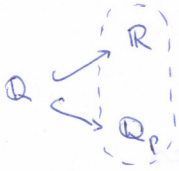
Local fields

→ introduce a metric on $\mathbb{Q}$, $d(x,y) = |x-y|$, complete $\mathbb{Q}$ under $|\cdot|$

p a prime, $x = p^n \cdot \frac{a}{b}$, $(a,b)=1$, $n \in \mathbb{Z}$ ⇒ $|x|_p := p^{-n}$ p-adic abs. value

This defines $d_p(x,y) := |x-y|_p$ a metric (easy), $\mathbb{Q}_p$ the completion of $\mathbb{Q}$.



local fields (there are way more than these though)

Field extensions of $\mathbb{Q}_p$?

Note: $\mathbb{Q}$ has inf. way, e.g. $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$ etc.

On the contrary, a loc. field usually has only a few:

Field	# quadratic ext.	# degree 3 Gal. ext.
$\mathbb{Q}_2$	7	1
$\mathbb{Q}_3$	3	4
$\mathbb{Q}_5$	3	1
$\mathbb{Q}_7$	3	4
$\mathbb{R}$	1	0

see database of local fields

Galois theory: everything is coded in $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$,

finite, order n quotients of the group ⟷ degree n Galois ext. $L/\mathbb{Q}_p$

Local class field theory

F finite extn of the local fields discussed so far,

then there is a canonical iso of top. groups

$$\widehat{F^\times} \xrightarrow{\sim} \mathrm{Gal}(\overline{F}/F)_{ab}$$

(profinite completion) (maximal ab. quotient)

Experiments with this claim:

1) $F = \mathbb{R}$, $\mathbb{R}^\times = \mathbb{R}\setminus\{0\} \cong C_2 \times \mathbb{R}$ since $x = \pm e^y$ with $y \in \mathbb{R}$

2) $F = \mathbb{C}$, $\mathbb{C}^\times \cong S^1 \times \mathbb{R}_{>0} \cong S^1 \times \mathbb{R}$

3) $F = \mathbb{Q}_p$, $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \underbrace{\mathbb{F}_p^\times}_{C_{p-1}} \times (\mathbb{Z}_p\text{-module})$

this yields the above statement about # quadr. extn

$$\widehat{\mathbb{Q}_p^\times} \cong \widehat{\mathbb{Z}} \times \mathbb{F}_p^\times \times (\mathbb{Z}_p\text{-module})$$

4) $F = \mathbb{F}_p$, $\mathbb{F}_p^\times \cong C_{p-1}$, $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \hat{\mathbb{Z}}$ $\longrightarrow$ completely hopeless

5) F = number field, $\mathbb{Q}^\times \cong C_2 \times \bigoplus_p \mathbb{Z}$, but sadly, this is much too small $\longrightarrow$ global class field theory. (We won't do this.)

Examples. $\mathbb{Q}_5$ has 3 quad. extensions (as claimed previously)

$F := \mathbb{Q}_5(\sqrt{6})$ $\longrightarrow$ this "should" give us a quad-extension of $\mathbb{Q}_5$.

Note that in this case, non-trivial extn $\Leftrightarrow$ quad. extn.

$$(1+x)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} x^n, \qquad \binom{\alpha}{n} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}$$ Taylor series

$$\sqrt{6} = \sqrt{1+5} = \sum_{n\geq 0} \binom{1/2}{n} 5^n$$ note that $|5|_5 = 1/5 < 1$, so we indeed have convergence in 5-adic topology

$\Rightarrow \mathbb{Q}_5(\sqrt{6}) = \mathbb{Q}_5$, although to actually prove this, we need the following Lemma. $\left|\binom{1/2}{n}\right|_5 \leq 1$.

PROOF: (unnecessarily fancy)

$$\begin{array}{ccc} \mathbb{Q} & \xrightarrow{\text{dense}} & \mathbb{Q}_5 \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathbb{Z}_5 \end{array}$$

and $\frac{1}{2} \in \mathbb{Z}_5$ since we have

$$\frac{1}{2} = 2 \cdot \frac{1}{4} = -2 \cdot \frac{1}{1-5} = -2 \sum_{n\geq 0} 5^n .$$

$\Rightarrow \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ is a polynomial in x, hence a cont. function

$\Rightarrow \binom{1/2}{n} = \lim_{\alpha \to 1/2} \binom{\alpha}{n}$. Let the sequence of alphas converging to $1/2$ be the partial sums of $-2\sum 5^n$, there are integers $\Rightarrow \binom{\alpha}{n}$ integer, $|\cdot| \leq 1$. □

Outlook (things to do after this course)

1) Langlands program $\rightsquigarrow$ fruitful for PhD

Local CFT: $\hat{F}^\times \xrightarrow{\cong} \mathrm{Gal}(\overline{F}/F)^{ab}$

$? \longrightarrow \mathrm{Gal}(\overline{F}/F)$

Note: the abs Galois group depends on the choice of $\overline{F}$

Langlands: replace the formulation by:

repn of $GL_n(F)$ repn of $\mathrm{Gal}(\overline{F}/F)$

Local Langlands: fully known, beautiful proof by Scholze

LCFT, lecture 1–2

Literature (for the course)

- Serre: Local fields
- Fesenko – Vostokov: Local fields and their extensions (Beware, weird notation for residue fields)
- Milne: ANT, Ch 7+, CFT
- ?: Local fields and class fields (quite recent)
- Gras: CFT from theory to practice (good for reference, not so good for studying from it)

---

2) Higher local fields → most already proven

$\left.\begin{matrix} \mathbb{D}_p((t_2))\dots((t_n)) \\ \mathbb{F}_p((t_1))\dots((t_n)) \end{matrix}\right\}$ n-local fields with last residue field $\mathbb{F}_p$

1-loc fields: the ones we considered above

0-loc fields: finite fields

Local CFT: $K_n^M(F) \longrightarrow \mathrm{Gal}(\overline{F}/F)^{ab}$

where $K_n^M(F) = \dfrac{\text{tensor algebra over } F^\times}{\text{Steinberg rel. } \langle x \otimes (1-x)\rangle \text{ for } x \neq 0,1}$

e.g. $K_1^M(F) = F^\times$, $K_0^M(F) = \mathbb{Z}$

Rmk. Slogan: local CFT can be phrased in a way that it looks like Poincaré duality.

Galois cohomology (spec. case of étale coh.)

Perfect pairing $H^p(F, \mathbb{Z}_\ell(1)) \otimes H^{2-p}(F, \mathbb{Z}_\ell) \longrightarrow H^2(F, \mathbb{Z}_\ell(1))$

→ looks like PD for a 2-dim oriented cpt. mf.

$p=1 \rightsquigarrow H^1(F, \mathbb{Z}_\ell(1)) \cong H^1(F, \mathbb{Z}_\ell)^\vee \cong H_1(F, \mathbb{Z})$

Hurewicz: $\pi_1(X) \longrightarrow H_1(X) = \pi_1(X)/[\pi_1(X), \pi_1(X)]$

Can be seen: $H^1(F, \mathbb{Z}_\ell(1)) \cong F^\times$, so we get back to the statement from before.

1. Basic theory

11.10.2018

Def K a field. An **abs. value** is a function $\|\cdot\| : K \to \mathbb{R}_{\geq 0}$ s.t.

(1) $\|x\| = 0$ iff $x = 0$

(2) $\|x \cdot y\| = \|x\| \cdot \|y\|$

(3) $\|x + y\| \leq \|x\| + \|y\|$

Def A **valued field** is a pair $(K, \|\cdot\|)$ where $\|\cdot\|$ is an abs. val. on K.

Ex $\mathbb{R}$ with the usual abs. value

$\mathbb{C}$ " " " " "

K any field with the trivial abs. value, i.e. $\|x\| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$

Tacit understanding: every valued field is a metric space with $d(x,y) := \|x - y\|$.

Def K field, $\|\cdot\|_1, \|\cdot\|_2$ abs. values are **equivalent** if they induce the same topology on K.

Prop $\|\cdot\|_1, \|\cdot\|_2$ abs. values on K, assume $\|\cdot\|_1$ is nontrivial. TFAE:

(1) $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent

(2) $\forall x \in K : \|x\|_1 < 1 \Rightarrow \|x\|_2 < 1$

(3) $\exists a > 0 \ \forall x \in K : \|x\|_2 = \|x\|_1^a$

Pf: As usual.

(1) $\Rightarrow$ (2): if $\|x\|_1 < 1$ then $\|x^n\|_1 = \|x\|_1^n \to 0 \Rightarrow x^n \xrightarrow{1} 0 \Rightarrow x^n \xrightarrow{2} 0 \Rightarrow \|x\|_2 < 1$

(2) $\Rightarrow$ (3): $\exists y \in K$ with $\|y\|_1 > 1$. $a := \dfrac{\log \|y\|_2}{\log \|y\|_1}$, this is well-def'd

Let $x \in K^\times \Rightarrow \exists b \in \mathbb{R}$, $\|x\|_1 = \|y\|_1^b$. Remains to show $\|x\|_2 = \|y\|_2^b$, from which we get $\|x\|_1^a = \|x\|_2$.

Pick $\frac{m}{n} \in \mathbb{Q}$ with $n > 0$, $\frac{m}{n} > b$. $\Rightarrow \|x\|_1 = \|y\|_1^b < \|y\|_1^{m/n} \Rightarrow \left\|\frac{x^n}{y^m}\right\|_1 < 1$

$\overset{2)}{\Rightarrow} \left\|\frac{x^n}{y^m}\right\|_2 < 1 \Rightarrow \|x\|_2 < \|y\|_2^{m/n}$. Do the same for $\frac{m}{n} < b$, get $\|x\|_2 > \|y\|_2^{m/n}$

(3) $\Rightarrow$ (1): easy, look at balls (they form a topology base) □

Okay, I've realised I don't like the norm notation after all. Switching over to $|\cdot|$.

Exc K valued field $\Rightarrow$ its metric completion $\tilde{K}$ is a valued field, extends $|\cdot|$.

Cor If $|\cdot|_1, |\cdot|_2$ are equivalent $\Rightarrow$ the completions wrt. them are canonically isomorphic. □

Pf: Balls form a topology base.

Def $|\cdot|$ is **non-archimedean** if $|x + y| \leq \max(|x|, |y|) \quad \forall x, y \in K$.

Otherwise $|\cdot|$ is **archimedean**.

Ex. $\mathbb{R}$ and $\mathbb{C}$ with the std. abs. value: archimedean.

Intermezzo on weird things

Prop. K non-arch valued field, $x \in K$, $r \in \mathbb{R}_{>0}$. Let $z \in B(x,r) \Rightarrow B(x,r) = B(z,r)$.
That is, every point of an open ball is a center of it.

Pf: $y \in B(z,r)$. $\Rightarrow$ $|x-y| = |x-z+z-y| \leq \max(\underbrace{|x-z|}_{<r}, \underbrace{|z-y|}_{<r}) < r \Rightarrow B(z,r) \subseteq B(x,r)$ Symetry.

Cor. All closed balls (of positive radius) in a non-arch valued field are open.

Pf: Same.

Prop. K non-arch valued field.

1) $(x_n)_n$ a sequence in K. If $(x_n - x_{n-1})_n \to 0$ then $(x_n)_n$ is Cauchy.
2) If K is complete as a metric space then if $(x_n - x_{n-1})_n \to 0$ then $(x_n)_n$ converges.
3) If $(x_n)_n \to 0$ then $\sum x_n$ is convergent. when K is complete.

Pf: 1) Pick $\varepsilon > 0$ and N s.t. $|x_n - x_{n-1}| < \varepsilon \quad \forall n \geq N$.

$$\forall m > n: |x_m - x_n| = |x_m - x_{m-1} + x_{m-1} - \dots - x_{n+1} + x_{n+1} - x_n| < \max_{i=n+1,\dots,m} |x_i - x_{i-1}| < \varepsilon$$

2) Cauchy sequences converge in complete spaces.

3) Partial sums are Cauchy.

Def. K non-arch valued field. $\mathcal{O}_K := \{x \in K \mid |x| \leq 1\}$ valuation ring of K.

Note. By convention, a ring is understood to be commutative and unital, ring homomorphism preserve 1.

Prop. 1) $\mathcal{O}_K$ is an open subring of K.

2) $\forall r \in (0,1]$: $\{x \in K \mid |x| < r\}$ and $\{x \in K \mid |x| \leq r\}$ are open ideals of $\mathcal{O}_K$.

3) $\mathcal{O}_K^\times = \{x \in K \mid |x| = 1\}$

Pf: Open balls are open, so are closed balls $\Rightarrow$ all the openness statements

1) $|1| = |1 \cdot 1| \Rightarrow |1| = 1$ since $1 \neq 0$. $|+1| = |-1|^2 \Rightarrow |-1| = 1$.

$x, y \in \mathcal{O}_K \Rightarrow |x+y| \leq \max(|x|, |y|) \leq 1$

$|x \cdot y| = |x| \cdot |y| \leq 1$.

$\Rightarrow \mathcal{O}_K$ is a ring.

2) Same.

3) If $x \in \mathcal{O}_K^\times \Rightarrow \underbrace{|x|}_{\leq 1} \cdot \underbrace{|x^{-1}|}_{\leq 1} = 1$ & $|x^{-1}| = \frac{1}{|x|}$ $\Rightarrow |x| = 1$. Converse: same.

2. Stuff about rings

Def. $R \subseteq S$ rings, $s \in S$. Then s is integral over R if there is a monic $f \in R[x]$ s.t. $f(s) = 0$.

Ex. $\forall r \in R$ is integral over R with $f(x) = x - r$.

Def $A = (a_{ij})$ an $n \times n$-matrix, $\forall a_{ij} \in R$. Then the adjugate / adjoint matrix is

$A^* = (A^*_{ij})$ where $A^*_{ij} = (-1)^{i+j} \det(A_{ji})$,

A_{ij} denotes the matrix obtained from A by deleting the i^{th} row, j^{th} column.

Prop. $AA^* = A^*A = \det(A) \cdot I$

PF: Linear algebra. □

Thm. $R \subseteq S$ rings, $s_1, \dots, s_n \in S$. TFAE:

(1) $\forall s_i$ is integral over R.

(2) The R-algebra $R[s_1, \dots, s_n] \subseteq S$ is finitely generated as an R-module.

PF: (1) $\Rightarrow$ (2): $R \subseteq R[s_1] \subseteq \dots \subseteq R[s_1, \dots, s_{n-1}] \subseteq R[s_1, \dots, s_n]$, reduce the proof to $n = 1$.

$R[s] = R\langle 1, s, s^2, \dots, s^k \rangle$ for some k since s was assumed to be integral.

($R[s]$: as a module; $1, s, s^2, \dots, s^k$: module generators)

(2) $\Rightarrow$ (1): Since we know that $R[s_1, \dots, s_n]$ is finge as an R-mod, we have generators $t_1, \dots, t_d$, i.e. $R[s_1, \dots, s_n] = R\langle t_1, \dots, t_d \rangle$

Let $b \in R[s_1, \dots, s_n]$ be arbitrary.

$\forall i$: $b \cdot t_i = \sum_j a_{ij} t_j$ $\rightsquigarrow$ $A := (a_{ij})$, $t := (t_1, \dots, t_d)^T$ $\Rightarrow (b \cdot I - A)\, t = 0$

$\Rightarrow \det(bI - A) \cdot t_j = 0 \quad \forall j$

Write $1 \in R$ as $1 = \sum_j c_j t_j$, $c_j \in R$.

$$\det(bI - A) \cdot 1 = \det(bI - A) \sum_j c_j t_j = \sum_j c_j \underbrace{\det(bI - A)\, t_j}_{0} = 0$$

Expanding det by Leibniz gives a monic polynomial in b. □

Cor. $R \subseteq S$ rings. If $s_1, s_2 \in S$ are integral over R then so are $s_1 + s_2$, $s_1 \cdot s_2$. 16.10.2018

In particular, the set $\tilde{R}$ of integral elts of S is a ring, called the integral closure of R in S.

PF: s_1, s_2 integral $\Rightarrow$ $R[s_1, s_2]$ fin. gen. /R

$s_1 \cdot s_2,\ s_1 + s_2 \in R[s_1, s_2] \Rightarrow R[s_1 \cdot s_2],\ R[s_1 + s_2] \subseteq R[s_1, s_2]$ subrings,

they are f.g. over R $\Rightarrow$ integrality. (by Thm. / Thm.) □

Def. $R \subseteq S$ ring ext. R is <u>integrally closed</u> in S if $\tilde{R} = R$.

Note: the notation $\tilde{R}$ suppresses the important data S.

The p-adic numbers

p prime number, fixed

$x \in \mathbb{Q}^\times$, $x = p^u \cdot \frac{a}{b}$, $a, b \in \mathbb{Z}$, a, b, p pairwise coprime $\longrightarrow$ unique (up to sign

Def. $|x|_p = \begin{cases} 0 & x = 0 \\ p^{-u} & x \neq 0 \end{cases}$ <u>p-adic absolute value.</u>

Prop. $|\cdot|_p$ is an absolute value on $\mathbb{Q}$, non-archimedean.

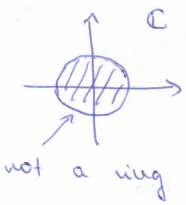
Pf: As usual.

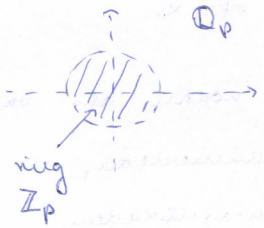
Def. The <u>p-adic numbers</u> $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ wrt. $|\cdot|_p$.

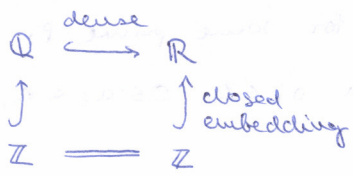
Thus $\mathbb{Q}_p$ is a complete non-archimedean valued field.

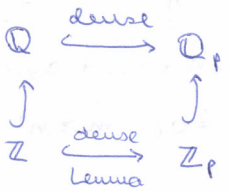
$\mathcal{O}_{\mathbb{Q}_p} = \{ x \in \mathbb{Q}_p \mid |x| \leq 1 \} =: \mathbb{Z}_p$, ring of <u>p-adic integers</u>

Rmk. Analogies:









Lemma. $\mathbb{Z}_p = \mathcal{O}_{\mathbb{Q}_p}$ agrees with the top. closure of $\mathbb{Z}$ inside $\mathbb{Q}_p$

Pf: $x \in \mathbb{Z}$, $x \neq 0 \Rightarrow x = p^u \cdot b$, $(b, p) = 1$, $u \geq 0 \Rightarrow |x|_p = p^{-u} \leq 1 \Rightarrow \mathbb{Z} \subseteq \mathbb{Z}_p$

$\mathbb{Z}_{(p)} := \{ x \in \mathbb{Q} \mid |x|_p \leq 1 \}$ is dense inside $\mathbb{Z}_p \Rightarrow$ sts $\mathbb{Z}_{(p)} \supseteq \mathbb{Z}$ dense

Let $x \in \mathbb{Z}_{(p)} \setminus \{0\}$ be given, $x = p^u \cdot \frac{a}{b}$, a, b, p pw. coprime, $u \geq 0$

Want: a sequence $x_i \longrightarrow x$, $\forall x_i \in \mathbb{Z}$.

$(p, b) = 1 \Rightarrow$ find $x_i, y_i \in \mathbb{Z}$ s.t. $b x_i + p^i y_i = 1 \quad \forall i$

$\Rightarrow \left| x_i - \frac{1}{b} \right|_p = \left| \frac{1}{b} \right|_p \cdot |b x_i - 1|_p = |p^i y_i|_p \leq p^{-i}$ since $y_i \in \mathbb{Z}$. Then (x_i) is as desired.

Cor. The nonzero ideals of $\mathbb{Z}_p$ are $p^n \mathbb{Z}_p$ for $n \geq 0$. Moreover, $\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z} / p^n \mathbb{Z}$.

Pf: Let $(0) \neq I \subseteq \mathbb{Z}_p$ be an ideal. Pick $x \in I$, $|x|_p$ is maximal among the elts of I.

Such an x exists. If $y \in I$ is arbitrary: $|y|_p \leq |x|_p \Leftrightarrow |y x^{-1}|_p \leq 1 \Leftrightarrow y x^{-1} \in \mathbb{Z}_p$

$\Rightarrow y = (y x^{-1}) \cdot x \in \mathbb{Z}_p \cdot (x) \Rightarrow I \subseteq \mathbb{Z}_p \cdot (x) \subseteq \mathbb{Z}_p \cdot I \Rightarrow I = x \mathbb{Z}_p$. **Cor.** $\mathbb{Z}_p$ is a PID.

Now, if $x = p^n \cdot u$ for some $|u|=1$, i.e. $u \in \mathbb{Z}_p^\times$. $\Rightarrow x\mathbb{Z}_p = p^n \underbrace{u\mathbb{Z}_p}_{\mathbb{Z}_p} = p^n\mathbb{Z}_p$, as claimed.

Next, consider $f_n : \mathbb{Z} \hookrightarrow \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$

$\ker f_n = \{x \in \mathbb{Z} \mid |x|_p \le p^{-n}\} = p^n\mathbb{Z}$

We get $\tilde{f}_n : \mathbb{Z}/p^n\mathbb{Z} \hookrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$. Remains to show: f_n surjective.

Known: $\mathbb{Z} \subseteq \mathbb{Z}_p$ dense. Claim. $\mathbb{Z}_p/p^n\mathbb{Z}_p$ has the discrete topology.

$\mathbb{Z}_p/p^n\mathbb{Z}_p$ carries the subset topology. The preimg of $z \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ is $\tilde{z} + p^n\mathbb{Z}_p$ where $\tilde{z}$ is any lift.

$\mathbb{Z}_p \xrightarrow{+\tilde{z}} \mathbb{Z}_p$ is a homeo. $\Rightarrow \tilde{z} + p^n\mathbb{Z}_p$ is an open ball

$\Rightarrow \forall \{z\}$ is open $\Rightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ carries the discrete topology, proving the Claim.

Claim. f_n surjective.

Pf: $x \in \mathbb{Z}_p$ arbitrary. Pick $x_i \longrightarrow x$, $\forall x_i \in \mathbb{Z}$. Since $\mathbb{Z}_p/p^n\mathbb{Z}_p$ has the discrete topology, $\overline{x_i} \in \mathbb{Z}_p/p^n\mathbb{Z}_p$ is eventually constant. The constant term $x_N \in \mathbb{Z}$ is a preimage of x. □

Thm. (Ostrowski) $|\cdot|$ nontriv abs value on $\mathbb{Q}$. Then

1) if $|\cdot|$ is archimedean, it is equivalent to $|\cdot|_\infty$
2) if $|\cdot|$ is non-archimedean, " $|\cdot|_p$ for some prime p.

Pf: Let $m, n \in \mathbb{Z}_{>0}$. Write $m = a_0 + a_1 n + \dots + a_r n^r$ with $a_i \in \mathbb{Z}$, $0 \le a_i < n$, i.e. take the n-adic expansion, $a_r \neq 0$, $m \ge n^r$

Let $N := \max\{1, |n|\}$.

By the ordinary triangle inequality: $|m| \le \sum_{i=0}^{r} |a_i| |n|^i \le \sum_{i=0}^{r} |a_i| N^r$

$$\left.\begin{array}{l} m \ge n^r \Rightarrow r \le \dfrac{\log m}{\log n} \\ |a_i| = |\underbrace{1 + \dots + 1}_{a_i < n \text{ times}}| \le a_i \cdot |1| = a_i < n \end{array}\right\} \Rightarrow |m| \le (1+r)\cdot n \cdot N^r \le \left(1 + \frac{\log m}{\log n}\right) n \cdot N^{\frac{\log m}{\log n}}$$

Do this for m^t in place of m, $t \in \mathbb{Z}_{>0}$

$\rightsquigarrow |m^t| \le \left(1 + \dfrac{t \log m}{\log n}\right) n N^{\frac{t \log m}{\log n}} \Rightarrow |m| \le \left(1 + \dfrac{t \log m}{\log n}\right)^{\frac{1}{t}} \sqrt[t]{n}\; N^{\frac{\log m}{\log n}}$

Take $t \longrightarrow +\infty$. $\Rightarrow |m| \le N^{\log m / \log n}$

Case 1: $|\cdot|$ is archimedean.

If $n > 1 \Rightarrow |n| > 1 \Rightarrow N = |n|$. $\Rightarrow |m|^{\frac{1}{\log m}} \le |n|^{\frac{1}{\log n}}$. Symmetry $\Rightarrow$ equality.

$|n|^{\frac{1}{\log n}} = C$ constant. $\Rightarrow |n| = C^{\log n} = n^{\log C}$ $\forall |n| > 1$

Now consider $\mathbb{Q}^\times$ as a group, $\mathbb{Q}^\times \cong \{\pm 1\} \times \bigoplus_p \mathbb{Z}$

-1, primes generate $\mathbb{Q}^\times$ in Ab $\Rightarrow$ $|\cdot|$ is equivalent to $|\cdot|_\infty$ by prev. argument.

18.10.20

Case 2: $\exists n \in \mathbb{Z}_{>1}$ s.t. $|n| \leq 1$.

Get $N=1$ for this n. $\Rightarrow |m| \leq 1 \ \forall m \in \mathbb{Z}$ $\Rightarrow |\cdot|$ is non-archimedean.

Thus we have a valuation ring $\mathcal{O}$ with max. ideal $\mathfrak{m} = \{x \in \mathcal{O} \mid |x| < 1\}$:

we have already seen that it is an ideal, and $\mathcal{O} \setminus \mathfrak{m} = \mathcal{O}^\times$ $\Rightarrow$ maximality.

$\Rightarrow \mathfrak{m}$ is prime, and so is $\mathfrak{m} \cap \mathbb{Z}$. Not the zero ideal, then $|\cdot|$ would be trivial on $\mathbb{Z}$ and hence on $\mathbb{Q}$, but that was excluded.

$\Rightarrow \mathfrak{m} \cap \mathbb{Z} = (p)$ $\Rightarrow \forall p \nmid m$: $|m| = 1$,

$$|n p^r| = |n| \cdot |p|^r = 1 \cdot |p|^r \quad \text{for } p \mid n.$$

Choose a s.t. $|p| = \left(\frac{1}{p}\right)^a$ $\Rightarrow$ $|\cdot| = |\cdot|_p^a$

Remark*. There is a more general version:

Thm: $K/\mathbb{Q}$ number field, $|\cdot|$ nontrivial abs. val. on K. Then

1) if $|\cdot|$ is non-archimedean then $\exists \mathfrak{p} \subseteq \mathcal{O}_K$ prime s.t. $|\cdot|$ is equivalent to the abs. value def'd by $|x|_{\mathfrak{p}} := \left(\frac{1}{\# \mathcal{O}_K/\mathfrak{p}}\right)^{\mathrm{ord}_{\mathfrak{p}}(x)}$

2) if $|\cdot|$ is archimedean, it is equivalent to $|x|_\sigma := |\sigma(x)|_{\mathbb{C}}$ for some embedding $\sigma: K \hookrightarrow \mathbb{C}$.

Some more language

Def. K field. A valuation: $v: K \to \mathbb{R} \cup \{\infty\}$ with

(1) $v(x) = \infty \iff x = 0$

(2) $v(xy) = v(x) + v(y)$

(3) $v(x+y) \geq \min\left(v(x), v(y)\right)$. Tacit convention

Correspondence b/w valuations and abs. values:

given v, let $|x|_v := \begin{cases} e^{-v(x)} & v(x) \neq \infty \\ 0 & v(x) = \infty \end{cases}$ $\rightarrow$ this is non-arch.

given $|\cdot|$ non-arch, let $v(x) := \begin{cases} \infty & x = 0 \\ -\log|x| & x \neq 0 \end{cases}$ $\rightarrow$ valuation.

"So this is obviously a complete waste of time."

Ex. k a field, $k((T)) := \left\{ \sum_{i=\nu \in \mathbb{Z}}^{\infty} a_i T^i \;\middle|\; a_i \in k \right\}$ field of (formal) Laurent series

$k((T)) = \mathrm{Frac}\, k[\![T]\!]$.

Given $f \in k((T))$, let $v(f) := \begin{cases} \min\{ i \in \mathbb{Z} \mid a_i \neq 0 \} & \text{if this exists} \\ \infty & \text{otherwise} \end{cases}$

Exc.: $k((T))$ is a non-archimedean valued field, $\mathcal{O}_{k((T))} = k[\![T]\!]$, $\mathcal{O}_K/\mathfrak{m} \cong k$.

Def. (K, v) valued field. K is <u>discretely valued</u> if $v(K^\times) \subseteq \mathbb{R}$ is a discrete subgp.

The <u>normalised valuation</u> is the unique choice (within the equivalence class of absolute values) s.t. $v(K^\times) = \mathbb{Z}$.

Def. K discretely valued field with normalised valuation v. Then any $\pi \in K$ s.t. $v(\pi) = 1$ is a <u>uniformiser</u> (local uniformising parameter).

Ex. Let's unravel this for $\mathbb{Q}_p$.

Valuation: $v(x) = -\log |x|_p = -\log |p^n \cdot \underbrace{u}_{u \in \mathbb{Z}_p^\times}|_p = -\log |p|_p^n = -(-n)\cdot \log p = n \log p \qquad (x \neq 0)$

$\Rightarrow v(\mathbb{Q}_p^\times) = \mathbb{Z} \log p \quad \Rightarrow \mathbb{Q}_p$ is discretely valued.

Normalised valuation: $v_p(x) = \frac{1}{\log p} \cdot v(x)$

Those who still feel uncomfortable with these notions should feel free (or rather: encouraged) to do the same for $k((T))$.

Lemma. K discretely valued field.

1) $\mathfrak{m} = \{ x \in \mathcal{O} \mid |x| < 1 \} = \{ x \in \mathcal{O} \mid v(x) > 0 \}$ is a principal ideal generated by any uniformiser.
2) $\pi \in \mathcal{O}$ uniformiser $\Leftrightarrow (\pi) = \mathfrak{m}$
3) Nonzero ideals of $\mathcal{O}$ are of the form $\pi^n \mathcal{O}$, $n \geq 1$.

PF: Same as for $\mathbb{Z}_p$. □

Hensel's Lemma. K discretely valued <u>complete</u> field, $f \in \mathcal{O}[x]$, $\overline{f}$ its image in $\mathcal{O}/\mathfrak{m}[x]$.

Suppose $f = \varphi_1 \cdot \varphi_2 \mod (\pi)$, $\varphi_1, \varphi_2 \in \mathcal{O}/\mathfrak{m}[x]$, coprime.

Then $\exists f_1, f_2 \in \mathcal{O}[x]$ s.t. $f = f_1 \cdot f_2$, $\deg f_1 = \deg \varphi_1$, $\overline{f_1} = \varphi_1$, $\overline{f_2} = \varphi_2$.

In words: coprime factorisation mod $\mathfrak{m}$ can be lifted to a factorisation in $\mathcal{O}$.

PF: We find $f_1^{(n)}, f_2^{(n)} \in \mathcal{O}[x]$ s.t.

(1) $f \equiv f_1^{(n)} f_2^{(n)} \ (\pi^n)$, $\quad f_1^{(n+1)} - f_1^{(n)} \equiv 0 \ (\pi^n)$, $\quad f_2^{(n+1)} - f_2^{(n)} \equiv 0 \ (\pi^n)$

(2) $\deg f_1^{(n)} = \deg \varphi_1$

(3) $\overline{f_1^{(n)}} = \varphi_1$, $\overline{f_2^{(n)}} = \varphi_2$

(4) $\deg f_2^{(n)} \leq \deg f - \deg \varphi_2$.

If these $f_1^{(n)}, f_2^{(n)}$ can indeed be constructed, define $f_i := \lim_{n\to\infty} f_i^{(n)}$.

Since K is assumed to be complete, the limits exist, and have the desired properties, by the properties of $f_i^{(n)}$.

We begin with $n=1$. Just pick any lifts of the correct degree. ✓

For $n \geq 2$: induction:

$f_i^{(n+1)} := f_i^{(n)} + \pi^n g_i$ for $g_i \in \mathcal{O}[x]$ to be chosen appropriately.

$f = f_1^{(n)} \cdot f_2^{(n)} + \pi^n \cdot h^{(n)}$ for some $h^{(n)} \in \mathcal{O}[x]$

$$f_1^{(n+1)} \cdot f_2^{(n+1)} = \left(f_1^{(n)} + \pi^n g_1\right)\left(f_2^{(n)} + \pi^n g_2\right)$$

$$= f_1^{(n)} f_2^{(n)} + \pi^n \left(f_1^{(n)} g_2 + f_2^{(n)} g_1\right) + \pi^{2n}(\dots)$$

Modulo π^{n+1} this yields the condition

$$f \equiv \underbrace{f_1^{(n)} f_2^{(n)}}_{f - \pi^n h^{(n)}} + \pi^n \left(f_1^{(n)} g_2 + f_2^{(n)} g_1\right) \pmod{\pi^{n+1}}$$

$$\Leftrightarrow 0 \equiv \left(-h^{(n)} + f_1^{(n)} g_2 + f_2^{(n)} g_1\right) \cdot \pi^n \pmod{\pi^{n+1}}$$

$$\Leftrightarrow 0 \equiv -h^{(n)} + f_1^{(n)} g_2 + f_2^{(n)} g_1 \pmod{\pi}$$

$$\Leftrightarrow h^{(n)} \equiv \varphi_1 g_2 + \varphi_2 g_1 \pmod{\pi}$$

Since φ_1 and φ_2 are coprime in $\mathcal{O}/\mathfrak{m}[x]$, such g_1 and g_2 exist.

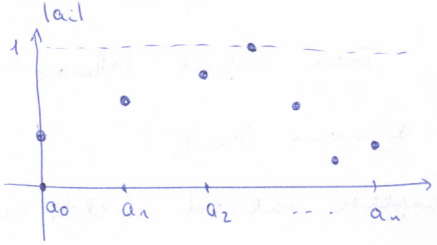
Even more, they can be obtained by the Euclidean algorithm ($\mathcal{O}/\mathfrak{m}$ is a field, $\mathcal{O}/\mathfrak{m}[x]$ is a Euclidean domain), which gives precisely the bounds we need for the degree. The other conditions are easily seen to be met.

23.10.20

Def. $f = a_n x^n + \dots + a_0 \in K[x]$ is <u>primitive</u> if $\max(|a_i|) = 1$.

Rmk. Primitive $\Rightarrow \in \mathcal{O}[x]$ by def.

Cor. Suppose K is a complete discrete valued field, and $f = a_n x^n + \dots + a_0 \in K[x]$, then if f is irreducible then $|a_i| \leq \max(|a_0|, |a_n|)$ $\forall i = 0, \dots, n$. $a_n, a_0 \neq 0$



Pf: Wlog: f is primitive. Then the claim reduces to showing $\max(|a_0|, |a_n|) = 1$.

↯ $\exists\, 0 < r < n$ minimal, $|a_r| = 1$.

$\bar{f} := x^r \cdot (a_r + a_{r+1} x + \dots + a_n x^{n-r}) \bmod \mathfrak{m}$

This is a factorisation into coprime factors since the 2nd term does not vanish for $x = 0$ by $|a_r| = 1$. HL ⇒ lift, f is not irr'ble. ↯

Cor. Let $f \in \mathcal{O}[x]$ be monic and K complete. If f has a simple root $\alpha \bmod m$ then f itself has a simple root a s.t. $a \equiv \alpha \bmod m$.

Pf: $f \equiv (x-\alpha)\cdot g \bmod m$, $g \in \mathcal{O}[x]$.

Apply HL with $\varphi_1 = x-\alpha$, $\varphi_2 = g$. □

Thm. K complete discrete valued field. Let L/K be a finite field extension. Then there is a unique extension to an absolute value on L, and concretely

$$|x|_L = \sqrt[n]{|N_{L/K}(x)|_K} \quad \text{where } n = [L:K].$$

Moreover, L is complete wrt. $|\cdot|_L$. □

Cor There is also a unique extension to all algebraic extensions of K.

Pf: $L := \bigcup \{\tilde{L} \mid [\tilde{L}:K] < \infty\}$ □

Cor. K complete discrete val. field, L/K finite, $\sigma \in \mathrm{Aut}(L/K) \Rightarrow |\sigma(x)|_L = |x|_L$.

Pf: $x \mapsto |\sigma(x)|_L$ is an abs value, agrees with $|\cdot|_L$ on K $\Rightarrow$ they agree on L by uniqueness. □

Def. K non-arch val field, V a K-vector space. A <u>non-arch norm</u> on V is a function $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ s.t.

(1) $\|x\| = 0$ iff $x = 0$

(2) $\|\lambda x\| = |\lambda| \cdot \|x\|$ $\forall \lambda \in K$ $\forall x \in V$

(3) $\|x+y\| \leq \max(\|x\|, \|y\|)$ $\forall x, y \in V$.

Def. $\|\cdot\|_A$, $\|\cdot\|_B$ are <u>equivalent</u> if $\exists C, D > 0$: $C\|x\|_A \leq \|x\|_B \leq D\|x\|_A$. $\forall x \in V$.

Exc. If $\|\cdot\|_A \sim \|\cdot\|_B$, defining $d_A(x,y) := \|x-y\|_A$ and d_B induces equivalent topologies on V. The converse is not true for norms (but it is for abs values, as we have already seen.)

Ex. Suppose K is complete val. field, V/K fin. dim. K-vector space, $x_1, \dots, x_n \in V$ a basis. Then define $\|x\|_{\max} := \max |a_i|$ where $x = \sum_{i=1}^{n} a_i x_i$, $a_i \in K$.

This is a norm (exc.).

Prop. K complete valued field, non-arch, and V/K a fin. K-space. Then V is complete as a metric space under $\|\cdot\|_{\max}$.

Pf: $(a_n)_n$ Cauchy wrt $\|\cdot\|_{\max}$ $\Leftrightarrow$ Cauchy in the coordinates (for a fixed basis)

Prop. K complete non-arch valued field, V/K fin dim space. Then any norm $\|\cdot\|$ on V is equivalent to the max-norm.

PF OF THM: Step 1. L is complete.

If $|\cdot|_L$ is an abs val in L, it is also a norm when viewed as a fin dim K-space. By the Prop.: equivalent to $\|\cdot\|_{max}$. Since L is complete wrt $\|\cdot\|_{max}$, it is also complete wrt. $|\cdot|_L$. ✓

Step 2. Uniqueness.

$|\cdot|_L$, $|\cdot|_L'$ extensions of $|\cdot|_K$. Then both define a norm. By the Prop., they are equivalent as norms. $\Rightarrow$ The associated metrics induce the same topology. We have already seen that two absolute values inducing the same topology are equivalent, i.e. $\exists b \in \mathbb{R}: \forall x \in L \; |x|_L = (|x|_L')^b$

This also holds for $x \in K \subseteq L \Rightarrow b = 1$. ✓

Here we used the assumption that $\exists x$ for which $|x| \neq 0, 1$. However, the Thm. also holds for trivial abs. value. (exc.)

Step 3. Existence.

WTS $|x|_L := \sqrt[n]{|N_{L/K}(x)|_K}$ defines an abs. value.

(1) $|x|_L = 0 \iff x = 0$ ✓

(2) Multiplicativity by multiplicativity of $N_{L/K}$, $|\cdot|_K$ and $\sqrt[n]{\cdot}$.

(3) Triangle inequality.

Claim. Sts $|x|_L \leq 1 \iff |x+1|_L \leq 1$.

PF: $x, y \neq 0$, $|x| \leq |y| \iff \left|\frac{x}{y}\right|_L \leq 1 \Rightarrow \left|\frac{x}{y} + 1\right|_L \leq 1 \Rightarrow |x+y|_L \leq |y|_L$

Let $\mathcal{O} := \{\alpha \in L \mid N_{L/K}(\alpha) \leq 1\}$. (This will coincide with $\mathcal{O}_L$ once we prove that $|\cdot|_L$ is an abs value.)

Claim. $\mathcal{O}$ is the int. closure of $\mathcal{O}_K$ in L.

PF: $\alpha \in \mathcal{O}_L$. Suppose $\alpha \neq 0$, min. poly. $f = a_0 + \dots + a_{m-1}x^{m-1} + x^m \in K[x]$

Nts: $a_i \in \mathcal{O}_K \; \forall i \iff |a_i|_K \leq 1 \; \forall i$

For a_0: $N_{L/K}(\alpha) = \pm a_0^k$ for some $k \in \mathbb{Z}_{\geq 1}$ ✓

First Cor. to HL $\Rightarrow |a_i| \leq \max(\underbrace{|a_0|}_{1}, |1|) = 1 \Rightarrow$ for $i \geq 1$ ✓

Conversely, suppose α to be integral $/\mathcal{O}_K$. Let $\bar{K}/K$ be an alg. closure.

Then $N_{L/K}(\alpha) = \left(\prod_{\sigma: K \hookrightarrow \bar{K}} \sigma(\alpha)\right)^k$. Since α is integral, so are all the $\sigma(\alpha)$.

$\Rightarrow N_{L/K}(\alpha)$ is also integral $/\mathcal{O}_K$. Since $\mathcal{O}_K$ is int. closed, $N_{L/K}(\alpha) \in \mathcal{O}_K$

$\Rightarrow |N_{L/K}(\alpha)| \leq 1$.

Note: what we did with $N_{L/K}$ holds only for separable extensions.

The triangle inequality follows. □

25.10.2018

Complete DVRs

Def. Complete DVR: • R integral domain,

• $\exists x \in R$: $R/(x)$ is a field and R is x-complete, i.e. $R \simeq \varprojlim_n R/(x^n)$

(called the residue field)

Rmk. Fix $\alpha \in (0,1)$, $d(a,b) := \alpha^{-v_x(a-b)}$. Then R is x-complete iff (R,d) is a complete metric space.

Motivation. Fix a field k. What are the DVRs with residue field k?

Ex. $k = \mathbb{F}_p$ is the residue field of $\mathbb{F}_p[\![T]\!] \neq \mathbb{Z}_p$

Def. k a field, $\operatorname{char} k = p$. Then k is perfect if the p-Frobenius $x \mapsto x^p$ is bijective.

Rmk. For most of what is done with perfect fields, the field hypothesis plays no role, and most stuff could be done for rings too.

Thm. (Teichmüller lifts) Let R be a ring, $R/(x)$ perfect ring of char k, R is x-complete. Then $\exists!\, \sigma: R/(x) \longrightarrow R$ for which $\sigma(a) \equiv a \pmod{x}$

and $\sigma(a^p) = \sigma(a)^p$.

Moreover, even the more general $\sigma(ab) = \sigma(a)\sigma(b)$ holds, i.e. σ is multiplicative, and if $\operatorname{char} R = p$ then $\sigma(a+b) = \sigma(a) + \sigma(b)$, i.e. σ is additive.

Lemma. A a ring, $b \in A$, $\operatorname{char} A/(b) = p$. If $x \equiv y \pmod b \Rightarrow x^p \equiv y^p \pmod{b^2}$

Pf: $x^p - y^p = \underbrace{(x-y)}_{\equiv 0\,(b)} \cdot \underbrace{\left(x^{p-1} + x^{p-2}y + \dots + y^{p-1}\right)}_{\equiv x^{p-1} + \dots + x^{p-1}\,(b) \equiv p x^{p-1}\,(b)}$

Divisibility by p $\Rightarrow$ divisibility by b. □

Note that in the p-adic topology, $x \mapsto x^p$ is a contraction: intuitively speaking, if two elements are close, their p^{th} powers are even closer.

Recall the **Banach fixed point theorem**: M complete metric space, $f: M \longrightarrow M$ a contraction, that is, $d(f(x), f(y)) \leq C\, d(x,y)$ for some $0 < C < 1$.

Then f has a unique fixed point.

Pf of Thm: $M := \{\sigma: R/x \longrightarrow R \text{ sections}\}$, $d(\sigma,\tau) := \sup\left\{ d_{x\text{-adic}}\left(\sigma(a), \tau(a)\right) \,\middle|\, a \in R/x \right\}$ metric on M

This turns M into a complete metric space, using x-completeness of R.

Define $f: M \longrightarrow M$, $f(\sigma)(a) = \sigma(a^{1/p})^p$ ($a^{1/p}$ is valid since R is perfect)

This $f(\sigma)$ is indeed a section: $\sigma(a^{1/p}) \equiv a^{1/p}\,(x) \Rightarrow \sigma(a^{1/p})^p \equiv (a^{1/p})^p\,(x)$

Wts f is a contraction.

$$d(f(\sigma), f(\tau)) = \sup\left\{ d_x\big(f(\sigma)(a), f(\tau)(a)\big) \;\middle|\; a \in R/(x) \right\}$$

$$= \sup\left\{ d_x\left(\sigma(a^{1/p})^p, \tau(a^{1/p})^p\right) \;\middle|\; a \in R/(x) \right\}$$

$$\leq \sup\left\{ \alpha \cdot d_x\left(\sigma(a^{1/p}), \tau(a^{1/p})\right) \;\middle|\; a \in R/(x) \right\}$$

Lemma $\Rightarrow d_x(u^p, v^p) \leq \alpha \cdot d_x(u,v) \quad \forall u,v \in R$ where $\alpha \in (0,1)$ is the number defining the x-adic topology

Banach $\Rightarrow \exists!\ \sigma \in M$ fixed pt, which satisfies the Thm.

Construction: $\forall n \geq 1$ take an arbitrary lift x_n of a^{1/p^n}. Then $\sigma(a) = \lim_{n\to\infty} (x_n)^{p^n}$

Multiplicativity: (x_n) reps for a, (y_n) reps for b $\Rightarrow (x_n y_n)$ for ab

Additivity when $\operatorname{char} R = p$: $x \mapsto x^p$ is additive.

Application. R complete DVR with perfect residue field k of char p. Then if $\operatorname{char} R = p$ then $R \simeq k[\![T]\!]$.

PO: This is true more generally when R is equicharacteristic but not necessarily perfect, but that's harder (Cohen's structure thm.) ($\operatorname{char} R = \operatorname{char} k$.)

PF: Choose $x \in R$ uniformiser.

Recall that $R = \{a_0 + a_1 x + a_2 x^2 + \dots\}$ where a_i lie in an arbitrarily chosen set of lifts of all elements of R/x

Consider $k[\![T]\!] \longrightarrow R$

$$\sum_{n\geq 0} c_n T^n \longmapsto \underbrace{\sum_{n\geq 0} \sigma(c_n) x^n}_{\in R \text{ convergent since } |\sigma(c_n)x^n| \to 0}$$

where $\sigma : R/(x) \longrightarrow R$ is the Teichmüller lift

This is a ring homomorphism because σ is.

To see bijectivity, we need that every element $r \in R$ can be written uniquely as $\sum_{n\geq 0} \sigma(c_n) x^n$.

Uniqueness: suppose $0 = \sum_{n\geq 0} \sigma(c_n) x^n$. ↯ not all $c_n = 0$. $\Rightarrow \exists\, i$ minimal, $c_i \neq 0$.

$\Rightarrow \sigma(c_i)$ is a unit $\Rightarrow \sum \sigma(c_n) x^n = x^N \cdot (\text{unit}) \neq 0$. ↯

Existence: $c_0 :=$ img of r in R/x

c_1: consider $\frac{r - c_0}{x}$, repeat the previous step.

And so on...

30.10.2018

Prop. L/K purely inseparable, K non-arch val fd. $\Rightarrow$ $\exists!$ extension of $|\cdot|$ to L.

PF: Given $x \in L$, $x \neq 0$ $\exists p^m$: $x^{p^m} =: a \in K$.

Suppose we also have $x^{p^n} =: b \in K$. Wlog $m > n$

$$\Rightarrow \left(x^{p^n}\right)^{p^{m-n}} = b^{p^{m-n}} = a^{p^{m-n}} \quad \to \quad p^{m-n} \cdot v(b) = v(a) \quad \Rightarrow \quad \frac{v(b)}{p^n} = \frac{v(a)}{p^m}$$

Define $\tilde{v}$ on L as follows: $\tilde{v}(0) = \infty$, $\tilde{v}(x) := \frac{v(a)}{p^m}$ for any $a \in K$, $m \geq 0$ when $x^{p^m} = a$.

Now if $x^{p^m} = a$, $y^{p^n} = b$; $m < n$: $(xy)^{p^n} = a^{p^{n-m}} \cdot b \in K$. $\Rightarrow$

$$\Rightarrow \tilde{v}(xy) = \frac{1}{p^n} v\left(a^{p^{n-m}} \cdot b\right) = \frac{1}{p^m} v(a) + \frac{1}{p^n} v(b) = \tilde{v}(a) + \tilde{v}(b)$$

For the triangle inequality, do a similar computation. $\Rightarrow$ $\tilde{v}$ is a valuation. $\square$

Ex. $\mathbb{F}_p((t))$ discretely valued non-arch val field, $v(f)$ = order of vanishing at $t=0$

$\mathbb{F}_p((t^{1/p}))\,/\,\mathbb{F}_p((t))$ is purely inseparable ext

$$K_n := \mathbb{F}_p\left(\left(t^{1/p^n}\right)\right) \quad \to \quad v(K_0^\times) = \mathbb{Z}, \; \tilde{v}(K_1^\times) = \frac{1}{p}\mathbb{Z}, \; \tilde{\tilde{v}}(K_2^\times) = \frac{1}{p^2}\mathbb{Z}, \ldots, \; \overset{\sim}{\approx} v(K_n^\times) = \frac{1}{p^n}\mathbb{Z}.$$

Defn. F field, G totally ordered abelian group.

$$F((t^G)) := \left\{ \text{formal expressions } \sum_{i \in G} x_i t^i \;\middle|\; x_i \in F, \; \{i \in G \mid x_i \neq 0\} \text{ contains no infinite decreasing sequence} \right\}$$

Lemma. $F((t^G))$ is a field wrt formal addition and multiplication.

Define $v : F((t^G)) \longrightarrow G \cup \{-\infty\}$,

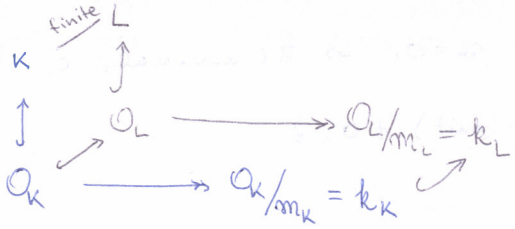
$$0 \longmapsto -\infty$$

$$0 \neq \sum_{i \in G} x_i t^i = f \longmapsto \min\{i \mid x_i \neq 0\}$$

If one picks $G \subseteq \mathbb{R}$ this gives a non-arch val field, $v\left(F((t^G))^\times\right) = G$

(look up "Hahn series"). There are also examples for mixed characteristics.

Let K be a complete discrete non-archimedean valued field with perfect residue field



We observe $\mathfrak{m}_K \subseteq \mathfrak{m}_L$, $\mathcal{O}_K \subseteq \mathcal{O}_L$

$\to$ $k_K \hookrightarrow k_L$.

Def. $f_{L/K} := [k_L : k_K]$ inertia degree, $e_{L/K} := v_L(\pi_K)$ where v_L : normalised val on L,

π_K a uniformiser in K

Thm. L/K finite field extension, K complete discrete valued non-arch field with perfect residue field. Then

1) $[L:K] = e_{L/K} \cdot f_{L/K}$

2) $\exists \alpha \in \mathcal{O}_L : \mathcal{O}_K[\alpha] = \mathcal{O}_L$.

Prop. $\mathcal{O}_L$ is fin gen and free as an $\mathcal{O}_K$-module, of rk $[L:K]$ and $[k_L : k_K] \leq [L:K]$

PF: Choose basis of L as K-vector space: $\alpha_1, \dots, \alpha_n \in L$, $n = [L:K]$

For the sup-norm $\|\cdot\|$ we have shown that it is equivalent to $|\cdot|_L$.

So we find values $r > s > 0$ s.t. $M := \{x \in L \mid \|x\| \leq s\} \subseteq \mathcal{O}_L \subseteq N := \{x \in L \mid \|x\| \leq r\}$

$\mathcal{O}_L = \{x \in L \mid |x|_L \leq 1\}$

Wlog $\exists a, b \in K : r = |a|$, $s = |b|$ (here we may need to modify r, s).

$$M = \bigoplus_{i=1}^{n} \mathcal{O}_K \cdot b \cdot \alpha_i \subseteq \mathcal{O}_L \subseteq N = \bigoplus_{i=1}^{n} \mathcal{O}_K \cdot a \cdot \alpha_i$$

Observe that M, N are fin gen rk n free $\mathcal{O}_K$-modules. (There can't be any torsion since $M \subseteq N \subseteq L$ field.) Classification of fin gen modules over a PID $\Rightarrow$ ($\mathcal{O}_K$ is a PID)

$\Rightarrow \mathcal{O}_L$ is of rk n (in particular, it is fin. gen.)

Recall $k_K = \mathcal{O}_K / \mathfrak{m}_K \subseteq \mathcal{O}_L / \mathfrak{m}_L = k_L$. Since $\mathcal{O}_L$ fin gen $/\mathcal{O}_K$ by n elts, k_L is gen by n elts over k_K, i.e. $[k_L : k_K] \leq n = [L:K]$.

PF OF THM: Prop. $\Rightarrow k_L/k_K$ finite. Also separable since k_K is perfect. $\Rightarrow$

$\exists \bar{\alpha} \in k_L$ s.t. $k_L = k_K(\bar{\alpha})$. Let $\bar{f}$ be the minimal polynomial of $\bar{\alpha}$, $\bar{f} \in k_K[X]$.

Let $f \in \mathcal{O}_K[X]$ be a monic lift of the same degree.

Claim $\exists \alpha \in \mathcal{O}_L$ lift of $\bar{\alpha}$ s.t. $v_L(f(\alpha)) = 1$.

PF: Observe $v_L(f(\alpha)) \geq 0$. We can even assume ≥ 1, for otherwise $f(\alpha)$ is a unit, then so is $\bar{f}(\bar{\alpha}) = 0$ ↯

If for an arbitrary lift β we have $v_L(f(\beta)) = 1$, $\alpha := \beta$, we are done. ✓

Assume $v_L(f(\beta)) \geq 2$, and let $\alpha := \beta + \pi_L$.

Then $f(\alpha) = f(\beta + \pi_L) = f(\beta) + f'(\beta)\pi_L + (\dots)\pi_L^2$ Taylor expansion of f

($f(\beta)$: $v_L \geq 2$; $(\dots) \in \mathcal{O}_L$; $v_L \geq 2$)

We have $v_L(f'(\beta)) = 0$, otherwise β is a multiple root mod $\mathfrak{m}_L$, but k_L/k_K is sep'ble.

$\Rightarrow v_L(f'(\beta)\pi_L) = v_L(f'(\beta)) + v_L(\pi_L) = 0 + 1 = 1 \Rightarrow v_L(f(\alpha)) = 1$ ✓

Claim. $\{\alpha^i \pi_L^j \mid 0 \le i \le f-1,\ 0 \le j \le e-1\}$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$.

Pf: Linear independence: $\lightning$ $\sum a_{ij} \alpha^i \pi_L^j = 0$, not all $a_{ij} \in \mathcal{O}_K$ are 0.

Define $s_j := \sum_{i=0}^{f-1} a_{ij} \alpha^i$. We claim $\exists j: s_j \neq 0$. $\lightning$ If all $s_j = 0$ then by linear independence of the α^i, all $a_{ij} = 0$, this holds for every j. $\lightning$

(they are indep over $k_K \Rightarrow$ indep over $\mathcal{O}_K$)

Now we claim $e \mid v_L(s_j)$ for $s_j \neq 0$.

Pf: Pick k s.t. $|a_{kj}|$ is maximal. (This is $\neq 0$).

$\Rightarrow a_{kj}^{-1} s_j = \sum_{i=0}^{f-1} a_{kj}^{-1} a_{ij} \alpha^i \Rightarrow$ all coeffs on RHS have $|\cdot| \le 1$ and one has $|\cdot| = 1$.

$\Rightarrow a_{kj}^{-1} s_j \not\equiv 0 \mod \mathfrak{m}_L$ because $|a_{kj}^{-1} s_j| \not< 1$

$\Rightarrow v_L(a_{kj}^{-1} s_j) = 0 \Rightarrow v_L(s_j) = v_L\left(a_{kj}^{-1} a_{kj} s_j\right) = \underbrace{v_L(a_{kj}^{-1} s_j)}_{0} + v_L(a_{kj}) \in \underbrace{v_L(K^\times)}_{e \cdot v_L(L^\times) = e\mathbb{Z}}$

Now write $\sum a_{ij} \alpha^j \pi_L^j = \sum_j s_j \pi_L^j = 0$

if $s_j \neq 0 \Rightarrow v_L(s_j \pi_L^j) = \underbrace{v_L(s_j)}_{\in e\mathbb{Z}} + j \Rightarrow$ all summands in the sum have pairwise different valuation $\lightning$

This proves linear independence. ✓ 06.11.2018

Generators: $M := \bigoplus_{i,j} \alpha^i \pi^j \mathcal{O}_K$, $N := \bigoplus_{i=0}^{f-1} \alpha^i \mathcal{O}_K$ Wts $M = \mathcal{O}_L$

$M = N + \pi_L N + \dots + \pi_L^{e-1} N$

$\mathcal{O}_L = N + \pi_L \mathcal{O}_L$ since $1, \bar{\alpha}, \dots, \bar{\alpha}^{f-1}$ are a k_K-basis of k_L

$= N + \pi_L(N + \pi_L \mathcal{O}_L) = \dots$ repeat

$= \underbrace{N + \pi_L N + \dots + \pi_L^{e-1} N}_{M} + \pi_L^e \mathcal{O}_L$

$e = v_L(\pi_K) \Rightarrow v_L(\pi_L^e) = v_L(\pi_K) \Rightarrow v_L\left(\frac{\pi_L^e}{\pi_K}\right) = 1$

$\Rightarrow \frac{\pi_L^e}{\pi_K}$ is a unit $\Rightarrow \mathcal{O}_L = M + \pi_K \mathcal{O}_L$

$\Rightarrow \mathcal{O}_L = M + \underbrace{\pi_K M}_{\subseteq M \text{ by def of } M \text{ and } \pi_K^e = \pi_L} + \pi_K^2 \mathcal{O}_L = M + \pi_K^2 \mathcal{O}_L = \dots$ repeat

$= M + \underbrace{\pi_K^m \mathcal{O}_L}_{\text{of arbitrarily small val.}}$ for any $m \ge 1 \Rightarrow M$ is dense in $\mathcal{O}_L$

M is the closed unit ball in the max-norm wrt the K-basis $\{\alpha^i \pi^j\}$ of L

$\Rightarrow M$ is closed. But K is complete wrt its abs val $\Rightarrow L$ is complete wrt. its abs. val. $\Rightarrow M$ is itself complete.

Complete + dense in $\mathcal{O}_L \Rightarrow M = \mathcal{O}_L$. ✓

It remains to show $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

Write $\alpha^i \pi^j = \alpha^i f(\alpha)^j$ and note that the latter, when expanded, is a polynomial in α.

↑ Here we finally use that $f(\alpha)$ is of valuation 1, hence a uniformiser, and π_L is an arbitrary uniformiser, so we may simply choose $\pi_L := f(\alpha)$.

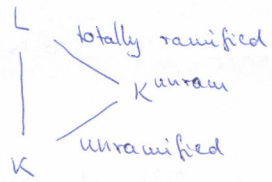
Cor. $M/L/K$ tower of field extensions. $\Rightarrow f_{M/K} = f_{M/L} \cdot f_{L/K}$, $e_{M/K} = e_{M/L}\, e_{L/K}$.

Pf: For f, this is just the tower law for field extensions $k_M / k_L / k_K$.

For e, we could check directly or use the Thm. and the formula for f.

Def. L/K is unramified if $e=1$, totally ramified if $f=1$.

We will show later that any extn has a unique unramified subextn.



So to understand field extensions, we need to understand unram and tot. ram. extensions.

↑ friendly ↑ difficult.

Thm. K as before. For any finite extn l/k_K $\exists!$ finite unram extn L/K s.t. $k_L = l$ and L/K is Galois with $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(l/k_K)$. ↑ up to iso (or up to alg closure)

Pf: Let $\bar{\alpha}$ be a primitive element for l/k_K, i.e. $l = k_K(\bar{\alpha})$.

Let $\bar{f}$ be its min poly, f a monic lift in $\mathcal{O}_K[x]$; $\deg f = \deg \bar{f}$.

$\bar{f}$ irr'ble $\Rightarrow f$ irr'ble.

Let $L := K(\alpha)$, i.e $L = K[x]/(f(x))$. We have $[L:K] = \deg f = \deg \bar{f} = [k_K(\bar{\alpha}) : k_K] = [l : k_K]$.

Furthermore, k_L contains a root of $\bar{f} \Rightarrow$ there is a field embedding $l \hookrightarrow k_L$.

By comparing degrees, we deduce $l = k_L$:

$[k_L : k_K] \geq [l : k_K] = [L : K] \Rightarrow L/K$ is unramified and $l = k_L$.

Ex. $K = \mathbb{F}_p((t))$, $k_K = \mathbb{F}_p$. By the Thm. any fin. extn of $\mathbb{F}_p$ lifts uniquely up to iso to an unramified extn of $\mathbb{F}_p((t))$. Recall: $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$

This also works for $\mathbb{Q}_p$:

$\mathbb{Q}_p$
$\cup$
$\mathbb{Z}_p \longrightarrow \mathbb{F}_p$

"choosing any f"

08.11.2018

Prop. The unramified extns of $\mathbb{Q}_p$ are $\mathbb{Q}_p(\zeta_{p^n-1})$ $\forall n \geq 1$

PF: $\mathbb{F}_{p^n} = \mathbb{F}_p(\zeta_{p^n-1})$ is the residue field. □

Ex. ("choosing any e") $K := \mathbb{C}((t))$, $L := \mathbb{C}((t^{1/n}))$,

$$\begin{array}{ccc} \mathbb{C}((t^{1/n})) & n \\ | & \| \\ \mathbb{C}((t)) & 1 \end{array}$$

$[\mathbb{C}((t^{1/n})) : \mathbb{C}((t))] = n$, $k_K = \mathbb{C}$

$\mathbb{C} = \overline{\mathbb{C}} \Rightarrow k_L = \mathbb{C} \Rightarrow f = 1 \Rightarrow e = n$ (using heavy machinery, i.e. fund. thm. of alg.)

Note that t is an uniformiser of $\mathbb{C}((t))$

$v_L(t) = n \Rightarrow e = n$ directly by defn.

Ex. $\mathbb{Q}_3(\zeta_8, \sqrt{3})/\mathbb{Q}_3$ has $n = 4$, $e = 2$, $f = 2$, is Galois with $\mathrm{Gal}(\cdot/\cdot) = \mathbb{Z}_2 \times \mathbb{Z}_2$

We develop some machinery to compute Galois groups of such extensions.

Thm. K discrete non-arch valued field with k_K perfect. Then $\forall\, \ell/k_K$ fin extn $\exists!$ up to iso unramified L/K s.t. $k_L = \ell$. Moreover, if ℓ/k_K is Galois then so is L/K and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k_K)$.

PF: Let us have $\ell = k_K(\bar{\alpha})$, $\bar{f}$ min poly of $\bar{\alpha}$, $f \in \mathcal{O}_K[x]$ monic lift of same deg.

this is irr'ble b/c f is. $L := K(\alpha)$ where α is any root of f.

Already seen: unramified.

Lemma. L/K fin. unram. extn., M/K any finite extn $\Rightarrow$ we have a nat. bijection

$$\mathrm{Hom}_{K\text{-alg}}(L, M) \longrightarrow \mathrm{Hom}_{k_K\text{-alg}}(k_L, k_M)$$

PF: We have canonical unique extension of abs values to L, M.

So if $\varphi \in \mathrm{Hom}(L, M)$, $\varphi : L \to M$, $\varphi|_{\mathcal{O}_L} : \mathcal{O}_L \to \mathcal{O}_M$, $\varphi|_{\mathfrak{m}_L} : \mathfrak{m}_L \to \mathfrak{m}_M$,

induces $k_L = \mathcal{O}_L/\mathfrak{m}_L \xrightarrow{\bar{\varphi}} \mathcal{O}_M/\mathfrak{m}_M = k_M$.

$$\begin{array}{ccc} \mathrm{Hom}(L, M) & \longrightarrow & \mathrm{Hom}(k_L, k_M) \\ \| & & \| \\ \{x \in M \mid f(x) = 0\} & \xrightarrow[\text{reduction mod } \mathfrak{m}]{*} & \{y \in k_M \mid \bar{f}(y) = 0\} \end{array}$$

φ is defined by $\varphi(\alpha)$, recall $L = K(\alpha)$

$\bar{\varphi}$ def'd by $\bar{\varphi}(\bar{\alpha})$

HL $\Rightarrow$ any simple root of $\bar{f}$ lifts uniquely to a simple root over $\mathcal{O}_L$

This settles surjectivity of $*$.

Injectivity follows from looking at degrees. $\Big\}$ $\Rightarrow$ iso

Gal just consists of automorphisms $\Rightarrow$ use the correspondence given in the lemma for Aut, it sends auts to auts. This also shows that L/K is Galois. □

Rmk. For any Galois extn L/K there is a canonical map

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(k_L/k_K).$$

Prop. K as before. Let L/K be fin unram and M/K fin. Suppose L, M lie in a joint alg closure of K. Then:

- LM/M is unramified
- any subext of L/K is unramified
- if M/K is unram $\Rightarrow$ LM/K is unram.

Rmk: this looks like a base change in AG, a compositum is a bit like a tensor product.

Pf: $\bar{\alpha}$ primitive elt of k_L/k_K, $\bar{f}$ min. poly., $f \in \mathcal{O}_L[x]$ monic lift with $\deg f = \deg \bar{f}$, α a lift of $\bar{\alpha}$, $L = K(\alpha)$. (These are the same steps as before.)

$\Rightarrow LM = M(\alpha)$.

Let $\bar{g}$ be the min poly of k_{LM}/k_M. $\Rightarrow \bar{g} \mid \bar{f}$, $\bar{g}\cdot\bar{h} = \bar{f}$

$\bar{g}$ and $\bar{h}$ are coprime, apply HL $\Rightarrow$ $f = gh \in \mathcal{O}_M[x]$ lifting $\bar{f} = \bar{g}\bar{h}$, $\deg g = \deg \bar{g}$

$\Rightarrow$ g is a min. poly of α over M.

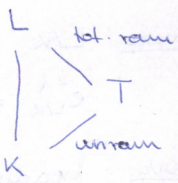
$$\left.\begin{aligned} &[LM:M] = \deg g = \deg \bar{g} = [k_{LM}:k_M] \\ &e_{LM/M}\cdot[k_{LM}:k_M] = [LM:M] \end{aligned}\right\} \Rightarrow e_{LM/M} = 1, \text{ i.e. } LM/M \text{ is unram.} \checkmark$$

Let L' be a subext of L/K. $\Rightarrow$ $\underbrace{e_{L/K}}_{=1} = \underbrace{e_{L/L'}}_{\in\mathbb{Z}_{\geq 0}}\cdot\underbrace{e_{L'/K}}_{\in\mathbb{Z}_{\geq 0}}$ $\Rightarrow e_{L/L'} = e_{L'/K} = 1$. $\checkmark$

Suppose that M/K is unram. $\Rightarrow e_{LM/K} = e_{LM/M}\cdot e_{M/K} = 1\cdot 1 = 1$. $\checkmark$

Prop. K as before, L/K fin extn $\Rightarrow$ $\exists!$ maximal unramified subextension T.

Furthermore, $[T:K] = f_{L/K}$. (Hence L/T is totally ramified.)

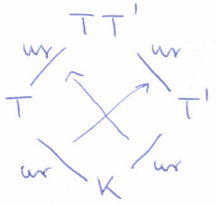


Pf: Let T be the unique (up to iso) extn of K with res field k_L.

Then id: $k_T \xrightarrow{\sim} k_L$ lifts to an embedding $T \hookrightarrow L$ by prev. Lemma.

We get $L/T/K$ and $[T:K] = f_{L/K}$.

Now let T' be another unram extn, and consider the compositum TT'.



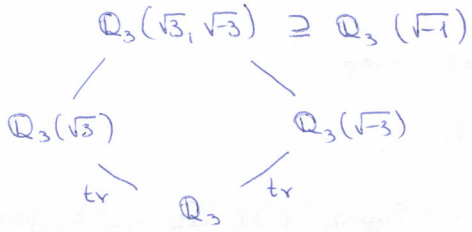
TT'/T and TT'/T are ur by Prop. above ("base change")

$[T:K] \leq [TT':K] \leq f_{L/K} = [T:K]$ $\Rightarrow [TT':K] = f_{L/K}$

$$\underbrace{[TT':K]}_{f_{L/K}} = [TT':T]\cdot\underbrace{[T:K]}_{f_{L/K}}$$

$\Rightarrow [TT':T] = 1$, $TT' = T$ $\Rightarrow T'$ is unique.

Ex.



Exc.: find $L_1/\mathbb{Q}_p$, $L_2/\mathbb{Q}_p$ totally ramified extensions s.t. $L_1L_2/\mathbb{Q}_p$ is not ramified.

Outlook:

k field, X/k a smooth curve, $x \in X$ a closed point.

Then $\mathcal{O}_{X,x}$ is a DVR, $\widehat{\mathcal{O}_{X,x}}$ completion wrt m_x $\Rightarrow$ $\widehat{\mathcal{O}}_{X,x}$ complete DVR.

$\widehat{K}_x := \operatorname{Frac} \widehat{\mathcal{O}}_{X,x}$ non-arch disc val field, complete

Ex. $k = \mathbb{F}_q$ $\Rightarrow$ $\widehat{K}_x$ is a complete val. field of the same characteristic.

$\widehat{K}_x \simeq \mathbb{F}_q((t))$. If $f: X \to Y$ is a morph of curves, $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$, get a field extn $\widehat{K}_x / \widehat{K}_{f(x)}$ (a.o.u.).

Then f is unramified if $\widehat{K}_x / \widehat{K}_{f(x)}$ is unram in our sense, for every $x \in X$.

13.11.2018

Prop. K non-arch discretely val field with perfect residue field.

Then there is a canonical equivalence of categories

$$\left\{\begin{array}{l}\text{unramified extensions } L/K \\ \text{with } K\text{-algebra homomorphisms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{finite extensions } \ell/k_K \\ \text{with } k_K\text{-alg homomorphisms}\end{array}\right\}$$

This was proven last time, this is just a rephrasing. □

Totally ramified extensions Standing assumption: K is complete.

Def. K non-arch disc. val. field. Suppose $f = x^n + \dots + a_0 \in \mathcal{O}_K[x]$ such that $a_1, \dots, a_{n-1} \in m_K$ and a_0 is a uniformiser. Then f is an Eisenstein polynomial.

Thm. (Eisenstein criterion) Every Eisenstein polynomial is irreducible.

Pf: As over $\mathbb{Z}$. □

Lemma. L/K fin extn, v_K normalised val of K, w the unique extension to L. Then

$$e_{L/K} = w(\pi_L) = \min\{ w(x) \mid x \in m_L \}$$

Rmk: Already seen: unique extension of valuations, $v(x) = \begin{cases} -\log|x| & x \neq 0 \\ \infty & x = 0 \end{cases}$

Note that w need not be normalised.

PF OF LEMMA: $v_L :=$ normalised val on L $\Rightarrow$ $\exists C > 0$: $w = C \cdot v_L$

What is this C? $v_K(\pi_K) = 1$ $\Rightarrow$ $w(\pi_K) = 1$ since w extends v_K

$1 = w(\pi_K) = e^{-1}_{L/K} v_L(\pi_L)$ by def of $e_{L/K}$ $\Rightarrow$ $C = e^{-1}_{L/K}$

$w(\pi_L) = e^{-1}_{L/K} v_L(\pi_L) = e^{-1}_{L/K} \cdot 1$. ✓

$w(\pi_L) = \min\{ w(x) \mid x \in m_L \}$ because π_L is a uniformiser ✓ □

Thm. 1) Let L/K be totally ramified finite ext. $\Rightarrow$ any uniformizer π_L of L has Eisenstein minimal polynomial.

2) If $L = K(\alpha)$ and α has Eisenstein minimal polynomial then L/K is totally ramified and α is a uniformizer.

Lemma. $x, y \in K$, $|x| \neq |y| \Rightarrow |x+y| = \max(|x|, |y|)$

$v(x) \neq v(y) \Rightarrow v(x+y) = \min(v(x), v(y))$

PF OF THM: 1) $n := [L:K]$, v_K norm. valuation of K, w the unique extn to L

$K \subseteq K(\pi_L) \subseteq L$, $e_{K(\pi_L)/K} \cdot f_{K(\pi_L)/K} = [K(\pi_L):K] \Rightarrow [K(\pi_L):K] \geq e_{K(\pi_L)/K}$

$\Rightarrow [K(\pi_L):K]^{-1} \leq e^{-1}_{K(\pi_L)/K} = \min\{w(x) \mid x \in \mathfrak{m}_{K(\pi_L)}\} \leq w(\pi_L) = \frac{1}{n}$ ($\uparrow$ L/K tot. ram.)

$\Rightarrow [K(\pi_L):K] \geq n = [L:K] = [K(\pi_L):K] \cdot \underbrace{[L:K(\pi_L)]}$

$\Rightarrow 1$, i.e. $L = K(\pi_L)$.

Let π_L have min poly $f(x) = x^n + \dots + a_0 \in \mathcal{O}_K[x]$

$\Rightarrow \pi_L^n = -a_0 - a_1\pi_L - \dots - a_{n-1}\pi_L^{n-1}$. Note that $w(\pi_L^n) = 1$ because w extends v_K.

$1 = w(\pi_L^n) = w(-a_0 - \dots - a_{n-1}\pi_L^{n-1}) \overset{\text{Lemma}}{=} \min_{0 \leq i \leq n-1} \left(\underbrace{v_K(a_i)}_{\in \mathbb{Z}} + \underbrace{\frac{i}{n}}_{\notin \mathbb{Z} \text{ unless } i=0} \right)$

have pwise distinct valuations because their fractional parts differ: $w(a_i \pi_L^i) = v_K(a_i) + \frac{i}{n} \in \mathbb{Z} + \frac{i}{n}$

$\Rightarrow \forall i \in \{1, \dots, n-1\}: v_K(a_i) \geq 1$ and $v_K(a_0) = 1$.

2) $n := [L:K]$, let g be the min poly of α, $g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0 \in \mathcal{O}_K[x]$

g is Eisenstein $\Rightarrow 1 = w(b_0) = n \cdot w(\alpha) \Rightarrow w(\alpha) = \frac{1}{n} \Rightarrow \alpha \in \mathfrak{m}_L$

$e^{-1}_{L/K} = \min\{w(x) \mid x \in \mathfrak{m}_L\} \leq w(\alpha) = \frac{1}{n} \Rightarrow e_{L/K} \geq n \geq e_{L/K} \Rightarrow e_{L/K} = n$, L/K tot. ram.

Galois groups in the ramified situation

L/K Galois $\Rightarrow$ $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(\ell/k_K)$

Def. For $s \geq 1$: $U_K^{(s)} := 1 + \pi_K^s \mathcal{O}_K$ higher unit groups (with multiplication from $\mathcal{O}_K$),

$U^{(1)} \supseteq U^{(2)} \supseteq \dots$ higher unit filtration.

Claim. These are groups indeed.

PF: $(1+\pi^s u)(1+\pi^s v) = 1 + \pi^s(u+v) + \pi^{2s}(uv) \in U^{(s)}$ ✓

$\frac{1}{1+\pi^s u} = \sum_{n \geq 0} (-\pi^s u)^n = 1 - \pi^s u + \dots \in U^{(s)}$ ✓

A more elegant way to show this: $U^{(i)} \hookrightarrow \mathcal{O}_K^\times \longrightarrow \left(\mathcal{O}_K / \pi^s \mathcal{O}_K\right)^\times$

Prop. Let $U_K := \mathcal{O}_K^\times$. Then $U_K/U_K^{(1)} \simeq (k_K^\times, \cdot)$ and $U_K^{(s)}/U_K^{(s+1)} \simeq (k_K, +)$.

Pf: We have $\mathcal{O}_K^\times \twoheadrightarrow k_K^\times$. Define the first iso as the mod π map, this has $U_K^{(1)}$ as its kernel. ✓

For the second iso, define $U_K^{(s)} \longrightarrow (k_K, +)$

$$1+\pi^s x \longmapsto x$$

This is a group homomorphism (easy). Also, it is surjective, and has kernel $U_K^{(s+1)}$. ✓ □

Def Let L/K be a finite Galois extension, v_L the normalised valuation of L.

Let $s \in \mathbb{R}$, $s \geq -1$. Define $G_s(L/K) := \{\sigma \in \mathrm{Gal}(L/K) \mid v_L(\sigma x - x) \geq s+1 \quad \forall x \in \mathcal{O}_L\}$.

Think of these G_s as a filtration of $G = \mathrm{Gal}(L/K)$.

Observe the following: $G_{-1}(L/K) = G$, $\bigcap_s G_s(L/K) = \{1\}$

$$\begin{aligned} G_0(L/K) &= \{\sigma \in G \mid v_L(\sigma x - x) \geq 1 \quad \forall x \in \mathcal{O}_L\} \\ &= \{\sigma \in G \mid \sigma x \equiv x \quad (\mathfrak{m}_L)\} \\ &= \ker\left(\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(k_L/k_K)\right) \end{aligned}$$

Rmk Now it would suffice to have $s \in \mathbb{Z}$ since jumps only happen at integers. Nevertheless, $s \in \mathbb{R}$ will offer a nice generalisation later.

Thm. L/K fin Galois $\Rightarrow$ $G_s/G_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)}$ $\forall s \geq 1$

Note that rhs is abelian $\Rightarrow$ G_s/G_{s+1} abelian. This will play an important role in proving solubility.

15.11.2018

Restating:

Thm. L/K Galois, finite extn., v_L norm val on L. Then $\forall s \in \mathbb{Z}_{\geq 0}$

1) $G_{s+1} \trianglelefteq G_s$

2) $G_s/G_{s+1} \longrightarrow U_L^{(s)}/U_L^{(s+1)}$ where π_L is any uniformiser is
$\sigma \longmapsto \sigma(\pi_L)/\pi_L$ independent of π_L and injective.

Def L/K as above. Inertia subgroup: $I := \ker\left(\mathrm{Gal}(L/K) \xrightarrow{\#} \mathrm{Gal}(k_L/k_K)\right)$

Observation: $G_0 = I$.

Lemma. $\#$ is surjective.

Pf: Let T/K be the maximal unramified subextension of L/K.

Then $k_T = k_L$. We had a commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(k_L/k_K) \\ \downarrow & & \| \\ \mathrm{Gal}(T/K) & \xrightarrow{\sim} & \mathrm{Gal}(k_T/k_K) \end{array}$$

Since T/K is unramified, the bottom horizontal map is an iso.

Consequently, the top horizontal map must be a surjection, proving the Lemma. □

Cor. We actually have a ses of gps:

$$0 \longrightarrow G_0 \hookrightarrow G \longrightarrow Gal(k_L/k_K) \longrightarrow 0$$

Lemma. $\sigma \in I \Rightarrow \forall x \in k_L : \sigma([x]) = [x]$.

more generally, if $\sigma \in Gal(L/K)$ with $\bar{\sigma}$ as its img under $G \twoheadrightarrow Gal(k_L/k_K)$ then $\left[\bar{\sigma}(x)\right] = \sigma([x])$.

Here $[\cdot]$ denotes the Teichmüller lift.

Pf: Consider the map $f: k_L \longrightarrow \mathcal{O}_L$.

$$x \longmapsto \sigma^{-1}\left([\bar{\sigma}(x)]\right)$$

This f is multiplicative because $[\cdot]$ is.

Computing modulo π_L, we get $\sigma^{-1}\left([\bar{\sigma}(x)]\right) \equiv x \pmod{\pi_L}$.

$\Rightarrow f$ has all the properties of the Teichmüller lift.

By uniqueness, $f = [\cdot]$. This yields the assertion of the Lemma.

Pf of THM: $\sigma \in G_s \Rightarrow v_L(\sigma(\pi_L) - \pi_L) \geq s+1$

$\varphi: G_s \longrightarrow U^{(s)}/U^{(s+1)}$, $\sigma \longmapsto \frac{\sigma(\pi_L)}{\pi_L}$

$\Rightarrow \sigma(\pi_L) = \pi_L + \pi_L^{s+1} \cdot x$ for some $x \in \mathcal{O}_L$

$\Rightarrow \frac{\sigma\pi_L}{\pi_L} \in 1 + \pi_L^s \mathcal{O}_L = U^{(s)}$ ✓ Well-definedness.

Independence of π_L: Let $u \in \mathcal{O}_L^\times = U$. $\Rightarrow \sigma(u) = u + \pi_L^{s+1} y$ for some $y \in \mathcal{O}_L$

$$\Rightarrow \frac{\sigma(u\pi_L)}{u\pi_L} = \frac{u + \pi_L^{s+1} y}{u} \cdot \frac{\pi_L + \pi_L^{s+1} x}{\pi_L}$$

$$= (1 + \pi_L^{s+1} y u^{-1}) \cdot (1 + \pi_L^s x)$$

$$= 1 + \pi_L^s x + \pi_L^{s+1} \cdot (\dots) \equiv 1 + \pi_L^s x \pmod{\pi_L^{s+1}},$$

i.e. $\frac{\sigma(u\pi_L)}{u\pi_L} = \frac{\sigma(\pi_L)}{\pi_L}$ in $U^{(s)}/U^{(s+1)}$ ✓

Group homomorphism: $\sigma, \tau \in G_s$

$$\varphi(\sigma\tau) = \frac{(\sigma\tau)(\pi_L)}{\pi_L} = \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \cdot \frac{\tau(\pi_L)}{\pi_L} = \frac{\sigma(\pi_L)}{\pi_L} \cdot \frac{\tau(\pi_L)}{\pi_L} = \varphi(\sigma)\varphi(\tau).$$

(by independence of π_L) ✓

Claim. $\ker \varphi = G_{s+1}$. Note that this settles the Thm.

$$\ker \varphi = \left\{\sigma \in G_s \mid v_L(\sigma(\pi_L) - \pi_L) \geq s+2\right\}$$

$$G_{s+1} = \left\{\sigma \in G \mid v_L(\sigma(x) - x) \geq s+2 \quad \forall x \in \mathcal{O}_L\right\} \Rightarrow G_{s+1} \subseteq \ker \varphi.$$

For the converse, we use Teichmüller lifts.

Let $x \in \mathcal{O}_L$, $x = \sum_{n=0}^{\infty} [x_n] \cdot \pi_L^n$

$\exists y \in \mathcal{O}_L : \sigma(\pi_L) = \pi_L + \pi_L^{s+1} y$

$$\Rightarrow \sigma(x) - x = \sigma\left(\sum_n [x_n] \pi_L^n\right) - \sum_n [x_n] \pi_L^n$$

$$= \sum_n [x_n] \cdot \left(\sigma(\pi_L)^n - \pi_L^n\right)$$

$$= \sum_n [x_n] \cdot \underbrace{\left(\sigma(\pi_L) - \pi_L\right)}_{v_L(\cdot) \geq s+1} \cdot \underbrace{(\dots)}_{\in \mathcal{O}_L}$$

σ acts trivially on Teichmüller lift by Lemma.

$\Rightarrow v_L(\sigma(x) - x) \geq s+2 \Rightarrow \ker \varphi \subseteq G_{s+1}$. ✓ □

Cor. 1. L/K totally ramified finite Galois extension $\Rightarrow$ $\mathrm{Gal}(L/K)$ solvable.

Pf: $0 \longrightarrow G_0 \longrightarrow G \longrightarrow \underbrace{\mathrm{Gal}(k_L/k_K)}_{0 \text{ because } L/K \text{ tot ram}} \longrightarrow 0$

$\Rightarrow G = G_0$. The latter is filtered with abelian subquotients. □

Cor. 2. L/K arbitrary finite Galois extension and k_K is finite $\Rightarrow$ $\mathrm{Gal}(L/K)$ solvable. Moreover, G_1 is the unique p-Sylow group of G_0.

Pf: As before, just use that $\mathrm{Gal}(k_L/k_K)$ is abelian, so there is just one more factor.

$U/U^{(1)} \simeq \mathbb{F}_q^\times$ where $k_K \simeq \mathbb{F}_q$, this is a fin gp of order prime to p.

$U^{(s)}/U^{(s+1)} \simeq (\mathbb{F}_q, +)$ is a finite p-group. □

Def: Local field (terminology of this course): complete discrete valued field with finite residue field.

Note: Many books also assume the res field to be perfect.

Other def: Local field: locally compact topological field with non-discrete topology.

Thm. (van Dantzig, Weil) F local field in the sense of the Other def. then it is

1) a fin ext of $\mathbb{F}_p((t))$
2) a fin ext of $\mathbb{Q}_p$
3) a fin ext of $\mathbb{R}$

The pf is done using Ostrowski's Thm.

We have equipped $\mathrm{Gal}(L/K)$ with a canonical filtration, called the (lower) ramification filtration. $\mathrm{Gal}(L/K)_s$

If $N/L/K$ is a Galois tower, how does the filtration behave there?

Prop. $\mathrm{Gal}(M/K)_s \cap \mathrm{Gal}(M/L) = \mathrm{Gal}(M/L)_s$

Pf: $\mathrm{Gal}(M/K)_s = \{\sigma \in \mathrm{Gal}(M/K) \mid v_M(\sigma x - x) \geq s+1 \quad \forall x \in \mathcal{O}_M\}$

$\mathrm{Gal}(M/L)_s = \{\sigma \in \mathrm{Gal}(M/L) \mid v_M(\sigma x - x) \geq s+1 \quad \forall x \in \mathcal{O}_M\}$

Thm. (Herbrand) Let M/L, L/K be finite Galois extensions.

Then $\exists \eta_{M/L}$ function s.t. $\mathrm{Gal}(M/L)_s \hookrightarrow \mathrm{Gal}(M/K)_s \twoheadrightarrow \mathrm{Gal}(L/K)_{\eta_{M/L}(s)}$

and $\eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}$.

Prop. L/K fin Galois extn, $\alpha \in \mathcal{O}_L$, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Then $i_{L/K}(\sigma) = v_L(\sigma\alpha - \alpha)$

where $i_{L/K}(\sigma) = \min\left\{v_L(\sigma x - x) \mid x \in \mathcal{O}_L\right\}$.

Pf: Fix σ. Then $i_{L/K}(\sigma) \leq v_L(\sigma x - x)$.

Let $x \in \mathcal{O}_L$ be arbitrary. Then $\exists g \in \mathcal{O}_K[t]$: $x = g(\alpha)$.

$$v_L(\sigma x - x) = v_L(\sigma g(\alpha) - g(\alpha)) \qquad g = \sum b_i t^i$$
$$= v_L\left(\sum b_i (\sigma(\alpha)^i - \alpha^i)\right)$$
$$= v_L\left(\sum b_i (\sigma(\alpha) - \alpha) \cdot \underbrace{(\cdots)}_{\in \mathcal{O}_L}\right) \qquad \sigma\alpha - \alpha \mid \sigma\alpha^i - \alpha^i.$$

$\Rightarrow v_L(\sigma\alpha - \alpha) \leq v_L(\sigma x - x)$.

Prop. $M/L/K$ as before. Then $\forall \sigma \in \mathrm{Gal}(L/K)$:

$$i_{L/K}(\sigma) = e_{M/L}^{-1} \sum_{\substack{\tau \in \mathrm{Gal}(M/K) \\ \tau|_L = \sigma}} i_{M/K}(\tau)$$

Pf: Suppose $\sigma \neq 1$. We write $\mathcal{O}_M = \mathcal{O}_K[\alpha]$, $\mathcal{O}_L = \mathcal{O}_K[\beta]$, $\alpha \in \mathcal{O}_M$, $\beta \in \mathcal{O}_L$

$\Rightarrow e_{M/L}\, i_{L/K}(\sigma) = e_{M/L}\, v_L(\sigma\beta - \beta) = v_M(\sigma\beta - \beta)$

If $\tau \in \mathrm{Gal}(M/K)$ then $i_{M/K}(\tau) = v_M(\tau\alpha - \alpha)$. Now assume $\tau|_L = \sigma$, and set $H := \mathrm{Gal}(M/L)$

$$\underbrace{\sum_{\substack{\tau' \in \mathrm{Gal}(M/K) \\ \tau'|_L = \sigma}} i_{M/K}(\tau')}_{v_M(\sigma\beta - \beta)} = \sum_{g \in H} v_M(\tau g(\alpha) - \alpha) = v_M\Big(\underbrace{\prod_{g \in H} (\tau g(\alpha) - \alpha)}_{a}\Big)$$

$b := \sigma\beta - \beta = \tau\beta - \beta$, $\quad a := \prod_{g \in H} (\tau g(\alpha) - \alpha)$

Let $z \in \mathcal{O}_L$ be arbitrary, $z = \sum_i z_i \beta^i$, $z_i \in \mathcal{O}_K$

$$\tau(z) - z = \sum z_i \left(\tau\beta^i - \beta^i\right) \Rightarrow \mathfrak{b} \mid \tau(z) - z$$

If F is the min poly of α over L then $F(x) = \prod_{g \in H} (x - g\alpha) = \prod_{g \in H} (x - \tau g\alpha)$

Since all coeffs are of the form $\tau z - z$ by previous observation, we have that $\mathfrak{b}$ divides every value of this polynomial $\Rightarrow \mathfrak{b} \mid (\tau F - F)(\alpha) = \prod (\alpha - g\alpha) = \pm a$

$\Rightarrow \mathfrak{b} \mid a$.

20.11.2018

Claim. $a \mid \mathfrak{b}$.

Pf: Pick $f \in \mathcal{O}_K[X]$ s.t. $f(\alpha) = \beta$. Then $F(X) \mid f(X) - \beta$

$\Rightarrow (f(X) - \beta) = F(X) \cdot h(X)$ for some $h \in \mathcal{O}_L[X]$.

$$(f - \tau\beta)(X) = (\tau f - \tau\beta)(X) = (\tau F)(X) \cdot (\tau h)(X)$$

Substitute $X = \alpha$: $\quad -\mathfrak{b} = \beta - \tau\beta = \pm a (\tau h)(\alpha)$. The Claim follows.

(by last line on p. 27)

This finishes the proof. □

Reference for this proof: [Neukirch § 10 Higher ramification groups]. p. 176

Def: Let L/K be a finite Galois extension. Then define $\eta_{L/K} : [-1, +\infty) \longrightarrow [-1, +\infty)$ as

$$\eta_{L/K}(s) := \left(e_{L/K}^{-1} \sum_{\sigma \in \mathrm{Gal}(L/K)} \min\left(i_{L/K}(\sigma), s+1\right) \right) - 1$$

Exc: $\eta_{L/K}$ is strictly increasing in s.

PF OF THM: $G := \mathrm{Gal}(M/K)$, fix $\bar{\sigma} \in \mathrm{Gal}(L/K)$. $t := \eta_{L/K}(s)$.

Among all $\tau \in \mathrm{Gal}(L/K)$ with $\tau|_L = \sigma$, pick the one maximising $i_{M/K}(\tau)$.

$\Rightarrow i_{M/K}(\tau) \geqslant i_{L/K}(\tau g) \quad \forall g \in H := \mathrm{Gal}(M/L)$

Claim. $i_{L/K}(\sigma) - 1 = \eta_{L/K}\left(i_{M/K}(\sigma) - 1\right)$

From this it follows that $\sigma \in \frac{G_s(M/K)\, H}{H}$

$\Leftrightarrow \tau \in G_s(M/K)$

$\Leftrightarrow i_{M/K}(\tau) \geq s+1$

using η is strictly incr: $\Leftrightarrow \eta_{M/L}\left(i_{M/K}(\tau) - 1\right) \geq \eta_{M/L}(s) - t$

using Claim: $\Leftrightarrow i_{L/K}(\sigma) - 1 \geq t$

$\Leftrightarrow i_{L/K}(\sigma) \geq t+1$

$\Leftrightarrow \sigma \in \mathrm{Gal}(L/K)$

So it remains to prove the Claim.

PF OF CLAIM: $i_{L/K}(\sigma) - 1 = e_{M/L}^{-1} \sum_{g \in H} i_{M/K}(\tau g) - 1$ by Prop.

Wts equality of these ↳ $\eta_{M/L}(i_{M/K}(\tau) - 1) = e_{M/L}^{-1} \sum_{g \in H} \min\left(i_{M/L}(g), i_{M/L}(\tau)\right) - 1$ by Def.

What remains after ⌙ looks like the strong triangle inequality.

We claim the stronger statement

$$i_{M/K}(\tau g) = \min\left(i_{M/L}(g), i_{M/L}(\tau)\right),$$

which indeed implies the Claim.

$$\begin{aligned} i_{M/K}(\tau g) &= v_M\left(\tau g(\alpha) - \alpha\right) \quad \text{where } \mathcal{O}_M = \mathcal{O}_K[\alpha] \\ &= v_M\left(\tau g(\alpha) - g(\alpha) + g(\alpha) - \alpha\right) \\ &\overset{(*)}{\geqslant} \min\left(v_M\left(\tau g(\alpha) - g(\alpha)\right), v_M\left(g\alpha - \alpha\right)\right) \quad \text{by ultrametric ineq.} \\ &= \min\left(i_{M/K}(\tau), i_{M/K}(g)\right) \end{aligned}$$

Case 1: $i_{M/K}(\tau) \leq i_{M/K}(g)$.

$\Rightarrow$ $i_{M/K}(\tau) \leq i_{M/K}(\tau g)$

On the other hand, by our choice of τ to maximise $i_{M/K}(\tau)$ we also have

$$i_{M/K}(\tau g) \leq i_{M/K}(\tau),$$

and we are done.

Case 2: $i_{M/K}(\tau) > i_{M/K}(g)$

Then we have equality in $(*)$, and we are done again.

Prop: $\eta_{L/K}(s) = \int_0^s \underbrace{\frac{dx}{\left(G_x(L/K) : G_s(L/K)\right)}}_{\vartheta(s) :=}$

PF:

Both $\eta_{L/K}$ and ϑ are piecewise linear functions, the break points are $\subseteq \mathbb{Z}$.

$\Rightarrow$ To prove equality, its left derivatives agree everywhere and the functions agree at one point.

$$\eta_{L/K}(0) = 0 = \int_0^0 \frac{dx}{(\cdot)} \quad \checkmark$$

$$\eta'_{L/K}(s) = e_{L/K}^{-1} \, \#\left\{\sigma \in G \,\middle|\, i_{L/K}(\sigma) \geqslant s+1\right\} = \frac{\#G_s(L/K)}{\#G_0(L/K)} = \frac{1}{\left(G_s(L/K) : G_0(L/K)\right)} = \vartheta'(s) \quad \checkmark$$

Def. $\psi_{L/K}(s) := \eta^{-1}_{L/K}(s)$. Note that the inverse $\eta^{-1}_{L/K}$ exists as $\eta_{L/K}$ is strictly increasing in s.

Def. L/K fin Galois. The upper ramification extension is

$$G^t(L/K) := G_{\psi_{L/K}(t)}(L/K)$$

If $M/L/K$ is a tower, the upper ram. filt. behaves nicely for M/L,
the lower " " " " for L/K

This follows from Herbrand's Thm.

Lemma. $M/L/K$ as before $\Rightarrow \eta_{M/K} = \eta_{L/K} \circ \eta_{M/L}$, $\psi_{M/K} = \psi_{M/L} \circ \psi_{L/K}$.

Pf: Herbrand for $s \in [-1, +\infty)$ and $t := \eta^{-1}_{L/K}(s)$ $\Rightarrow$

$$\Rightarrow G_t(L/K) \simeq \frac{G_s(M/L)H}{H} \simeq \frac{G_s(M/L)}{H \cap G_s(M/K)} \overset{\uparrow}{\simeq} \frac{G_s(M/K)}{G_s(M/L)} \qquad H = \mathrm{Gal}(M/L)$$

Prop. a p.27

$$\Rightarrow \frac{\# G_s(M/K)}{e_{M/K}} = \frac{\# G_t(L/K)}{e_{L/K}} \cdot \frac{\# G_s(M/L)}{e_{M/L}}$$

But we have $\eta'_{L/K}(s) = \dfrac{\# G_s(M/K)}{e_{M/K}}$

Chain rule for derivatives $\Rightarrow$ Lemma follows by integration and comparing at one point (0, most conveniently). □