Last time

Thm Let K be complete w.r.t. a disc. val. v and let L be a field ext. of degree n. Then, there is exactly one disc. val. v' on L that extends v: $v'(x) = \frac{1}{n} v(Nm_{L/K}(x))$ for $x \in L$.
$\mathcal{O}_{v'} \subset L$ is the int. closure of $\mathcal{O}_v \subset K$.
L is complete w.r.t. v'.

Cor There is exactly one valuation v' on $\overline{K}$ extending v.
It is not discrete! The field $\overline{K}$ might not be complete w.r.t. v'! Still, $\mathcal{O}_{v'}$ is the int. closure and $\mathfrak{p}_{v'}$ is the only nonzero prime ideal in $\mathcal{O}_{v'}$.

Notation If K is complete w.r.t. a disc. val. v, we denote the corr. normalized valuation by v_K.
We $\mathcal{O}_K = \mathcal{O}_{v_K}$, $\mathfrak{p}_K = \mathfrak{p}_{v_K}$, $\pi_K = \pi_{v_K}$, ...
We also denote the ext. of v_K to $\overline{K}$ by v_K.

Cor If $f(x) \in K[x]$ is an irreducible pol. over a field K as above, then all roots of $f(x)$ in $\overline{K}$ have the same valuation, namely $\frac{1}{n} v(\text{const. coeff. of } f(x)) = \frac{1}{n} v(f(0))$.

Analogy If $f(x) \in \mathbb{R}[x]$ is an irreducible pol. ($\Rightarrow \deg = 1$ or 2), then all roots in $\mathbb{C}$ have the same abs. val. (complex conjugates if $\deg = 2$).

Def Let $L|K$ as above and $\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^e$.

The number $e(L|K) = e$ is the <u>ramification index</u> of $L|K$.

The number $f(L|K) = f = [\kappa_L : \kappa_K]$ is the <u>inertia degree</u> of $L|K$.

Rmk $e = [\underbrace{v_K(L^\times)}_{= \frac{1}{e}\mathbb{Z}} : \underbrace{v_K(K^\times)}_{= \mathbb{Z}}] = [\underbrace{v_L(L^\times)}_{= \mathbb{Z}} : \underbrace{v_L(K^\times)}_{= e\mathbb{Z}}]$.

Rmk $v_L(x) = e \cdot v_K(x) \; \forall x \in L$.

Rmk $v_K(\pi_L) = \frac{1}{e}$.

Rmk If $M|L|K$ are as above, then

$$e(M|K) = e(M|L)\, e(L|K)$$
$$f(M|K) = f(M|L) f(L|K).$$

Thm Let $L|K$ be an ext. of degree n as above.

$\Rightarrow n = e \cdot f$

Pf Follows from following thm! $\square$

Thm Let $\omega_1, \dots, \omega_f \in \mathcal{O}_L$ be so that $\omega_1 \bmod \mathfrak{p}_L, \dots, \omega_f \bmod \mathfrak{p}_L$ form a basis of $\kappa_L | \kappa_K$. Then, $(\omega_i \pi_L^j)_{\substack{1 \le i \le f \\ 0 \le j < e}}$ is a basis of $\mathcal{O}_L | \mathcal{O}_K$ (and therefore of $L|K$).

Pf Write $x = \sum a_{ij} \omega_i \pi_L^j$ for $a_{ij} \in K$.

$$\Rightarrow x \equiv \sum_i a_{i0} \omega_i \mod \pi_L .$$

$$(x \bmod \mathfrak{p}_L) = \sum_i (a_{i0} \bmod \mathfrak{p}_K) \cdot (\omega_i \bmod \mathfrak{p}_L)$$

in κ_L.

Since $\omega_1 \bmod \mathfrak{p}_L, \dots, \omega_f \bmod \mathfrak{p}_L$ form a basis of $\kappa_L | \kappa_K$, this uniquely determines $a_{i0} \bmod \mathfrak{p}_K \; \forall i$.

$$x \equiv \sum a_{i0} \omega_i + \sum a_{i1} \omega_i \pi_L \mod \mathfrak{p}_L^2$$

$$\frac{x - \sum (a_{i0} \bmod \mathfrak{p}_K) \omega_i}{\pi_L} \equiv \sum a_{i1} \omega_i \pi_L \mod \mathfrak{p}_L$$

This uniquely determines $a_{i1} \bmod \mathfrak{p}_K \; \forall i$.

$\vdots$

$a_{i,e-1} \bmod \mathfrak{p}_K \; \forall i$.

$a_{i0} \bmod \mathfrak{p}_K^2 \; \forall i$

$\vdots$

$\square$

Def $L|K$ is <u>unramified</u> if $e = 1$ $(\Leftrightarrow f = n)$.

$L|K$ is <u>totally ramified</u> if $e = n$ $(\Leftrightarrow f = 1)$.

Comparing the splitting behavior of a prime before and after completion

Thm Let $\mathcal{O}_K$ be a Dedekind dom. and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let $L|K$ be a separable field ext. of degree n and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with inertia degrees $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

$$\Rightarrow L \otimes \widehat{K}_{\mathfrak{p}} \cong \widehat{L}_{\mathfrak{P}_1} \times \dots \times \widehat{L}_{\mathfrak{P}_r}$$

completion w.r.t. $v_{\mathfrak{p}}$

completion of L w.r.t. $v_{\mathfrak{P}_i}$

$$\mathcal{O}_L \otimes \widehat{\mathcal{O}}_{\mathfrak{p}} \cong \widehat{\mathcal{O}}_{\mathfrak{P}_1} \times \dots \times \widehat{\mathcal{O}}_{\mathfrak{P}_r}$$

$$e_i = e(\widehat{L}_{\mathfrak{P}_i} | \widehat{K}_{\mathfrak{p}}),$$

$$\mathcal{O}_L/\mathfrak{P}_i \cong \widehat{\mathcal{O}}_{\mathfrak{P}_i}/\mathfrak{P}_i\widehat{\mathcal{O}}_{\mathfrak{P}_i},$$

$$f_i = f(\widehat{L}_{\mathfrak{P}_i} | \widehat{K}_{\mathfrak{p}}).$$

Sketch of pf

$$\hat{\mathcal{O}}_{\mathfrak{p}} = \varprojlim \mathcal{O}_K/\mathfrak{p}^n .$$

$$\Rightarrow \mathcal{O}_L \otimes \hat{\mathcal{O}}_{\mathfrak{p}} = \varprojlim \mathcal{O}_L/\mathfrak{p}^n\mathcal{O}_L$$

$\mathcal{O}_L|\mathcal{O}_K$ fin. gen. because $L|K$ is separable

$$= \varprojlim \mathcal{O}_L/(\mathfrak{p}\mathcal{O}_L)^n$$

$$= \varprojlim \mathcal{O}_L/(\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r})^n$$

$$\underset{CRT}{=} \prod_i \varprojlim \mathcal{O}_L/\mathfrak{P}_i^{e_i n}$$

$$= \prod_i \varprojlim \mathcal{O}_L/\mathfrak{P}_i^{n}$$

$$= \prod_i \hat{\mathcal{O}}_{\mathfrak{P}_i} .$$

$\square$

In terms of polynomials:

If $\mathfrak{p} \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ for some $\alpha \in \mathcal{O}_L$, then its min. pol. $f(X) \in \mathcal{O}_K[X]$ factors in $\hat{\mathcal{O}}_{\mathfrak{p}}[X]$ as

$$f(X) = f_1(X) \cdots f_r(X)$$

with $f_i(X) \in \hat{\mathcal{O}}_{\mathfrak{p}}[X]$ irred. of degree

$[\hat{L}_{\mathfrak{P}_i} : \hat{K}_{\mathfrak{p}}] = e_i f_i \quad (\hat{L}_{\mathfrak{P}_i} = \hat{K}_{\mathfrak{p}}[X]/f_i(X))$

and each $f_i(X)$ factors mod $\mathfrak{p}$ as

$f_i(X) = g_i(X)^{e_i}$ with $g_i(X) \in \kappa_{\mathfrak{p}}[X]$

irreducible of degree f_i $\quad (\kappa_{\mathfrak{P}_i} = \kappa_{\mathfrak{p}}[X]/g_i(X))$.

1.7. Newton polygons

Let K be a field with val. v.

<u>Thm</u> Let $r_1, \dots, r_n \in K^\times$ with $v(r_1) \leq \dots \leq v(r_n)$.

Then, the coeff. of $(X-r_1)\cdots(X-r_n) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ satisfy $v(a_{n-i}) \geq v(r_1) + \dots + v(r_i)$ for $i = 1, \dots, n$.

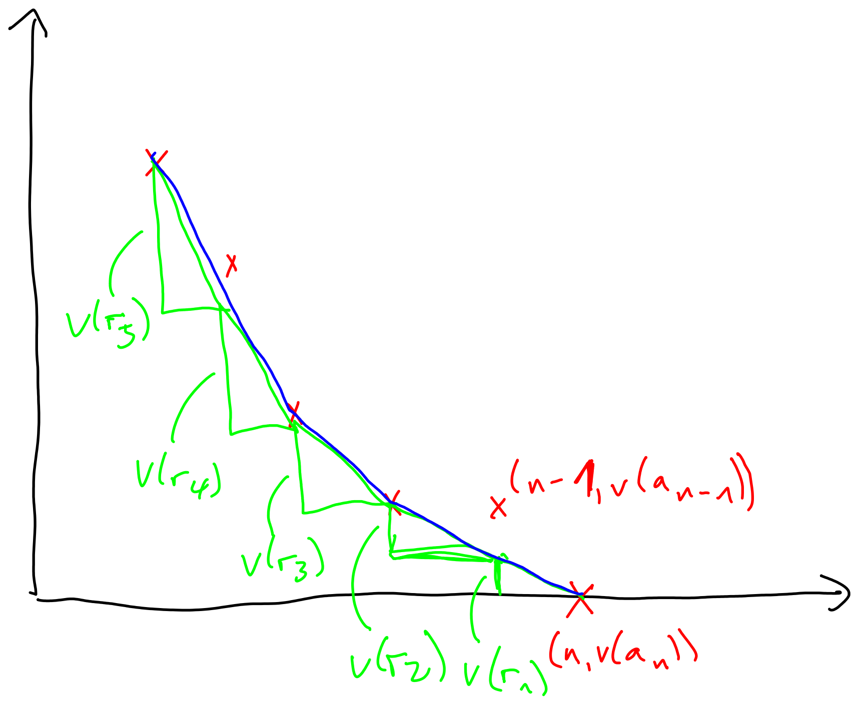
Equality holds (at least) if $v(r_i) < v(r_{i+1})$ or $i = n$.

<u>Pf</u> Expand the product $(X-r_1)\cdots(X-r_n)$.

$\rightsquigarrow$ $a_{n-i} = \pm$ the sum of all products of i of the numbers $r_1, \dots, r_n$.

Each prod. has val. $\geq v(r_1) + \dots + v(r_i)$.

This val. occurs in exactly one prod. if $v(r_i) < v(r_{i+1})$ or $i = n$. $\square$



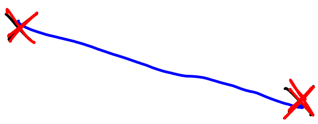
The points $(i, v(a_i))$ lie on or above this polygon.

There is a point at each corner of the polygon.

Def The <u>Newton polygon</u> of a pol. $f(x) = \sum_{i=0}^{n} a_i X^i$ (with $a_0, a_n \neq 0$) is the lower convex hull of the set of points $(i, v(a_i))$ $(i = 0, \dots, n)$.

Cor The val. of the roots of $f(x)$ in $\overline{K}$ are minus the slopes of the Newton polygon. (Width of line segment = number of roots with the corr. valuation).

Cor 1 If $f(x) \in K[X]$ is irreducible, its Newton polygon is just a single line segment.



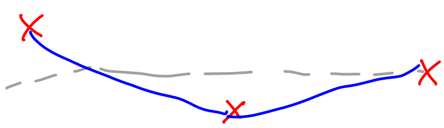
Pf All roots have the same valuation. $\square$

Rmk More generally, $f(x)$ has at least one irreducible factor per line segment.

Cor of Cor 1 The stupid lemma:

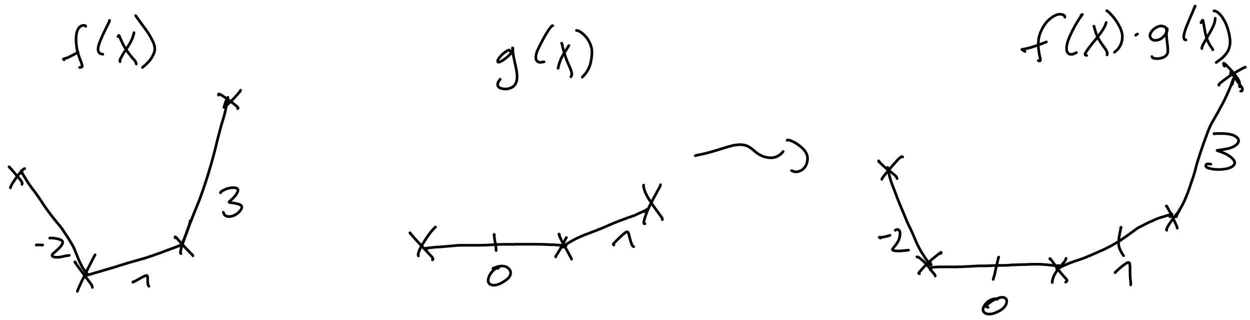
If $f(X)$ is irred., then $v(a_i) \geq \min(v(a_0), v(a_n))$ $\forall i$

Pf

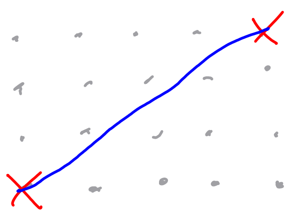


(not a single line segment) $\square$

Cor 2 To find the Newton polygon of $f(X)\cdot g(X)$, glue the Newton pol. of $f(X)$, $g(X)$ together and sort the line segments. (Move up/down to make $v(a_0)$ correct.)

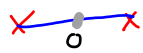


Cor of Cor 2 If $v = v_u$ is normalized and the Newton polygon is a line segment which contains no integer points except its endpoints, then $f(X)$ is irreducible.



Pf Can't have been glued together from two polygons whose corners lie at integer points. □

Warning Converse is false! (E.g. $X^2-2 \in \mathbb{Q}_3[X]$ is irred. (no roots mod 3))



Cor of Cor of Cor 2 (Eisenstein criterion)

If it is the line segment $[(0,1),(n,0)]$, then $f(X)$ is irred.

$\Updownarrow$

$$\boxed{v(a_0)=1,\ v(a_1),\dots,v(a_{n-1})\geq 1,\ v(a_n)=0.}$$