Lecture 29: Hensel's Lemma; Primes and Places

Last time: **Lemma:** $f \in \mathbb{Z}[x]$. If a_1 is a simple root of f mod p, then $\exists\, a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv a_1 \bmod p$.

Hensel's Lemma: Suppose $f \in \mathbb{Z}_p[x]$ is monic. Let $\bar{f} \in \mathbb{F}_p[x]$ be its reduction mod p. If $\bar{f}$ factors into $g_0 h_0$ with g_0 and h_0 monic and rel prime (in $\mathbb{F}_p[x]$), then $\exists$ monic $g, h \in \mathbb{Z}_p$ with $f = gh$ and $\bar{g} = g_0$ and $\bar{h} = h_0$.

Moreover, g and h are unique and $(g, h) = \mathbb{Z}_p[x]$.

[Lemma from last time is special case of g_0 linear; will omit proof, which has a similar inductive approach.]

[Usefullness of $\mathbb{Z}_p$ in computations, e.g. factoring poly's]

[On to number fields...] $\underset{\uparrow \text{ global field}}{K}, \mathfrak{p} \rightsquigarrow K_{\mathfrak{p}}$ "local field"

Def: Two valuations $|\cdot|_1$ and $|\cdot|_2$ on K are *equivalent* if
① $|\,|_2 = |\,|_1^a$ for some $a > 0$.
② $|\alpha|_1 < 1 \Rightarrow |\alpha|_2 < 1$
③ They define the same topology on K

Lemma: These are equivalent cond.

K a number field.

<u>Place</u> or <u>Prime</u> of K: an equivalence class of valuations.

<u>Thm</u>: There is exactly one place of K for each

① real embedding $\tau: K \to \mathbb{R}$, namely $|k|_\tau = |\tau(k)|$.

② pair of complex emb $\sigma, \bar{\sigma}: K \to \mathbb{R}$, namely $|k| = |\sigma(k)|^2$.

③ prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$:

$$|k|_{\mathfrak{p}} = |N(\mathfrak{p})|^{-m} \quad \text{where } (k) = \mathfrak{p}^m \mathfrak{a} \text{ with}$$
$\mathfrak{a}$ coprime to $\mathfrak{p}$.

<u>Notes</u>: ①+② are the <u>infinite</u> <u>places</u> (or primes)
③ the <u>finite</u> <u>places</u>

In ② its not really a valuation, but just ignore it

<u>Product Formula</u>:
$$\prod_{v \text{ place of } K} |k|_v = 1 \quad \text{for any } k \neq 0 \text{ in } K.$$

<u>Ex</u>: $k = 6+6i$ in $\mathbb{Q}(i)$ $\quad k = (1+i)^3(3)$

primes

So

$$|k|_v = \begin{cases} 72 = 2^3 \cdot 3^2 & \text{if } v = \infty \\ 2^{-3} & \text{if } v = (1+i) \\ 3^{-2} & \text{if } v = (3) \\ 1 & \text{otherwise.} \end{cases}$$

For a place v, let K_v denote its completion w.r.t. $| \, |_v$. Equivalently:

ⓐ if v is an infinite place, $K_v = \mathbb{R}$ or $\mathbb{C}$

ⓑ if v is a finite place comming from $\mathfrak{p}$, then take

$$\mathcal{O}_v \doteq \varprojlim \mathcal{O}_K/\mathfrak{p}^n \quad \text{and} \quad K_v = \text{field of fractions of } \mathcal{O}_v$$

<u>Ex</u>: $K = \mathbb{Q}(i)$

$v = (3)$: On $\mathbb{Q}$ we have $|r|_v = \left(\frac{1}{9}\right)^m$ where $r = 3^m \frac{x}{y}$ with x, y coprime to 3.
This is equivalent to the usual 3-adic valuation. So
$\mathbb{Q}_3 \subseteq K_{(3)}$; in fact $K_{(3)} = \mathbb{Q}_3(i)$, i.e. a finite extention of $\mathbb{Q}_3$.
$\mathcal{O}_{(3)}$ like $\mathbb{Z}_3$ except $\mathcal{O}_{(3)}/\text{unique prime ideal} \cong \mathcal{O}_K/(3) \cong \mathbb{F}_9$.

$v = (2+i)$: In this case, $K_{(2+i)} \cong \mathbb{Q}_5$

Point: -1 is already a square in $\mathbb{Q}_5$ as $X^2+1 \equiv (X+2)(X+3) \bmod 5$.

[$v = (1+i)$: The tricky ramified case.
Have $K_{(1+i)} \neq \mathbb{Q}_2$ since $X^2+1 \equiv 0 \bmod 4$ has no solutions. However, $(2\mathbb{Z}_2) \cdot \mathcal{O}_2$ isn't prime.]

<u>Global field</u>: a number field K (or a finite extension of $\mathbb{F}_p(T)$).

<u>Local field</u>: K_v for some place v.

<u>Local-to-global principles</u>:

A <u>quadratic form</u> $q : K^n \to K$ is $q(x) = \langle x, x\rangle$ for some symmetric bilinear form
$$\langle\, ,\rangle : K^n \times K^n \to K.$$

[Note: q determines $\langle\, ,\rangle$ by $\frac{1}{2}\{q(x+y) - q(x) - q(y)\}$.]

<u>Thm</u>: q a quad. form on $\mathbb{Q}^n$. Then $\exists\, x \in \mathbb{Q}^n$ with $q(x) = 0$ iff $\forall p\ \exists\, x_p \in \mathbb{Q}_p^n$ with $q(x_p) = 0$.

["q reps 0 globally iff it does at every local place."]

<u>Why this is good</u>: Local fields are "large" so there are few distinct quadratic forms over them.

E.g. at the infinite place $\mathbb{R}$, any form is equal to one of the form $x_1^2 + \cdots + x_k^2 - (x_{k+1}^2 + \cdots + x_m^2)$