Return to setting of general field, K, and again use dichotomy of valuations – archimedean v. non-arch. – to study them.

If v with assoc. $|\cdot|_v$ is non-archimedean then by 3 axioms for non-arch. valuation

know $\quad \mathcal{O} = \{ x \in K \mid v(x) \geq 0 \} = \{ x \in K \mid |x|_v \leq 1 \}$

is subring of K with units

$\mathcal{O}^\times = \{ x \in K \mid |x|_v = 1 \}$ and unique maximal ideal $\mathfrak{p} = \{ x \in K \mid |x|_v < 1 \}$

(Moreover, $\mathcal{O}$ is integral domain (since K is) with field of fractions K)
where either $x \in K$ is in $\mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

"valuation ring"

<u>Fact</u>: $\mathcal{O}$ is integrally closed. (in $\mathrm{Frac}(\mathcal{O}) = K$) Thus if $K = \#$ field, then $\mathbb{Z} \subseteq \mathcal{O}_v$ so $\mathcal{O}_K \subseteq \mathcal{O}_v$
v: valuation (non-arch.)

<u>pf</u>: Any elt $x \in K$ integral (over $\mathcal{O}$) satisfies monic equation

$x^n + a_1 x^{n-1} + \dots + a_n = 0$ with $a_i \in \mathcal{O}$. Want to show $x \in \mathcal{O}$.

If not, then since $\mathcal{O}$ valuation ring, $x^{-1} \in \mathcal{O}$. But then

$$x = -a_1 - a_2 x^{-1} - \dots - a_n x^{-(n-1)} \in \mathcal{O}. \quad ↯.$$

<u>Examples</u>: $K = \mathbb{Q}$, $v \longleftrightarrow p$: prime. then $\mathcal{O}_v = \underbrace{\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \,\middle|\, p \nmid b \right\}}_{\text{localization at } p.}$

(similarly for # fields)

$K = \mathbb{Q}_p$, then $\mathcal{O} = \mathbb{Z}_p$.

Say that valuation is "discrete" if it admits smallest positive value m.

Then the set of all possible valuations is $m \cdot \mathbb{Z}$ for elts. of K.

Always find equivalent valuation with $m=1$. ("normalized" valuations)

Note that sets $\mathcal{O}, \mathcal{O}^\times, \mathfrak{p}$ are independent of representative in equivalence class.

Final Proposition: if v is discrete then valuation ring $\mathcal{O}_v$ is P.I.D.

(so $\mathcal{O}_v$ is discrete valuation ring) with $\mathfrak{p}^n/\mathfrak{p}^{n+1} \simeq \mathcal{O}_v/\mathfrak{p}$ $\forall n$.

Moreover the chain of ideals $\mathcal{O} \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \dots$ form a basis of open nbhds of 0 in K. $\left(\mathfrak{p}^n = \left\{ x \in K \;\middle|\; |x|_v < \frac{1}{q^{n-1}} \right\} \right.$ if $\left. |\cdot| = q^{-v_{\mathfrak{p}}(\cdot)} \right)$

Similarly, $1+\mathfrak{p}^n$ give base of nbhds of 1 in $\mathcal{O}^\times$.

Archimedean valuations: Given K: field, any valuation v, form completion $\hat{K}$.

if v: archimedean, not many choices for $\hat{K}$:

Theorem (Ostrowski) K: field, $\hat{K}$: completion w.r.t. archimedean v, then there is an isomorphism $\sigma: \hat{K} \longrightarrow \mathbb{R}$ or $\mathbb{C}$ such that $|a|_v = |\sigma(a)|_\infty^s$ with $s \in (0,1]$. ∞: arch. on $\mathbb{R}$ or on $\mathbb{C}$.

We may extend valuations to the completion just as for $\mathbb{Q}$, setting

$\hat{v}$ on $\hat{K}$ to be given by $\hat{v}(a) = \lim_{n\to\infty} v(a_n)$, if $a = \lim_{n\to\infty} a_n$

$a_n \in K$, $a \in \hat{K}$

"ultrametric" property $\Rightarrow$ $\hat{v}(a) = v(a_n)$ if $n \geq n_0$ some n_0.

Earlier we showed $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p / p\cdot\mathbb{Z}_p$ and $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p$ $n \geq 1$

and same proof works for general valuation rings $\mathcal{O} \subseteq \hat{\mathcal{O}}$: val. ring of $\hat{K}$

with $\mathfrak{p}, \hat{\mathfrak{p}}$ resp. maximal ideals.

<u>Proposition</u> : v : discrete valuation on K with valuation ring $\mathcal{O}$

$R \subseteq \mathcal{O}$: set of rep's for $\mathcal{O}/\mathfrak{p}$: residue field ($0 \in R$)

Then $x \in \hat{K}$ ($\neq 0$) has unique power series rep'n:

$$x = \pi^m \cdot (a_0 + a_1\pi + \cdots) \qquad a_i \in R,\ a_0 \neq 0,\ m \in \mathbb{Z}$$

(convergent power series as all formal power series are Cauchy in non-arch. case.)

<u>Example</u> : ① $K = \mathbb{Q}$, $\mathfrak{p}$ = max. ideal for $v_p = p\cdot\mathbb{Z}$, just get back usual

p-adic expansion in $\mathbb{Q}_p$: $x = p^m(a_0 + a_1 p + \cdots)$

② $K = \mathbb{F}_q(t)$ with $\mathcal{O} = \mathbb{F}_q[t]$ $\mathfrak{p} = (t-a)$ $a \in \mathbb{F}_q$

then $\hat{K}$: completion w.r.t. $(t-a)$ is "field of formal power series" $\mathbb{F}_q((t-a))$

consisting of formal Laurent series $f(t) = (t-a)^m(a_0 + a_1 t + \cdots)$

There is even analogous result saying

$$\mathcal{O} \simeq \varprojlim_n \mathcal{O}/\mathfrak{p}^n \qquad \text{(postpone for next time)}$$

Given a valuation over $\hat{K}$, want to explain how to extend it to algebraic extension $\hat{L} | \hat{K}$. Key tool: Hensel's Lemma.

A polynomial $f(x) = a_0 + \cdots + a_n x^n$ $a_i \in \mathcal{O}$: valuation ring of $K = \hat{K}$. is called "primitive" if $f \not\equiv 0 \pmod{\mathfrak{p}}$. In terms of valuation, we could say $|f| := \max\{|a_0|, |a_1|, \dots, |a_n|\} = 1$. (since $|a_i| \leq 1$ with $a_i \in \mathcal{O}$)

Hensel's Lemma: if f primitive with

$\bar{f} \equiv \bar{g} \cdot \bar{h} \pmod{\mathfrak{p}}$ $\bar{g}, \bar{h}$ rel. prime polys.

then $f = g \cdot h$ in $\mathcal{O}[x]$ where g, h polys with $\deg(g) = \deg(\bar{g})$, $\deg(h) = \deg(\bar{h})$ and $g \equiv \bar{g}$, $h \equiv \bar{h} \pmod{\mathfrak{p}}$

Usual version of Hensel's lemma:

if $f(a) \equiv 0 \bmod p$, $f'(a) \not\equiv 0 \bmod p$, $a \in \mathbb{Z}_p$, $f \in \mathbb{Z}_p[x]$

then $\exists$ $\alpha \in \mathbb{Z}_p$ with $f(\alpha) = 0$ and $\alpha \equiv a \pmod{p}$.

(idea: lift the solution to higher and higher powers of p, making formal series)

Example: $x^2 - 7$ in $\mathbb{Z}_3$. so 1 is sol'n in $\mathbb{Z}/3\mathbb{Z}$

How to lift it to sol'n mod 9? 1 in $\mathbb{Z}/9\mathbb{Z}$ not sol'n. Can lift to $(1+3k)$ $k = 0, 1, 2$.

e.g. $(1+3)$ is lift to sol'n of $x^2 - 7$ in $\mathbb{Z}/3^2\mathbb{Z}$ as $16 - 7 \equiv 0 \ (9)$.

General recipe for accomplishing lift is version of Newton's method.

Neukirch's version is slight generalization since, if $a \in \cancel{\ } \mathcal{O}$ has

$f(a) \equiv 0 \mod \wp$ then we may write $f(x) \equiv (x-a)\,h(x)$

and condition that a is simple root (i.e. $f'(a) \not\equiv 0 \mod \wp$) mod $\wp$

guarantees that $(x-a)$ and $h(x)$ are relatively prime. (mod $\wp$).

---

proof of Hensel's lemma: $d = \deg(f)$, $m = \deg(\bar{g})$ $\deg(\bar{h}) \leq d-m$

If $g_0, h_0 \in \mathcal{O}[x]$ are polynomials s.t. $g_0 \equiv \bar{g}$, $h_0 \equiv \bar{h}$ (mod $\wp$) of equal degrees

~~the~~ then since $\bar{g}, \bar{h}$ assumed relatively prime,

$\exists\ a(x), b(x) \in \mathcal{O}[x]$ with $a \cdot g_0 + b \cdot h_0 \equiv 1 \pmod{\wp}$

Consider coeffs. of $f - g_0 h_0$ and $a g_0 + b h_0 - 1 \in \wp[x]$

Take one with smallest valuation, ~~the~~ call it π. (if min val $= \infty$, we're done)

Try to find desired g, h among

$$g = g_0(x) + p_1(x)\cdot\pi + p_2(x)\pi^2$$
$$h = h_0(x) + q_1(x)\cdot\pi + q_2(x)\pi^2$$

with p_i in $\mathcal{O}[x]$, $\deg(p_i) < m$
q_i in $\mathcal{O}[x]$, $\deg(q_i) \leq d-m$.

so that setting $g_{n-1}(x) = g_0(x) + p_1(x)\pi + \cdots + p_{n-1}(x)\pi^{n-1}$, similarly for $h_{n-1}(x)$,

then $f \equiv g_{n-1} \cdot h_{n-1} \pmod{\pi^n}$ $(*)$

Then, if this can be arranged, in limit as $n \to \infty$, get $f = g \cdot h$ in $\mathcal{O}[x]$

(The ideal $(\pi^n) \subset \wp^n$, in particular, so $(*)$ implies $f \equiv g_{n-1} h_{n-1} \pmod{\wp^n}$)

Prove this for all n by induction.