Hensel's lemma

HW 8 is posted. As usual, watch Zulip for corrections/clarifications/extra hints.

Also posted: notes on extension of valuations. These give a proof of the existence statement from the previous lecture using ideas from functional analysis, without separating the archimedean and nonarchimedean cases. (But I won't go over this approach in lecture.)

Reminder: extension of valuations

Let K be a field complete wrt an absolute value $|\cdot|_K$. Then for any finite extension L of K, there exists a unique extension of $|\ |_K$ to an absolute value on L.

And For all $\alpha \in L$, $|\alpha|_L = |\mathrm{Norm}_{L/K}(\alpha)|_K^{1/[L:K]}$

Last time i've showed the extension exists

- it is unique
- L is complete
- formula holds.

In nonarchimedean case, we need to prove: $|\alpha|_L \le 1 \Rightarrow |\alpha+1|_L \le 1$.

How this applies to number fields

let K be a number field

let $\mathfrak{p}$ be a prime of K, define $|\cdot|_{\mathfrak{p}} = c^{-v_{\mathfrak{p}}(\cdot)}$ for some $c > 1$

let $K_{\mathfrak{p}}$ be completion of K w.r.t. metric $|\cdot|_{\mathfrak{p}}$

let L/K be a finite extension. write $L = K(\alpha)$

$L \hookrightarrow LK_{\mathfrak{p}}$ i.e. $LK_{\mathfrak{p}} = K_{\mathfrak{p}}(\alpha)$

finite extension of $K_{\mathfrak{p}}$

So it has a <u>unique</u> extension of $|\ |_{\mathfrak{p}}$ which i. restrict to L.

Is this extension unique? <u>No</u>!

How this applies to number fields

$5\mathbb{Z}[i] = (2+i)(2-i)$

e.g. $K=\mathbb{Q}$, $\mathfrak{p}=(5)$ $L=\mathbb{Q}(i)$

$|\ |_5$ on $\mathbb{Q}$ extends to L two ways, as $|\ |_{2+i}$, $|\ |_{2-i}$

$(|2+i|_{2-i} = 1)$

point: $\mathbb{Q}_5 \cdot \mathbb{Q}(i) = \mathbb{Q}_5(i) \cong \mathbb{Q}_5$ because $\pm\sqrt{-1} \in \mathbb{Q}_5$

$$\mathbb{Q}(i) \otimes_{\mathbb{Q}} \mathbb{Q}_5 \cong \mathbb{Q}_5 \oplus \mathbb{Q}_5$$

$$i \longmapsto (\sqrt{-1}, -\sqrt{-1}).$$

(analogous to $K \to K_{\mathbb{R}} \cong K \otimes_{\mathbb{Q}} \mathbb{R}$)

in general, $\mathfrak{p} \subset O_K$, extensions of $|\ |_{\mathfrak{p}}$ to L are in 1-1 correspondence w/ primes of L above $\mathfrak{p}$

The missing step from last time

say $|\ |$ extends to L, $|\ |'$ for unk

nonarchimedean: $\mathfrak{p} = \{\alpha \in \mathcal{O}_L : |\alpha| < 1\}$

Let K be complete field for absolute value $|\cdot|_K$

Need to know: For $f(x) \in K(x)$ irreducible

$f(x) = a_n x^n + \dots + a_0$, we must have

$$\max\{|a_0|, \dots, |a_n|\} = \max\{|a_0|, |a_n|\}$$

(e.g. if $a_n = 1$, $|a_0| \leq 1$, then $|a_i| \leq 1$)

e.g.: $K = \mathbb{Q}_2$ $\quad x^2 + \frac{1}{2}x + 1$ is reducible.

Hensel's lemma: statement

K as above

$\mathcal{O}_K = \{\alpha \in K : |\alpha|_K \leq 1\}$ (is a subring)

$\mathfrak{p} = \{\alpha \in K : |\alpha|_K < 1\}$ (is a maximal ideal)

Let $f(x) \in \mathcal{O}_K[x]$ be a polynomial whose image $\bar{f}(x) \in (\mathcal{O}_K/\mathfrak{p})[x]$ is nonzero (i.e. f is primitive) (i.e. $f = a_0 + a_1 x \cdots + a_n x^n$ then $\max\{|a_i|\} = 1$)

and $\bar{f}(x)$ factors as $\bar{g}(x)\bar{h}(x)$ where $\bar{g}, \bar{h} \in (\mathcal{O}_K/\mathfrak{p})[x]$ are coprime. Then f factors as $g(x)h(x)$ where g reduces to $\bar{g}$, h reduces to $\bar{h}$ and $\deg(g) = \deg(\bar{g})$

Example: quadratic equations

For $p > 2$ odd prime,
if $a \in \mathbb{Z}_p$ is a nonzero square mod p,
then a is a square in $\mathbb{Z}_p$ mod p.

$$x^2 - a \equiv (x - \underbrace{r_1)(x - r_2}_{\text{coprime: self}}) \bmod p$$

Lift to Hensel to square roots in $\mathbb{Z}_p$.

For $p = 2$, you get a repeated root mod 2.

over $\mathbb{Q}_2$,

$$2(x^2 + \tfrac{1}{2}x + 1) = 2x^2 + x + 2$$

$$f(x) \in \mathbb{Z}_2(x)$$

$$\bar{f}(x) = x \cdot \underline{1}$$

Hensel $\Rightarrow$ $f(x) = g(x)h(x)$

$\deg(g) = 1$. $= (x + \sim)(2x + \sim)$

Example: roots of unity

θ prime

the polynomial $X^{p-1} - 1$ over $\mathbb{Z}_p$

factors completely as $\underbrace{(x-1)(x-2)\cdots(x-p+1)}_{\text{pairwise coprime}}$ mod p.

$\Rightarrow$ $\mathbb{Z}_p$ contains a full set of $(p-1)$st of unity.

in particular, $\mathbb{Q}_p(\zeta_{p-1}) = \mathbb{Q}_p$.

i.e. $\mathbb{Q}_5 \ni \zeta_4 = \sqrt{-1}$

$\Rightarrow$ the $(p-1)$st roots of unity in $\mathbb{Z}_p$, plus 0,

form an alternate set of digits (...)

Hensel's lemma: proof

$f(x) \in \mathcal{O}_K[x]$ $\quad \bar f = \bar g \bar h$ coprime.

Pick $g_0, h_0 \in \mathcal{O}_K[x]$ $\quad \bar g_0 = \bar g$, $\bar h_0 = \bar h$

Pick $a, b \in \mathcal{O}_K[x]$ s.t. $\bar a \bar g + \bar b \cdot \bar h = 1$

deg g_0 = deg $\bar g$

Then I can find $\pi \in \mathfrak{p}$ s.t. $f \equiv g_0 h_0 \bmod \pi$ and $a g_0 + b h_0 \equiv 1 \bmod \pi$

Want g_1, h_1 s.t. $g_1 \equiv g_0 \bmod \pi$ $\quad$ deg g_1 = deg $\bar g$,

$h_1 \equiv h_0 \bmod \pi$

and $f \equiv g_1 h_1 \pmod{\pi^2}$ $\quad$ (and then repeat)

candidate:

$g_1 = g_0 + p_1 \pi$ $\quad p_1, q_1 \in \mathcal{O}_K[x]$ $\quad g_1 h_1 \equiv g_0 h_0 + \underbrace{(g_0 q_1 + h_0 p_1)}\pi \bmod \pi^2$

$h_1 = h_0 + q_1 \pi$

$\stackrel{?}{\equiv} \left(\frac{f - g_0 h_0}{\pi}\right) \bmod \pi$

Use a, b to enforce this, i.e. $p_1 = b(\ldots) \bmod g_0$

From Hensel's lemma to the missing step

<u>Newton polygons</u>

to study factorizations in

$\mathbb{C}((x))$