Supplement to the previous lecture

Lemma 18.2 Let R be a DVR with max. ideal $\mathfrak{m}$, $\hat{R} = \varprojlim_n R/\mathfrak{m}^n$ its completion. Then $\mathfrak{m}\cdot\hat{R} = \ker(\hat{R} \to R/\mathfrak{m})$

Proof Recall: we have natural maps $\varphi_n : \hat{R} \longrightarrow R/\mathfrak{m}^n$. Let $u \in \mathfrak{m}$ be a uniformizer; we need to prove that $\hat{\mathfrak{m}} = \ker(\hat{R} \longrightarrow R/\mathfrak{m})$ is generated by u. Let $x \in \hat{\mathfrak{m}}$; $x = (\bar{x}_i)_{i \geq 1}$, with $\bar{x}_i \in R/\mathfrak{m}^i$ and $\overline{x_{i+1}} \equiv \overline{x_i} \pmod{\mathfrak{m}^i}$; also: $\bar{x}_1 = 0$ and $\bar{x}_i \in \mathfrak{m}/\mathfrak{m}^i$;

Let $x_i \in \mathfrak{m}$ be elements s.t.

$\bar{x}_i \equiv x_i \pmod{\mathfrak{m}^i}$. We construct a sequence $y_i \in R$ s.t. $y_{i+1} \equiv y_i \pmod{\mathfrak{m}^{i-1}}$ and $x_i \equiv u \cdot y_i \pmod{\mathfrak{m}^i}$

Induction: $i = 1 \Rightarrow y_1 = 0$

$i > 1$: $x_{i+1} \equiv x_i \equiv u y_i \pmod{\mathfrak{m}^i}$

$\Rightarrow x_{i+1} = u y_i + z_i$ with $z_i \in \mathfrak{m}^i$

$\Rightarrow z_i = u \cdot w_i$ with $w_i \in \mathfrak{m}^{i-1}$

$\Rightarrow x_{i+1} = u(y_i + w_i)$

take $y_{i+1} = y_i + w_i$; both conditions are satisfied. The seq. $(\overline{y_{i+1}})_{i\geq 1}$ $\overline{y}_{i+1}$ is the image of y_{i+1} in R/m^i gives an element $y \in \hat{R}$: $x = u \cdot y$ ☐

Hensel's lemma

Thm 18.3 Let R be a complete DVR (i.e. $\hat{R} = R$), $f \in R[X]$ and $a_0 \in R$ s.t. $|f(a_0)| < |f'(a_0)|^2$. Then there exists unique $a \in R$, s.t. $f(a) = 0$ and $|a - a_0| < |f'(a_0)|$.

Moreover:

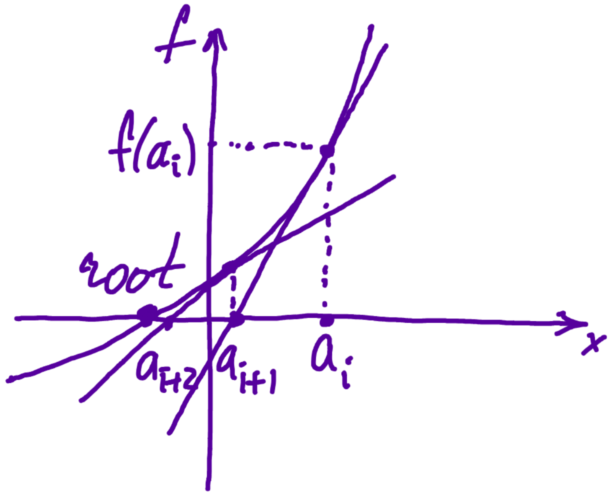
A) $|a - a_0| = \left|\frac{f(a_0)}{f'(a_0)}\right| < 1$

B) $|f'(a)| = |f'(a_0)|$

Rem: we use the absolute value induced by the valuation of R

Proof Consider the sequence $(a_i)_{i\geq 0}$

$$a_{i+1} = a_i - \frac{f(a_i)}{f'(a_i)} \quad \forall i \geq 0$$



Newton's method

Define: $\alpha = \left|\dfrac{f(a_0)}{f'(a_0)^2}\right|$, $\beta = \left|\dfrac{f(a_0)}{f'(a_0)}\right|$

Then: $\alpha < 1$ by assumption,

$$\beta = \alpha \cdot \underbrace{|f'(a_0)|}_{\leq 1} \leq \alpha < 1$$

Recall that $x \in R \iff |x| \leq 1$

We verify inductively $\forall i$ the following:

1) $|a_i| \leq 1$
2) $\left|\dfrac{f(a_i)}{f'(a_i)^2}\right| \leq \alpha^{2^i}$
3) $|f'(a_i)| = |f'(a_0)|$
4) $|a_{i+1} - a_0| = \beta$

For $i=0$: 1) $|a_0| \leq 1$ since $a_0 \in R$

2) by def of α

3) trivial

4) by def. of β

Assume 1), 2), 3) for i, deduce for $i+1$:

1) a_{i+1} is well-defined because $|f'(a_i)|=|f'(a_0)| \neq 0$.

also $|f'(a_i)| \leq 1$ because $f'(a_i) \in R$

We have:

$$|a_{i+1} - a_i| = \left| \frac{f(a_i)}{f'(a_i)} \right| \leq \left| \frac{f(a_i)}{f(a_i)^2} \right| \leq \alpha^{2^i} < 1$$

$$\Rightarrow |a_{i+1}| = |a_{i+1} - a_i + a_i| \leq \max\{|a_{i+1} - a_i|, |a_i|\} \leq 1.$$

2)+3) Use Taylor expansion for f:

if $x, \delta \in R$ then

$$f(x+\delta) = f(x) + f'(x)\delta + b\delta^2$$

for some $b \in R$

We have:

$$f(a_{i+1}) = f\Big(a_i - \underbrace{\frac{f(a_i)}{f'(a_i)}}_{\delta}\Big) =$$

$$= f(a_i) - f'(a_i)\frac{f(a_i)}{f'(a_i)} + b\left(\frac{f(a_i)}{f'(a_i)}\right)^2 = b\left(\frac{f(a_i)}{f'(a_i)}\right)^2$$

$$\Rightarrow |f(a_{i+1})| \leq |b| \left| \frac{f(a_i)}{f'(a_i)} \right|^2 \leq \left| \frac{f(a_i)}{f'(a_i)} \right|^2 \quad (*)$$

Apply Taylor expansion to f':

$$f'(x+\delta) = f'(x) + d \cdot \delta \quad \text{for some } d \in R$$

$$f'(a_{i+1}) = f'(a_i) - d\frac{f(a_i)}{f'(a_i)}$$

By induction: $\left|d\frac{f(a_i)}{f'(a_i)}\right| \le \left|\frac{f(a_i)}{f'(a_i)}\right| \le \alpha^{2^i}|f'(a_i)|$

$< |f'(a_i)|$

$\Rightarrow |f'(a_{i+1})| = |f'(a_i)|$

and we get 3)

Then by (*): $\left|\frac{f(a_{i+1})}{f'(a_{i+1})^2}\right| \le \frac{\left|\frac{f(a_i)}{f'(a_i)}\right|^2}{|f'(a_i)|^2} =$

$= \left|\frac{f(a_i)}{f'(a_i)^2}\right|^2 \le \left(\alpha^{2^i}\right)^2 = \alpha^{2^{i+1}}$ and we get 2)

Prove 4) by induction:

$|a_{i+1} - a_0| = |a_{i+1} - a_i + a_i - a_0| \le$

$\le \max\{|a_{i+1} - a_i|, |a_i - a_0|\}$

enough to prove: $|a_{i+1} - a_i| < \beta$ for $i \ge 1$

We prove inductively

4') $\left|\frac{f(a_i)}{f'(a_i)}\right| < \beta$ for $i \ge 1$

$i=1$: $|f(a_1)| \overset{(*)}{\le} \left|\frac{f(a_0)}{f'(a_0)}\right|^2 = \beta^2 =$

$= \beta \cdot \alpha \cdot |f'(a_0)| < \beta \cdot |f'(a_0)|$

$\Rightarrow \left|\frac{f(a_1)}{f'(a_1)}\right| = \left|\frac{f(a_1)}{f'(a_0)}\right| < \beta$

$i>1$: $\quad |f(a_{i+1})| \overset{(*)}{<} \beta^2 = \beta \cdot \alpha\, |f'(a_0)| <$

by inductive assumption

$< \beta\, |f'(a_0)|$

$$\Rightarrow \left|\frac{f(a_{i+1})}{f'(a_{i+1})}\right| = \left|\frac{f(a_{i+1})}{f'(a_0)}\right| < \beta$$

ande we get 4') and 4).

Property 3) implies:

$$|a_{i+1} - a_i| \le \alpha^{2^i}, \quad |a_{i+2} - a_i| \le \max\{|a_{i+2} - a_{i+1}|, |a_{i+1} - a_i|\} \le \alpha^{2^i}$$

$$\ldots, |a_{i+k} - a_i| \le \alpha^{2^i}$$

$\Rightarrow (a_i)_{i\ge 0}$ is a Cauchy sequence.

$\Rightarrow$ it converges to $a \in R$;

By 3): $\quad 0 \le |f(a_i)| \le \underbrace{\alpha^{2^i}}_{\xrightarrow[i\to\infty]{} 0} \underbrace{|f'(a_i)^2|}_{\xrightarrow[i\to\infty]{} |f'(a)|} \xrightarrow[i\to\infty]{} 0$

$$\Rightarrow |f(a)| = 0 \Rightarrow f(a) = 0$$

Property 4) implies A); 3) implies B) by passing to the limit.

<u>Uniqueness of a:</u> assume we have $\tilde{a} \in R$ s.t. $f(\tilde{a}) = 0$ and $|\tilde{a} - a_0| < |f'(a_0)|$

Then: $|\tilde{a} - a| \leq \max\{|\tilde{a} - a_0|, |a - a_0|\} < |f'(a_0)|$
$= |f'(a)|$

Taylor expansion:

$0 = f(\tilde{a}) = f(a + (\tilde{a} - a)) =$

$= f(a) + f'(a) \cdot (\tilde{a} - a) + b\,(\tilde{a} - a)^2$

for some $b \in R$

$\Rightarrow f'(a) \cdot (\tilde{a} - a) = -b\,(\tilde{a} - a)^2$

if $\tilde{a} - a \neq 0$ then we get

$f'(a) = -b\,(\tilde{a} - a)$

$|f'(a)| = |b| \cdot |\tilde{a} - a| \leq |\tilde{a} - a| < |f'(a)|$

— contradiction

$\Rightarrow \tilde{a} = a$ $\square$

<u>Corollary</u> If $f \in R[x]$ and $\bar{f} \in R/_m[x]$ has a simple root $\bar{a}_0 \in R/_m = k$

i.e. $\bar{f}'(\bar{a}_0) \neq 0$, $\bar{f}(\bar{a}_0) = 0$

Then f has unique simple root $a \in R$ s.t. $a \equiv \bar{a}_0 \pmod{m}$

Proof we have $a_0 \in R$ s.t. $a_0 \equiv \bar{a}_0 \pmod{m}$

$f(a_0) \in m$ since $\bar{f}(\bar{a}_0) = 0$

but $f'(a_0) \notin m$ since $\bar{f}'(\bar{a}_0) \neq 0$

$\Rightarrow |f(a_0)| < 1 = |f'(a_0)|^2$

and we can apply the theorem

to find a root $a \in R$ s.t.

$|f'(a)| = |f'(a_0)| = 1 \Rightarrow a$ is a

simple root

This root is unique s.t. $|a - a_0| < 1$

i.e. $a \equiv a_0 \pmod{m}$ $\square$

Example Consider $R = \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$

$\mathbb{Z}_p/m = \mathbb{F}_p$, $m = p \cdot \mathbb{Z}_p$

Take $f = X^{p-1} - 1 \in \mathbb{Z}_p[X]$

$\bar{f} \in \mathbb{F}_p[X]$ has $p-1$ distinct roots

(all elements of $\mathbb{F}_p^\times$) $\Rightarrow$ all roots

are simple:

If $\xi \in \mathbb{F}_p^\times$, by Hensel's lemma

we find $x \in \mathbb{Z}_p$: $x^{p-1} = 1$

and $x \equiv \zeta \pmod{m}$

$\Rightarrow f$ has $p-1$ distinct simple roots in $\mathbb{Z}_p^\times$;

If we consider the map

$$\mathbb{Z}_p^\times \twoheadrightarrow \mathbb{F}_p^\times,$$

then this gives a section of this map, i.e. $\mathbb{F}_p^\times \hookrightarrow \mathbb{Z}_p^\times$

<u>Corollary</u> 1) $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times U$ where $U = 1 + m$

2) $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{F}_p^\times \times U$

<u>Proof</u> 1) $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times \underbrace{\ker(\mathbb{Z}_p^\times \to \mathbb{F}_p^\times)}_{U}$

2) $\forall x \in \mathbb{Q}_p^\times$ is uniquely written as

$x = p^n \cdot y$ where $y \in \mathbb{Z}_p^\times$, $n \in \mathbb{Z}$

$\Rightarrow \mathbb{Q}_p \simeq \mathbb{Z} \times \mathbb{Z}_p^\times$ $\square$

<u>Roots of unity in $\mathbb{Q}_p$</u>

We assume $p \geq 3$. Let $\mu_1 \dots \mu_{p-1} \in \mathbb{Z}$ be all $(p-1)$'st roots of unity constructed above

<u>Prop. 18.4</u> Let $\zeta \in \mathbb{Q}_p$ be a root of unity. Then $\zeta = \mu_i$ for some i.

<u>Proof</u> it is clear $|\zeta| = 1 \Rightarrow \zeta \in \mathbb{Z}_p^\times$

Let m be the order of ζ; $m > 1$

<u>Case 1</u> $(m, p) = 1$

$\exists i$ s.t. $\zeta \equiv \mu_i \pmod{\mathfrak{m}}$, because $\mu_1 \dots \mu_{p-1}$ represent all residue classes mod $\mathfrak{m}$.

Then both ζ and μ_i are roots of $f = X^{m \cdot (p-1)} - 1$. Note:

$$|f'(\mu_i)| = |m \cdot (p-1) \mu_i^{m(p-1)-1}| = 1$$

By uniqueness part of Hensel's lemma μ_i is the unique root of f s.t.

$$|a - \mu_i| < |f'(\mu_i)| = 1$$

But $|\zeta - \mu_i| < 1$ because $\zeta - \mu_i \in \mathfrak{m}$

$$\Rightarrow \zeta = \mu_i$$

<u>Case 2</u> $m = np^k$; it is enough to consider the case $m = p$: $\zeta^{np^k} = (\zeta^{np^{k-1}})^p$

we prove that there are no p-th roots of unity.

We assume $\zeta^p = 1$

$\zeta^p \equiv \zeta \pmod m \Rightarrow \zeta \equiv 1 \pmod m$

Consider $f = X^p - 1$

$|f'(\zeta)| = |p\zeta^{p-1}| = 1/p$ (we use the normalized abs. val: $|x| = p^{-v_p(x)}$)

By Hensel's lemma ζ is unique root of f with $|a - \zeta| < |f'(\zeta)| = \frac{1}{p}$

We claim that $\zeta \equiv 1 \pmod{p^2}$

Then $|1 - \zeta| \leq 1/p^2 < 1/p \Rightarrow \zeta = 1$

Proof of claim: write $\zeta = 1 + px$ for some $x \in \mathbb{Z}_p$;

$1 = \zeta^p = (1+px) = 1 + p^2 x + \binom{p}{2}(px)^2 + \dots + (px)^p$

$\binom{p}{k}$ is divisible by p for $1 \leq k \leq p-1$

Since $p \geq 3$ $\quad 1 \equiv 1 + p^2 x \pmod{p^3}$

$\Rightarrow p^2 x \equiv 0 \pmod{p^3} \Rightarrow x = py$ for some $y \in \mathbb{Z}_p$

$\Rightarrow \zeta = 1 + p^2 y$ as claimed $\square$

Exercise: the only roots of unity in $\mathbb{Q}_2$ are ± 1