \lightning$$

□

Hensel's lemma (V3)

Let $f(X) \in \mathcal{O}_v[X]$ and assume $f(X) \equiv \bar{g}(X)\bar{h}(X) \bmod \mathfrak{p}_v$ for relatively prime polynomials $\bar{g}(X), \bar{h}(X) \in k_v[X]$.

Then, there exist unique $g(X), h(X) \in \mathcal{O}_v[X]$ (lifts) such that $g(X) \equiv \bar{g}(X) \bmod \mathfrak{p}$, $\deg(g) = \deg(\bar{g})$

$$h(X) \equiv \bar{h}(X) \bmod \mathfrak{p},$$

with $f(X) = g(X) \cdot h(X)$.

Warning It's possible that $\deg(f) > \deg(f \bmod \mathfrak{p}_v)$.

(Leading coeff. of f is $\equiv 0 \bmod \mathfrak{p}_v$.)

$\Rightarrow$ We can't simultaneously ensure

$\deg(g) = \deg(\bar{g})$ and $\deg(h) = \deg(\bar{h})$.

Pf See Neukirch, Algebraic Number Theory, Thm II.4.6. □

Pf that V3 $\Rightarrow$ V1

If $\alpha \in k_v$ is a simple root mod $\mathfrak{p}$, we can take $\bar{g}(X) = X - \alpha$, $\bar{h}(X) = \dfrac{f(X) \bmod \mathfrak{p}_v}{X - \alpha}$.

simple $\Rightarrow$ rel. prime

$\rightsquigarrow$ lin. pol. $g(X) = X - \beta$ dividing $f(X)$.

$\rightsquigarrow$ root $\beta \in \mathcal{O}_v$. □

1.6. Algebraic extensions

Stupid lemma

Let K be complete w.r.t. disc. val. v and let $f(X) = a_n X^n + \dots + a_0 \in K[X]$ be irreducible.

Then, $v(a_i) \geq \min(v(a_n), v(a_0))$ $\forall i$.

Pf Multiply by some power of π so that w.l.o.g.

$v(a_i) \geq 0$ $\forall i$ and $v(a_i) = 0$ for some i.

Let $v(a_i) = 0$ and $v(a_{i-1}), \dots, v(a_0) > 0$.

$\Rightarrow f(X) \equiv a_n X^n + \dots + a_i X^i$

$\equiv \underbrace{X^i}_{\bar{g}(X)} \underbrace{(a_n X^{n-i} + \dots + a_i)}_{h(X)}$ mod $\mathfrak{p}$

$h(X) \leftarrow$ not divisible by X because $a_i \not\equiv 0 \bmod \mathfrak{p}_v$.

$\Rightarrow \bar{g}(X), h(X)$ rel. prime

$\overset{V3}{\Rightarrow} f(X) = g(X)h(X)$ for some pol. $g(X), h(X) \in \mathcal{O}_v[X]$ with $\deg(g) = \deg(\bar{g}) = i$.

$\Rightarrow f(X)$ is not irred. unless

$i = 0$ (so $v(a_0) = 0$)
$i = n$ (so $v(a_n) = 0$)
$\Rightarrow \min(v(a_n), v(a_0)) = 0$.

□

Thm Let K be complete w.r.t. the disc. val. v and let L be a field extension of degree n. Then, there is exactly one disc. val. v' on L that extends v (so that $v'|_K = v$):

$$v'(x) = \frac{1}{n} v(\mathrm{Nm}_{L|K}(x)) \quad \text{for } x \in L.$$

$$|x|' = \sqrt[n]{|\mathrm{Nm}_{L|K}(x)|}$$

Then, $\mathcal{O}_{v'} \subseteq L$ is the integral closure of $\mathcal{O}_v$ in L.

Also, L is complete w.r.t. v'.

Analogy The only extension of $|\cdot|$ from $K = \mathbb{R}$ to $L = \mathbb{C}$ is $|x| = \sqrt{|x\bar{x}|}$.

Pf of thm

v' is a disc. val. satisfying the stated conditions

For $x \in K$: $v'(x) = \frac{1}{n} v(\underbrace{\mathrm{Nm}_{L|K}(x)}_{x^n}) = v(x)$. $\Rightarrow v'|_K = v$.

a) For $x \in L$: $v'(x) = \infty \Leftrightarrow \mathrm{Nm}_{L|K}(x) = 0 \Leftrightarrow x = 0$.

b) For $x, y \in L$: $v'(xy) = \frac{1}{n} v(\underbrace{\mathrm{Nm}(xy)}_{\mathrm{Nm}(x)\mathrm{Nm}(y)}) = v'(x) + v'(y)$.

Claim: $x \in L$ integral over $\mathcal{O}_v \iff v'(x) \geq 0$

Pf Let $f(X) = X^t + a_{t-1} X^{t-1} + \dots + a_0 \in K[X]$ be the min. pol. of x.

$\Rightarrow \mathrm{Nm}_{K(x)|K}(x) = \pm a_0$

$\Rightarrow \mathrm{Nm}_{L|K}(x) = \mathrm{Nm}_{K(x)|K}(\underbrace{\mathrm{Nm}_{L|K(x)}(x)}_{x^{[L:K(x)]}}) = (\pm a_0)^{[L:K(x)]}$.

"$\Rightarrow$" x integral $\Rightarrow f(X) \in \mathcal{O}_v[X] \Rightarrow a_0 \in \mathcal{O}_v$

$\Rightarrow \underbrace{\mathrm{Nm}_{L|K}(x)}_{v(\dots) \geq 0} \in \mathcal{O}_v \Rightarrow v'(x) \geq 0$.

"$\Leftarrow$" $v'(x) \geq 0 \Rightarrow v(a_0) \geq 0$

$\Rightarrow v(a_i) \geq 0 \ \forall i \Rightarrow f(X) \in \mathcal{O}_v[X]$

(Stupid lemma)

$\Rightarrow x$ integral. $\square$

c) Claim For $x, y \in L$: $v'(x+y) \geq \min(v'(x), v'(y))$.

Pf W.l.o.g. $v'(x) \geq v'(y)$. $\Rightarrow v'(\frac{x}{y}) \geq 0$.

$\Rightarrow \frac{x}{y}$ integral $\Rightarrow \frac{x}{y} + 1$ integral

$\Rightarrow v'(\frac{x}{y} + 1) \geq 0$

$\Rightarrow v'(x+y) \geq v'(y) = \min(v'(x), v'(y))$. $\square$

L is complete w.r.t. v' because it is a fin.-dim. normed vector space over a complete field.

(choose a basis of L. Take any Cauchy sequence $a_1, a_2, \ldots \in L$. In any fixed coordinate, the sequence is a Cauchy seq. and hence converges in K. $\Rightarrow$ The seq. converges in L.)

Uniqueness of v'

Assume that v'' is another disc. val. extending v.

$\mathcal{O}_{v''}$ is a PID contain $\mathcal{O}_v$.

$\Downarrow$

integrally closed

$\Rightarrow \mathcal{O}_{v'} \subseteq \mathcal{O}_{v''}$ [Idea: Enlarging $\mathcal{O}_{v'}$ would kill primes but the local ring $\mathcal{O}_{v'}$ already has just one prime!]

$\mathfrak{p}_{v''} \cap \mathcal{O}_{v'}$ is a nonzero prime ideal of $\mathcal{O}_{v'}$.

$\Rightarrow \mathfrak{p}_{v''} \cap \mathcal{O}_{v'} = \mathfrak{p}_{v'}$

$\Rightarrow \mathfrak{p}_{v'} \subseteq \mathfrak{p}_{v''}$

If $v''(x) \geq 0$, then $v''\left(\frac{1}{x}\right) \leq 0$. $\Rightarrow \frac{1}{x} \notin \mathfrak{p}_{v''} \Rightarrow \frac{1}{x} \notin \mathfrak{p}_{v'}$

$\Rightarrow v'\left(\frac{1}{x}\right) \leq 0 \Rightarrow v'(x) \geq 0$.

$\Rightarrow \mathcal{O}_{v''} \subseteq \mathcal{O}_{v'} \Rightarrow \mathcal{O}_{v'} = \mathcal{O}_{v''}$

$\Rightarrow \mathfrak{p}_{v'} = \mathfrak{p}_{v''} \Rightarrow v' = \lambda \cdot v''$ for some $\lambda > 0$.

$\Rightarrow v' = v''$ ($v'|_K = v''|_K$) $\square$

Alternative proof of uniqueness (Thanks, Wyatt and Xavier!)

Apply the norm equivalence theorem to the finite-dimensional K-vector space L. If the norms $|x|' = \lambda^{-v'(x)}$ and $|x|'' = \lambda^{-v''(x)}$ arising from discrete valuations v', v'' differ by a bounded factor, we must have $v' = v''$. $\square$