TODAY:

§ Hensel's lemma & completions

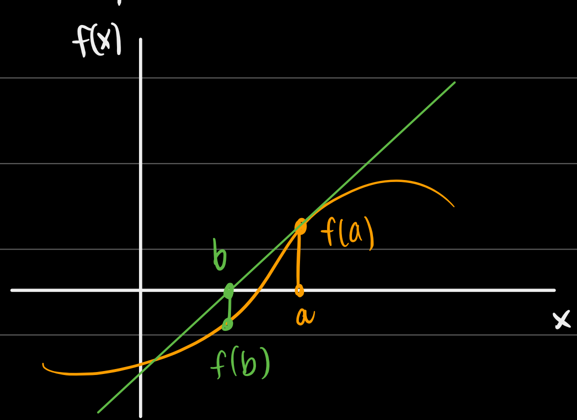
§ equivalent forms of henselianity

§ Hensel's lemma

We will work with $vK \cong \mathbb{Z}$.

We will figure out Hensel's lemma starting from a very basic question: given a valued field (K,v) and $f \in \mathcal{O}_v[x]$, how do we find a root of f in $\mathcal{O}_v$? A necessary condition is certainly that $\bar{f} \in Kv[x]$ has a root. Let $\bar{a} \in Kv$ be such. This is of course not enough: take residues of the coefficients indeed, it may very well be that $f(a) \neq 0$. Yet, we may be optimistic and hope for $b \in \mathcal{O}_v$ such that $\bar{b} = \bar{a}$ & $f(b) = 0$. How do find such a b?

The necessary requirement that $\bar{f}(\bar{a}) = \bar{0}$ is really the same as $v(f(a)) > 0$, which intuitively speaking means that $f(a)$ is very small — i.e., a is an approximation of a root of f. What we might be tempted to do is approach this like a numerical problem, so we might try to find a better approximation of a root than a, i.e. $b \in \mathcal{O}_v$ s. that $v(f(b)) > v(f(a))$. To do that, we will use Newton's method:



$$b := a - \frac{f(a)}{f'(a)}.$$

Let's see whether b is really a better approximation:

$$f(b) = f\left(a - \frac{f(a)}{f'(a)}\right) =$$

Taylor expansion $= f(a) + \left(-\frac{f(a)}{\cancel{f'(a)}}\right)\cancel{f'(a)} + \left(\frac{f(a)}{f'(a)}\right)^2 \cdot \underset{\in \mathcal{O}_v}{c}$

so,

$$f(b) = \cancel{f(a)} - \cancel{f(a)} + \left(\frac{f(a)}{f'(a)}\right)^2 \cdot c = \left(\frac{f(a)}{f'(a)}\right)^2 \cdot c$$

hence

$$v(f(b)) - v(f(a)) = \underbrace{2v(f(a))} - 2v(f'(a)) + \underbrace{v(c)}_{\geq 0} - \underbrace{v(f(a))}$$

$$\geq v(f(a)) - 2v(f'(a))$$

$$> 0 \iff v(f(a)) > 2v(f'(a)).$$

So we need to add $v(f(a)) > 2v(f'(a))$ to our hypotheses.

Note that this already implies $v(f(a)) > 0$.

If we want to iterate this, we need to check that $\boxed{\text{this}}$ holds for b too, i.e. that $v(f(b)) > 2v(f'(b))$. However,

$$f'(b) = f'\left(a - \frac{f(a)}{f'(a)}\right)$$

Taylor expansion $= f'(a) + \left(-\frac{f(a)}{f'(a)}\right) f''(a) + \cdots$

$$= f'(a)\left[1 + \frac{f(a)}{(f'(a))^2} \cdot \underset{\mathcal{O}_v}{d}\right]$$

so $v(f'(b)) = v(f'(a)) + v\left(1 + \frac{f(a)}{f'(a)^2} \cdot d\right)$

$= v(f'(a))$ since $v\left(\frac{f(a)}{f'(a)^2} d\right) = v\left(\frac{f(a)}{f'(a)^2}\right) + v(d) > 0$

and hence

$$v(f(b)) > v(f(a)) > 2v(f'(a)) = 2v(f'(b)).$$

This means that we can iterate this! Say $a_0 = a$, $a_1 = b$, $\cdots$ we obtain a sequence $(a_n)_{n \in \mathbb{N}} \subseteq \mathcal{O}_v$ such that i.) $a_{n+1} = a_n - \dfrac{f(a_n)}{f'(a_n)}$,

ii.) $v(f(a_{n+1})) > v(f(a_n))$.

Indeed, we may see that

$$v(a_2 - a_1) = v\left(\frac{f(a_1)}{f'(a_1)}\right) = v\left(f'(a_1)\cdot\frac{f(a_1)}{f'(a_1)^2}\right)$$

$$= v(f'(a_1)) + v(f(a_1)) - 2v(f'(a_1))$$

$a_1 = b$ $$= v(f'(b)) + v(f(b)) - 2v(f'(b))$$

$v(f'(b)) = v(f'(a))$ $$= v(f'(a)) + v(f(b)) - 2v(f'(a))$$

$$= v(f'(a)) + v\left(\left(\frac{f(a)}{f'(a)}\right)^2\cdot c\right) - 2v(f'(a))$$

$v(f'(a)) \geq 0$ $$\geq 2v(f(a)) - 2v(f'(a)) + v(c) - 2v(f'(a))$$

$v(c) \geq 0$ $$\geq 2\left[\underbrace{v(f(a)) - 2v(f'(a))}_{\varepsilon}\right]$$

and more generally, $v(a_{n+1} - a_n) \geq 2^n\varepsilon$, so

$$\lim_{n\to\infty} v(a_{n+1} - a_n) = \infty.$$

This should ring a bell: $(a_n)_{n\in\mathbb{N}} \subseteq \mathcal{O}_v$ is cauchy! But wait, we don't have a metric, right?

§ INTERLUDE

Given $v : K^\times \twoheadrightarrow \mathbb{Z}$, we may give K a metric by

$$d_v(a,b) = \exp(-v(a-b)) \in \mathbb{R}^{\geq 0} \quad \& \quad \exp(-\infty) := 0.$$

We can thus consider (K, d_v) as a metric space and consider Cauchy sequences in it. To complete - pun not intended - our proof we will need $(a_n)_{n\in\mathbb{N}}$ to converge, i.e. (K, d_v) to be complete as a metric space.

→ if (X,d) is not complete, we can always embed (X,d) as the dense subspace of a complete metric space $(\hat{X},\hat{d})$, which is unique up to isometry over X. It is built this way:

1) $\hat{X} = \{\text{Cauchy sequences}\}/\sim$, where $(a_n)_n \sim (b_n)_n \Leftrightarrow \lim_{n\to\infty} d(a_n,b_n)=0$,

2) $\hat{d}([a_n],[b_n]) = \lim_{n\to\infty} d(a_n,b_n)$.

Think of $\mathbb{Q}$, with $d(a,b)=|a-b|$. Then $\hat{\mathbb{Q}} \simeq \mathbb{R}$!

If we take d_{v_p} instead, i.e. $d_p(a,b) = p^{-v_p(a-b)}$, then

$$(\hat{\mathbb{Q}}, \hat{d_{v_p}}) =: (\mathbb{Q}_p, d_p)$$

is a friend we will meet often. We could write

$$\mathbb{Q}_p = \left\{ \sum_{n\geq N} a_n p^n \;\middle|\; N\in\mathbb{Z},\ a_n \in \{0,1,\dots p-1\} \right\}$$

and do computations by carry-over.

Then, if we assume (K,v) is complete (i.e., (K,d_v) is complete as a metric space), $(a_n)_{n\in\mathbb{N}}$ has a limit $\alpha\in\mathcal{O}_v$ and we have

$$f(a_n) \to f(\alpha) \quad \text{as } f \text{ is continuous in the } d_v\text{-topology}$$

$$\Rightarrow \quad f(\alpha)=0. \quad \text{since } v(f(a_n)) \to \infty \text{ and } v(f(\alpha)) = \lim_{n\to\infty} v(f(a_n))$$

Moreover, $v(\alpha - a) > v(f'(a)) \geq 0$ and so $\bar{\alpha} = \bar{a}$.

Summing up,

HENSEL'S LEMMA. Suppose (K,v), $vK \simeq \mathbb{Z}$, is a complete valued field. Then, for any $f\in\mathcal{O}_v[x]$ and $a\in\mathcal{O}_v$ such that $v(f(a)) > 2v(f'(a))$, there is $\alpha\in\mathcal{O}_v$ such that $v(\alpha-a) > v(f'(a))$ & $f(\alpha)=0$.

any value group!

Def.^{n} if (K,v) satisfies ▨, we call it $\boxed{\text{henselian.}}$

What we have just proved is, hence, the statement

complete valued fields are henselian.

§ equivalent forms of henselianity

LEMMA. (K,v) is henselian $\iff$ for each $f \in \mathcal{O}_v[X]$ and $a \in \mathcal{O}_v$, if $v(f(a)) > 0$ and $v(f'(a)) = 0$, then there is $b \in \mathcal{O}_v$ such that $f(b) = 0$ and $v(b-a) > 0$.

PROOF. $(\Rightarrow)$ if $v(f'(a)) = 0$, then

$$v(f(a)) > 0 = 2v(f'(a)).$$

$(\Leftarrow)$ using Taylor expansion,

$$f(a-X) = f(a) - f'(a)X + X^2 g(a,X)$$

for $g(Y,X) \in \mathcal{O}_v[Y,X]$. Let $Y = \frac{X}{f'(a)}$, then

$$h(Y) := \frac{f(a-f'(a)Y)}{f'(a)^2} = \frac{f(a)}{f'(a)^2} - Y + g(a, f'(a)Y)Y^2$$

satisfies $\bar{h}(\bar{0}) = \bar{0}$, $\bar{h}'(\bar{0}) = \overline{-1}$. Let $h(\alpha) = 0$, so $b = a - f'(a)\alpha \in \mathcal{O}_v$ is a root of f as requested. ▨

THEOREM. (K,v) valued field, TFAE:

i.) v extends uniquely to any finite extension to K,

ii.) (K,v) is henselian,

iii.) every polynomial of the form

$$X^n + X^{n-1} + a_{n-2}X^{n-2} + \dots + a_0$$

with $a_i \in \mathfrak{m}_v$, $0 \le i \le n-2$, has a zero in K.

PROOF. We prove (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i $\Rightarrow$ ii). Take $f \in \mathcal{O}_v[X]$, $a \in \mathcal{O}_v$ with $\bar{f}(\bar{a}) = \bar{0}$, $\bar{f}'(\bar{a}) \neq \bar{0}$. Upon replacing f by one of its irreducible components, we may assume it is irreducible. Further, we may assume it is separable; if $f = g(X^p)$, then $\bar{f}' \equiv 0$, a contradiction.

Let L be the splitting field of f over K. Write

$$f = c \prod_{i=0}^{n} (X - a_i)$$

for some $c \in \mathcal{O}_v^\times$, say with $\bar{a}_1 = \bar{a}$. Let w be the unique extension of v to L. If $n=1$, we are done; so assume $n>1$. Let $\sigma \in Gal(L/K)$ satisfy $\sigma(a_1) = a_2$. Then σ induces $\bar{\sigma} \in Gal(Lw/Kv)$ (since w is the unique extension!) with

$$\bar{a}_2 = \bar{\sigma}(\bar{a}_1) = \bar{\sigma}(\bar{a}) = \bar{a} = \bar{a}_1,$$

but then $\bar{a} = \bar{a}_1 = \bar{a}_2$ is not a simple root. ↯

(ii $\Rightarrow$ iii). We have

$$\bar{f} = (X+1)X^{n-1}$$

and thus $\overline{-1}$ is a simple zero.

(iii $\Rightarrow$ i). Assume not, so there is $K \subseteq N$ finite and v has finitely many distinct extensions to N, say $v_1, \dots, v_n$. Let

$$D = \{\sigma \in Gal(N/K) : \sigma(\mathcal{O}_{v_1}) = \mathcal{O}_{v_1}\} \le Gal(N/K)$$

and note that $D \lneq Gal(N/K)$ (because of the Conjugation Theorem!). Then $L = Fix(D) \supsetneq K$ is a proper extension. Call $\mathcal{O}_1' = L \cap \mathcal{O}_{v_1}$. Note that, by Conjugation, $\mathcal{O}_1'$ has a unique prolongation to L. Note that then if $\sigma_1 \notin D$, $\mathcal{O}_1' = \mathcal{O}_{v_1} \cap L = \sigma_1(\mathcal{O}_{v_1}) \cap L \neq \mathcal{O}_1'$. We can then apply Weak Approximation and find $\beta \in R = \mathcal{O}_1' \cap \dots \cap \mathcal{O}_n' \subseteq L$ such that $\beta - 1 \in m_1'$, $\beta \in m_i'$ for $i > 1$. As $\mathcal{O}_1' \neq \mathcal{O}_i'$, $\beta \notin K$: let f be its minimal polynomial over K, say

$$f(X) = X^k + a_{k-1} X^{k-1} + \dots + a_0$$

for some $a_i \in K$.

Say $\beta = \beta_1, \dots \beta_k$ are the conjugates of β in N. For $\sigma \in G \setminus D$, $\beta \in \sigma(m_1)$ by definition, so $\sigma(\beta) \in m_1$ for all $\sigma \in G \setminus D$. As the $\beta_2, \dots \beta_k$ are exactly the $\sigma(\beta_1)$ for $\sigma \in G \setminus D$, $\beta_i \in m_1$ for all i.

And now

$$f(X) = \prod (X - \beta_i)$$

satisfies

$$a_{k-1} = -(\beta_1 + \dots + \beta_k) \in (1 + m_1) \cap K = 1 + m_v$$

and $a_i \in m_1 \cap K = m_v$.

Thus

$$g(X) = \frac{f(a_{k-1}X)}{(a_{k-1})^k} = X^k + X^{k-1} + \tilde{a}_{k-2} X^{k-2} + \dots + \tilde{a}_0 \in \mathcal{O}_v[X]$$

satisfies the assumptions of (iii). However, f is irreducible, so g cannot have a zero! ↯ ▨