Example *(cont'd)*: *Function fields* in one variable...

Practice: consider K a finite extension of $k = \mathbb{C}(X)$, and $\mathfrak{O}$ the integral closure in K of $\mathfrak{o} = \mathbb{C}[X]$.

$K = \mathbb{C}(X, Y)$ for some Y, and can renormalize so $Y \in \mathfrak{O}$, so $\mathbb{C}[X, Y] \subset \mathfrak{O}$.

For example, for *hyperelliptic curves* $Y^2 = P(X)$ with $P(X) \in \mathbb{C}[X]$ square-free, have $\mathfrak{O} = \mathbb{C}[X, Y]$ exactly.

Puiseux expansions and field extensions of $\mathbb{C}((X - z))$. Introduction to Newton polygons.

Hensel's lemma: With monic $F(T) \in \mathbb{C}[[X]][T]$, given $\alpha_1 \in \mathbb{C}[[X-z]]$ with $F(\alpha_1) = 0 \bmod X - z$, $F'(\alpha_1) \neq 0 \bmod X - z$, the recursion

$$\alpha_{n+1} \;=\; \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)} \bmod (X-z)^{n+1}$$

gives $\alpha_\infty = \lim_n \alpha_n \in \mathbb{C}[[X-z]]$ with $F(\alpha_\infty) = 0$ in $\mathbb{C}[[X-z]]$, and α_∞ is the *unique* solution congruent to $\alpha_1 \bmod X - z$.

Theorem: All finite field extensions of $\mathbb{C}((X - z))$ are by adjoining solutions to $Y^e = X - z$ for $e = 2, 3, 4, \ldots$. [Proof below.]

This approximates the assertion that, *locally*, Riemann surfaces are combinations of *coverings* of the z-plane and power maps $w^e = z$.

The proof invites extending Hensel's lemma to cover *factorization*.

Hensel's Lemma II: Let R be a UFD, and π a prime element in R. Given $a \in R$, suppose $b_1, c_1 \in R$ such that

$$a \;=\; b_1 \cdot c_1 \bmod \pi \qquad\qquad \textit{and} \qquad\qquad Rb_1 + Rc_1 + R\pi \;=\; R$$

Then there are b, c in the π-adic completion $R_\pi = \lim_n R/\pi^n$ such that $b = b_1 \bmod \pi$, $c = c_1 \bmod \pi$, and

$$a = b \cdot c \qquad\qquad (\text{in } \lim_n R/\pi^n = R_\pi)$$

Remark: Apply this to $R = \mathbb{C}[[X - z]][T]$ or $R = \mathbb{C}[X, T]$ and $\pi = X - z$ to talk about field extensions of $\mathbb{C}((X - z))$.

Proof: With $a = b_1 \cdot c_1 \bmod \pi$, try to adjust b_1, c_1 by multiples of π to make the equation hold mod π^2: require

$$a \;=\; \big(b_1 + x\pi\big) \cdot \big(c_1 + y\pi\big) \bmod \pi^2$$

Simplify: the π^2 term $\pi^2 xy$ disappears, and

$$\frac{a - b_1 c_1}{\pi} \;=\; xc_1 + yb_1 \bmod \pi$$

By hypothesis, expressions $xc_1 + yb_1 + z\pi$ with $x, y, z \in R$ give R, so there exist (non-unique!) x, y to make the equation hold.

Thus, the genuine induction step involves $a = b_n c_n \bmod \pi^n$, and trying to solve for x, y in

$$a \;=\; \big(b_n + x\pi^n\big)\cdot\big(c_n + y\pi^n\big) \mod \pi^{n+1}$$

which gives

$$\frac{a - b_n c_n}{\pi^n} \;=\; xc_n + yb_n \mod \pi$$

Inductively, $c_n = c_1 \bmod \pi$ and $b_n = b_1 \bmod \pi$, so

$$Rb_n + Rc_n + R\pi \;=\; Rc_1 + Rb_1 + R\pi \;=\; R$$

and there are x, y satisfying the condition. Induction succeeds.

///

Caution: By Gauss' lemma, *polynomial* rings $\mathfrak{o}[X]$ over UFDs $\mathfrak{o}$ are UFDs, but what about $\mathfrak{o}[[X]]$?

We don't really need the more general case, since we only care about $\mathbb{C}[[X]] = \lim_n \mathbb{C}[X]/X^n$, which is completely analogous to $\mathbb{Z}_p$, where we recall that the ideals in $\mathbb{Z}_p$ are just $p^\ell \cdot \mathbb{Z}_p$. Many fewer than in $\mathbb{Z}$, and all *coming from* $\mathbb{Z}$.

Thus, $\mathbb{C}[[X]]$ is a PID, with a unique non-zero prime ideal $X \cdot \mathbb{C}[[X]]$, and *all* ideals are of the form $X^n \cdot \mathbb{C}[[X]]$.

Even though $\mathfrak{o}[[X]]$ is much bigger than $\mathfrak{o}[X]$, it has many more *units*, for example.

At the same time, UFDs like $\mathbb{Z}[x, y]$ are not PIDs, so we have to be careful what we imagine...

Maybe proving $\mathbb{Z}[[X]]$ and $\mathbb{C}[[X]][T]$ are UFDs is a good exercise.

Corollary: (Now $z = 0$ and $X - z = X$.) Consider

$$f(X,T) = T^n + a_{n-1}(X)T^{n-1} + \ldots + a_1(X)T + a_o(X)$$

with $a_j(X) \in \mathbb{C}[[X]]$ and such that the equation

$$f(0,Y) \;=\; (Y - w_1)^{\nu_1}(Y - w_2)^{\nu_2} \ldots (Y - w_m)^{\nu_m}$$

with $w_i \neq w_j$ for $i \neq j$. Then $f(X,T)$ factors in $\mathbb{C}[[X]][T]$ into m monic-in-T factors, of degrees ν_j in T:

$$T^n + a_{n-1}(X)T^{n-1} + \ldots + a_o(X) \;=\; f_1(X,T) \ldots f_m(X,T)$$

with

$$f_j(0,T) \;=\; (T - w_j)^{\nu_j}$$

That is,

$$f_j(X,T) \;=\; (T - w_j)^{\nu_j} \mod X$$

Proof: In Hensel II, take $R = \mathbb{C}[[X]][T]$, $\pi = X$, and

$$b_1 \;=\; (T - w_1)^{\nu_1} \qquad\qquad c_1 \;=\; (T - w_2)^{\nu_2} \ldots (T - w_m)^{\nu_m}$$

An equality of polynomials $g(X) \;=\; h(X)$ mod X is equality of complex numbers $g(0) \;=\; h(0)$. Since w_1 is distinct from $w_2, \ldots, w_m$, there are r_1, r_2 in the PID $\mathbb{C}[T]$ such that $r_1 b_1 + r_2 c_1 = 1$, so certainly $Rb_1 + Rc_1 + R\pi = R$. By Hensel II,

$$f(X, T) \;=\; g(X, T) \;\cdot\; h(T, X) \qquad\qquad (\text{in } \mathbb{C}[[X]][T])$$

and

$$g(X, T) \;=\; (T - w_1)^{\nu_1} \mod X$$

$$h(X, T) \;=\; (T - w_2)^{\nu_2} \ldots (T - w_m)^{\nu_m} \mod X$$

Since $1 + c_1 X + \ldots \in \mathbb{C}[[X]]^\times$, we can make g, h *monic* in T. Induction on m. ///

Corollary: Unless $f(0,w) = 0$ has just a single (distinct) root in $\mathbb{C}$, $f(X,T)$ has a proper factor in $\mathbb{C}[[X]][T]$. ///

That is, over scalars $\mathbb{C}[[X]]$, the irreducible factors of $f(X,T)$ are (factors of) the groupings-by-*distinct*-factors mod X.

Now consider $w_1 = 0$, and $f(X,T) = T^n \bmod X$. That is, $f(X,T)$ is of the form

$$f(X,T) \;=\; T^n \;+\; X \cdot a_{n-1}(X) \cdot T^{n-1} \;+\; \ldots \;+\; X \cdot a_o(X)$$

In the simplest case $a_o(0) \neq 0$, Eisenstein's criterion in $\mathbb{C}[[X]][T]$ gives *irreducibility* of $f(X,T)$. Let's consider this case.

Extend $\mathbb{C}[[X]]$ by adjoining $X^{1/n}$. Replacing T by $X^{1/n} \cdot T$, the polynomial becomes

$$X \cdot T^n + X^{1+\frac{n-1}{n}} a_{n-1}(X) \cdot T^{n-1} + \ldots + X^{1+\frac{1}{n}} a_1(X) \cdot T + X a_o(X)$$

Taking out the common factor of X gives

$$T^n + (X^{1/n})^{n-1} a_{n-1}(X) \cdot T^{n-1} + \ldots + X^{1/n} a_1(X) \cdot T + a_o(X)$$

Mod $X^{1/n}$, this is

$$T^n + 0 + \ldots + 0 + a_o(0) = T^n + a_o(0) \mod X^{1/n}$$

For $a_o(0) \neq 0$, $w^n + a_o(0) = 0$ has *distinct* linear factors in $\mathbb{C}$. By the Hensel paraphrase, $f(X, X^{1/n}T)$ factors into linear factors in $\mathbb{C}[[X^{1/n}]][T]$. *We're done in this case:* the field extension is

$$\mathbb{C}((X))(Y) = \mathbb{C}((X^{1/n}))$$

Example: To warm up to Newton polygons and the general case, consider $(T - X^{1/3})^3(T - X^{1/2})^2$. Write $\mathrm{ord}(X^{a/b}) = a/b$. The symmetric functions of roots have ords

$$\begin{aligned}
\mathrm{ord}\,\sigma_1 &= \mathrm{ord}(3X^{1/3} + 2X^{1/2}) &&= \tfrac{1}{3} \\
\mathrm{ord}\,\sigma_2 &= \mathrm{ord}(3X^{\frac{1}{3}+\frac{1}{3}} + 6X^{\frac{1}{3}+\frac{1}{2}} + X^{\frac{1}{2}+\frac{1}{2}}) &&= \tfrac{2}{3} \\
\mathrm{ord}\,\sigma_3 &= \mathrm{ord}(X^{3\cdot\frac{1}{3}} + 6X^{2\cdot\frac{1}{3}+\frac{1}{2}} + 3X^{\frac{1}{3}+2\cdot\frac{1}{2}}) &&= 1 \\
\mathrm{ord}\,\sigma_4 &= \mathrm{ord}(2X^{3\cdot\frac{1}{3}+\frac{1}{2}} + 3X^{2\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) &&= \tfrac{3}{2} \\
\mathrm{ord}\,\sigma_5 &= \mathrm{ord}(X^{3\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) &&= 2
\end{aligned}$$

That is, the *increments* in $\mathrm{ord}\,\sigma_\ell$ are $\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{2}, \frac{1}{2}$.

Variant: Varying the example, take

$$f(X,T) \;=\; (T-z_1X^{\frac{1}{3}})(T-z_2X^{\frac{1}{3}}(T-z_3X^{\frac{1}{3}}(T-z_4X^{\frac{1}{2}})(T-z_5X^{\frac{1}{2}})$$

with non-zero $z_i \in \mathbb{C}$. Now we mostly have *inequalities* for ords:

$$\begin{array}{lcll}
\mathrm{ord}\,\sigma_1 &=& \mathrm{ord}((z_1+z_2+z_3)X^{1/3}+(z_4+z_5)X^{1/2}) & \geq \frac{1}{3} \\
\mathrm{ord}\,\sigma_2 &=& \mathrm{ord}((z_1z_2+\ldots)X^{\frac{1}{3}+\frac{1}{3}}+(\ldots)X^{\frac{1}{3}+\frac{1}{2}}+z_4z_5X^{\frac{1}{2}+\frac{1}{2}}) & \geq \frac{2}{3} \\
\mathrm{ord}\,\sigma_3 &=& \mathrm{ord}(z_1z_2z_3X^{3\cdot\frac{1}{3}}+(\ldots)X^{2\cdot\frac{1}{3}+\frac{1}{2}}+3X^{\frac{1}{3}+2\cdot\frac{1}{2}}) & = 1 \\
\mathrm{ord}\,\sigma_4 &=& \mathrm{ord}(z_1z_2z_3(z_4+z_5)X^{3\cdot\frac{1}{3}+\frac{1}{2}}+(\ldots)X^{2\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) & \geq \frac{3}{2} \\
\mathrm{ord}\,\sigma_5 &=& \mathrm{ord}(z_1z_2z_3z_4z_5X^{3\cdot\frac{1}{3}+2\cdot\frac{1}{2}}) & = 2
\end{array}$$

A stark example of the latter is

$$f(X,T) \ = \ T^5 - XT^2 + X^2$$

The crucial mechanism is that the *smallest* ord is 1/3, and replacing T by $X^{1/3} \cdot T$ will distinguish the two sizes of roots:

$$f(X, X^{1/3} \cdot T) \ = \ X^{\frac{5}{3}} T^5 - X^{\frac{5}{3}} T^2 + X^2$$

Dividing through by $X^{5/3}$ gives

$$T^5 - T^2 + X^{\frac{1}{3}}$$

Mod $X^{\frac{1}{3}}$, this has 3 *non-zero* factors, and 2 *zero* factors, so by Hensel II *factors properly* into cubic and quadratic.

More generally, consider

$$f(X,T) \;=\; (T-X^{1/e_1})^{\nu_1}\ldots(T-X^{1/e_m})^{\nu_m} \qquad \left(\text{with } \tfrac{1}{e_1}\le\ldots\le\tfrac{1}{e_m}\right)$$

By the ultrametric inequality,

$$\mathrm{ord}(\sigma_\ell)\;\ge\;\mathrm{ord}\Big(\text{sum of ords of the } \ell \text{ smallest-ord zeros}\Big)$$

$$\ge\;\begin{cases} \ell\cdot\frac{1}{e_1} & \text{for } 1\le\ell\le\nu_1 \\ \frac{\nu_1}{e_1}+(\ell-\nu_1)\cdot\frac{1}{e_2} & \text{for } \nu_1\le\ell\le\nu_1+\nu_2 \\ \frac{\nu_1}{e_1}+\frac{\nu_2}{e_2}+(\ell-\nu_1-\nu_2)\cdot\frac{1}{e_3} & \text{for } \nu_1+\nu_2\le\ell\le\nu_1+\nu_2+\nu_3 \\ \ldots & \ldots \end{cases}$$

with *equality* at $\ell=0,\nu_1,\nu_1+\nu_2,\ldots,\;\nu_1+\ldots+\nu_m$.

Since $\frac{1}{e_1} \leq \ldots \leq \frac{1}{e_m}$, the *convex hull* (downward) of the points $(\ell, \operatorname{ord}\sigma_\ell)$ has boundary the polygon of lines connecting the points in $\mathbb{R}^2$

$$(0,0)$$

$$(\nu_1, \tfrac{\nu_1}{e_1}) = (\nu_1, \operatorname{ord}\sigma_{\nu_1})$$

$$(\nu_1+\nu_2, \tfrac{\nu_1}{e_1}+\tfrac{\nu_2}{e_2}) = (\nu_1+\nu_2, \operatorname{ord}\sigma_{\nu_1+\nu_2})$$

$$\ldots$$

$$(\nu_1+\ldots+\nu_m, \tfrac{\nu_1}{e_1}+\ldots+\tfrac{\nu_m}{e_m}) = (\nu_1+\ldots+\nu_m, \operatorname{ord}\sigma_{\nu_1+\ldots\nu_m})$$

This convex hull is the *Newton polygon* of the polynomial. For $f(X,T) \in \mathbb{C}[[X]][T]$, the ords are in $\mathbb{Z}$. Eisenstein's criterion is the case $\nu_1 = n$, and $\operatorname{ord}\sigma_n = 1$, and all the exponents are $1/n$.

The general case was reduced to $f(X,T) = T^n + \ldots + a_o(X)$ with an n-fold multiple zero w_o at $X = 0$. Replacing T by $T + w_o$, without loss of generality, this root is 0, so $a_j(0) = 0$ for all j.

Replace T by $X^\rho \cdot T$ with ρ the *slope* of the first segment from $(0,0)$ to $(\ell, \mathrm{ord}\,\sigma_\ell)$ on the Newton polygon. That is, disregard any $(\ell', \mathrm{ord}\,\sigma_{\ell'})$ with $\ell' < \ell$ lying *above* that segment.

Replacing T by $X^\rho \cdot T$ and dividing through by $X^{n\rho}$ gives

$$T^n + \ldots + \frac{a_{n-\ell}(X)}{X^{\ell\rho}} \cdot T^{n-\ell} + \ldots$$

The Newton polygon says the *ord* of the coefficient of T^j for $n \geq j > n - \ell$ is *non-negative*, at $T^{n-\ell}$ the ord is 0, and for $n - \ell > j$ it is *strictly positive*.

That is, mod X,

$$f(0,T) = T^n + \ldots + \underbrace{b_{n-\ell}(0)}_{\text{non}-\text{zero}} \cdot T^{n-\ell}$$

Thus, $f(0,w) = 0$ has ℓ non-zero complex roots, and $n - \ell$ roots 0.

Hensel II says that there are degree ℓ factor and degree $n - \ell$ factors in $\mathbb{C}[[X^\rho]][T]$.

Note that $\mathbb{C}[[X^\rho]] \approx \mathbb{C}[[X]]$, so the argument can be repeated.

Induction on degree. ///