Higher Ramification

June Terzioğlu

April 14, 2025

Contents

1 Abstract

This paper will be a sort of survey of various topics related to higher ramification; first I will cover some of the basic theory of the subject (much of which is elaboration on a treatise of Serre), and ultimately the end goal will be a partial exposition of a theorem of Deligne, which states that the category of at-most-s-upper-ramified extensions of a local field K is determined (up to equivalence) by $K^\times/(1+\mathfrak{m}_K^s)$. In other words, even if you only have knowledge of the field's multiplicative structure up to (modulo) a power of the maximal ideal, you can still recover knowledge about its extensions that are not too 'wildly' ramified (very roughly speaking). I will also discuss some results from a paper of Lubin, who uses something called the Newton copolygon to study the so-called 'Hasse-Herbrand' functions which help us understand higher ramification, contrasting with the Newton polygon that Deligne uses. (Ideally, it would be good to discuss more the relationship between the two in the final draft.)

2 Preliminaries

2.1 Valued fields

Definition 1. *A **valuation** on a field K is a map $v_K : K \to \mathbb{R} \cup \{\infty\}$ such that*

- $v_K(0) = \infty$
- $v_K|_{K^\times}$ *is a group homomorphism* $K^\times \to (\mathbb{R}, +)$
- $v_K(x + y) \geq \min(v_K(x), v_K(y))$ *for all* $x, y \in K$ *(where we say* $\min(\infty, a) = a$ *for all* $a \in \mathbb{R} \cup \{\infty\}$*)*

*A field K equipped with a valuation v_K is called a **valued field**, and we sometimes instead say this as that (K, v_K) is a valued field.*

One can define these in greater generality by having v_K instead map into a totally ordered abelian group Γ, but I will not need this. Really what I have defined above is called by some as a *rank one valuation*. Typically I will drop the subscript K when there is no ambiguity.

Here are a few easy lemmas about valuations; the last will be fundamental in our discussion later about Newton copolygons / valuation functions:

Theorem 1. *Let (K, v) be a valued field.*

- $v(1) = v(-1) = 0$ *(in particular,* $v(-x) = v(x)$*).*
- *If* $x \in K^\times$*, then* $v(x^{-1}) = -v(x)$*.*
- *If* $x_1, \ldots, x_n \in K$ *with* $v(x_j) < v(x_i)$ *for all* $i \neq j$*, then* $v\left(\sum\limits_{i=1}^{n} x_i\right) = v(x_j)$ *(i.e. even though* $v\left(\sum\limits_{i=1}^{n} x_i\right) \geq \min\limits_{1 \leq i \leq n} \{v(x_i)\}$ *in general, equality holds when the minimum is unique).*

Proof: The first is because $v(1^2) = v(1) + v(1)$ and $0 = v(1) = v((-1)^2) = v(-1) + v(-1)$; the second is because $v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$. For the third, let's assume $j = 1$ by relabelling. Write $r \triangleq v(x_1)$, so that $v(x_i) > r$ and so $v(-x_i) > r$ for all $i > 1$. Then if $v\left(\sum\limits_{i=1}^{n} x_i\right) > r$ as well, we have

$$v(x_1) = v\left(\sum_{i=1}^{n} x_i + \sum_{i=2}^{n} (-x_i)\right) \geq \min\left(v\left(\sum_{i=1}^{n} x_i\right), \min_{2 \leq i \leq n} \{v(-x_i)\}\right) > r$$

which is a contradiction.

$\square$

Definition 2. *A* ***discrete valuation*** *is simply a valuation whose image is* $r\mathbb{Z} \cup \{\infty\}$*, for some* $r \in \mathbb{R}_{>0}$ *(which, by post-composing with a scaling, we will always assume is* 1 *unless otherwise stated); a field* K *equipped with a discrete valuation* v *is called a* ***discretely valued field*** *(sometimes written as a pair* (K, v)*).*

A concept closely related to valuations is absolute values:

Definition 3. *An* ***absolute value*** *on a field* K *is a map* $|\cdot|_K : K \to \mathbb{R}_{\geq 0}$ *such that*

- $|0|_K = 0$
- $|\cdot|_K|_{K^\times}$ *is a homomorphism* $K^\times \to (\mathbb{R}_{>0}, \cdot)$
- $|x + y|_K \leq |x|_K + |y|_K$ *(triangle inequality)*

If $|\cdot|_K$ *satisfies the ultrametric inequality* $|x + y|_K \leq \max(|x|_K, |y|_K)$ *and not just the weaker triangle inequality, we call it non-archimedean.*

There is a bijection between non-archimedean absolute values and valuations on a field K; simply fix some $c \in (0, 1)$ and map a valuation v to c^{-v}. For this reason we can essentially think of them as the same thing - topologically, it makes little difference which c we choose, since c^{-v} is equivalent to d^{-v} for any $c, d \in (0, 1)$ (in the sense that they give K the same topology) [1]

Definition 4. *A* ***discrete valuation ring*** *(abbreviated* ***DVR****) is a local PID that is not a field.*

Equivalently, one can show this is equivalent to being a local Dedekind domain; then in an arbitrary DVR R, nonzero proper ideals factor uniquely into a product of maximal ideals (this is actually one way to *define* Dedekind domains), so since there is only one maximal ideal $\mathfrak{m}$, often written $\mathfrak{m}_R$ (which is nonzero since DVRs are not fields) then the set of ideals equals $\{\langle 0\rangle, \mathfrak{m}, \mathfrak{m}^2, \mathfrak{m}^3, \dots\}$ (where all are distinct by uniqueness of the factorization). R being a PID tells us we can even write this as $\{\langle 0\rangle, \langle \pi\rangle, \langle \pi^2\rangle, \langle \pi^3\rangle, \dots\}$ for some π generating $\mathfrak{m}$ - this suggests the following definition:

Definition 5. *A* ***uniformizer*** *for a DVR* R *is a generator* π *for its maximal ideal.*

So we often write $\mathfrak{m}_R$ as πR, where π is implicitly a uniformizer. Note the uniformizers are exactly the elements of $\mathfrak{m} - \mathfrak{m}^2$, and that relative to a fixed uniformizer π any $x \in R^\times$ can be written as $u\pi^n$ where u is a unit, $n \geq 0$, *and both are unique relative to* x.

Another few natural definitions:

Definition 6. *The* ***residue field*** *for a DVR* R *with maximal ideal* $\mathfrak{m}$ *is the field* $R/\mathfrak{m}$*; the* ***residue field*** *for the pair* $(\mathrm{frac}(R), R)$ *is defined as the same.*

If R is considered fixed and $K = \mathrm{frac}(R)$; we often write the residue field as k; similarly if $L = \mathrm{frac}(R)$, we write the residue field as l.

[1] Though when K has finite residue field k, it's preferred to take $c = 1/|k|$.

There is a natural bijective correspondence between discrete valuation subrings of a field K whose fraction field is K and discrete valuations on K. This is because, for a discrete valuation v on K, $\{x \in K : v(x) \geq 0\}$ is a DVR subring with fraction field K (and maximal ideal $\{x \in K : v(x) \geq 1\}$), and inversely such a DVR subring with maximal ideal $\mathfrak{m}$ gives rise to a valuation

$$v_{\mathfrak{m}}(x) \triangleq \begin{cases} \sup\{i \geq 0 : x \in \mathfrak{m}^i\}, & x \in R \\ \sup\{i \geq 0 : x^{-1} \in \mathfrak{m}^i\}, & x \notin R \end{cases}.$$

Note this is well-defined since any element of R can be written as $u\pi^n$ for a uniformizer π, and $x \in K = \mathrm{frac}(R)$ has $x \in R$ or $x^{-1} \in R$. Also note that these two processes of going from DVR to discrete valuation and vice versa are inverses.

This correspondence gives a natural translation of definition 5: the uniformizers for a DVR associated with a discrete valuation v are exactly the elements x with $v(x) = 1$, and in general the generators of $\mathfrak{m}^i$ are the elements with valuation i (for $i \geq 0$, and even for $i < 0$ if you define negative powers of $\mathfrak{m}$ appropriately - but then you need to talk about 'fractional ideals' and it's not worth to make this detour now). Another comment about uniformizers: we often say that a uniformizer for a DVR R is also one for its fraction field, and instead of saying π is a uniformizer for R or $\mathrm{frac}(R)$ we sometimes instead say that π *uniformizes* R or $\mathrm{frac}(R)$.

Definition 7. *Given a discretely valued field (K, v), the DVR subring associated with v is called the* ***ring of integers*** *of K and denoted $\mathcal{O}_K$ (or perhaps $\mathcal{O}_{K,v}$ when the valuation needs to be made clear). The maximal ideal of $\mathcal{O}_K$ is often written $\mathfrak{m}_K$.*

A discrete valuation v on a field K gives it a natural topology under which the field operations (addition, negation, multiplication and inversion) become continuous; such a field is called a *topological field*. The topology induced by the valuation can be described by simply giving a neighborhood basis of 0 and declaring that its additive translates are also open, as is doable for any topological group. So we declare that $\{x \in K : v(x) > n\}$ is open for all $n \in \mathbb{Z}$.

There is a certain condition on the topology of a discretely valued field that proves to be very useful:

Theorem 2. *A discretely valued field K is locally compact (w.r.t. its valuation topology) iff it is complete and its residue field is finite.*

Proof: If K is locally compact, then it has a compact subset C containing some open neighborhood of 0; since the $\mathfrak{m}^i$ form a neighborhood basis for 0, this means it contains some $\mathfrak{m}^k$. But the $\mathfrak{m}^k$ are clopen in K, so $\mathfrak{m}^k$ is also closed in C and so compact. Then $\pi^{-k}\mathfrak{m}^k = \mathcal{O}_K$ (with π a uniformizer of K) is compact. In particular, since the cosets of $\mathfrak{m}$ cover $\mathcal{O}_K$, and all are homeomorphic (and so open since $\mathfrak{m}$ is), then they must admit a finite cover, so that there are only finitely many cosets of $\mathfrak{m}$ in $\mathcal{O}_K$ (meaning $k = \mathcal{O}_K/\mathfrak{m}$ is finite). Additionally, given a cauchy sequence $(x_i)_1^\infty$ in K, $(v_K(x_i))_1^\infty$ must stabilize since v_K is continuous with discrete codomain, so there is $N, r \in \mathbb{Z}$ with $v_K(x_i) = r$ when $i \geq N$. But then $(\pi^{-r}x_i)_1^\infty$ is cauchy and eventually in $\mathcal{O}_K$, so it converges to some α, meaning x_i converges to $\pi^r\alpha$. So K is complete.

Conversely, if K is complete and $\mathcal{O}_K/\mathfrak{m}$ is finite, then $\mathcal{O}_K/\mathfrak{m}^i$ is finite too for any $i \geq 1$ (since multiplication by π^i gives a isomorphism of $\mathcal{O}_K/\mathfrak{m}$ with $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ for all $i \geq 1$, and we can multiply indexes). Then since $\mathcal{O}_{\widehat{K}} \cong \varprojlim \mathcal{O}_K/\mathfrak{m}^i$, it is profinite and so compact (should I explain this bahaha it's not hard but it's a detour I guess - this whole theorem is already sort of a detour but i'm just writing it cuz i like the proof); but $\mathcal{O}_{\widehat{K}} \cong \mathcal{O}_K$ by completeness, so $\mathcal{O}_K$ is compact. And since $\mathcal{O}_K$ contains the open neighborhood $\mathcal{O}_K$ of 0, K is locally compact at 0, and so at every point (since we can additively translate $\mathcal{O}_K$ as needed).

□

Definition 8. *Any discretely valued field satisfying the hypotheses of theorem 2 (or equivalently the conclusion) is called a **local field**.*

Nowadays it seems like people like to use a slightly more general definition, that a local field should instead be a complete discretely valued field with *perfect* residue field; in fact, this is the definition we will use in the Deligne section.

Complete discretely valued fields are quite nice in general, and they also allow their valuation to be 'extended' in a nice way to finite extensions, so it would be profitable to have a way to 'complete' a discretely valued field - but in order to explore this, we need to first define some basic concepts related to ramification.

2.2 Ramification basics

If A is a Dedekind domain (remember that this means nonzero A-ideals factor uniquely as a product of prime ideals) and L is a finite extension of $K \triangleq \mathrm{frac}(A)$, then the integral closure $B \triangleq \overline{A}^L$ of A in L is also a Dedekind domain - let's keep this setup throughout this section. Given a nonzero prime A-ideal $\mathfrak{p}$, we can uniquely factorize $\mathfrak{p}B$ as a product of nonzero prime B-ideals. If $\mathfrak{p}B = \prod_1^r \mathfrak{P}_i^{e_i}$, where $e_i \geq 1$ for all i, then the $\mathfrak{P}_i$ are exactly the prime B-ideals lying above $\mathfrak{p}$ (i.e. whose intersection with A is $\mathfrak{p}$). Then we can make the following definitions:

Definition 9. *Let* $\mathfrak{p}B = \prod_1^r \mathfrak{P}_i^{e_i}$.

- *The **ramification index** e_i is defined as the e_i in the above equation.*
- *The **residue degree** f_i is defined as $[B/\mathfrak{P}_i : A/\mathfrak{p}]$* [2]

If $\mathfrak{P} = \mathfrak{P}_i$, we also write e_i as $e_{\mathfrak{P}/\mathfrak{p}}$ and f_i as $f_{\mathfrak{P}/\mathfrak{p}}$.

- *If $e_i > 1$ for some i, we say $\mathfrak{p}$ **ramifies** in L.*
- *If $e_i = 1$ and $f_i = 1$, we say $\mathfrak{p}$ **splits completely** in L.*
- *If $e_i = 1$ and $r = 1$, we say $\mathfrak{p}$ **remains prime** in L.*

[2] Note this embedding makes sense since $\mathfrak{P}_i = \mathfrak{p} \cap A$ (so that $\mathfrak{p}$ is actually the kernel of the map $A \hookrightarrow B \twoheadrightarrow B/\mathfrak{P}_i$)

Theorem 3. *If L/K is also galois, then e_i, f_i are independent of i (in this case, we usually omit the subscript and just write e, f instead).*

Proof: This is essentially because the action $\mathrm{gal}(L/K) \curvearrowright \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ via element-wise images (which is a well-defined action since any $\sigma \in \mathrm{gal}(L/K)$ fixes B (it preserves polynomials over A) and fixes A pointwise and actually maps a prime ideal lying above $\mathfrak{p}$ to a prime ideal lying above $\mathfrak{p}$) is transitive, since given $j \neq k$ and $x \in P_j$, we have

$$N^L_{\mathrm{frac}(A)}(x) = x \cdot \prod_{\mathbb{1}_L \neq \sigma \in \mathrm{gal}(L/K)} \sigma(x) \in A \cap P_j = \mathfrak{p} \subseteq P_k$$

so that $\sigma(x) \in P_k$ for some σ by primality of P_k.

□

Theorem 4. $\sum_{i=1}^r e_{\mathfrak{P}_i/\mathfrak{p}} f_{\mathfrak{P}_i/\mathfrak{p}} = [L : K]$*; in particular, if L/K is galois then $efr = [L : K]$.*

Proof: I will omit the details, but the idea is to show $[B/\mathfrak{p}B : A/\mathfrak{p}] = [L : K]$ and then use that $B/\mathfrak{p}B \cong \prod_1^r (B/\mathfrak{P}_i)^{e_i}$ (via the Chinese Remainder Theorem).

In the case that K, L are discretely valued, $\mathcal{O}_K$ and $\mathcal{O}_L$ have only one nonzero prime ideal, so $\mathfrak{m}_K\mathcal{O}_L$ factors as $\mathfrak{m}_L^{e_K^L}$ for some e_K^L, which we call the ramification index of the extension L/K. Analogously, we call $[\mathcal{O}_L/\mathfrak{m}_L : \mathcal{O}_K/\mathfrak{m}_K] = [l : k]$ the residue degree f_K^L of the extension L/K. I'll alternatively write these as $e_{L/K}$, $f_{L/K}$ respectively, depending on which one looks better in a given context (lol).

Now we can get back to completing and extending discretely valued fields!

2.3 Completion

With the familiar construction using Cauchy sequences, one can topologically complete a discretely valued field K (with respect to its valuation topology); further, one can check that the result $\widehat{K}$ has the structure of a topological field.given by applying the operations of K element-wise to sequences. Additionally, one can check that this completion topology is induced by an extension of v: define $\overline{v}((x_i)_1^\infty) \triangleq \lim_{n\to\infty} v(x_n)$ (which is well-defined because v is continuous, if we give $\mathbb{Z} \cup \{\infty\}$ the order topology); then this is a discrete valuation, which extends v if we consider K embedded in $\widehat{K}$ (via $x \mapsto (x)_1^\infty$) since $\widehat{v}((x)_1^\infty) = \lim_{n\to\infty} v(x) = v(x)$ for all constant sequences $(x)_1^\infty$.

We have a few useful facts, summarized in the following theorem:

Theorem 5.

(1) $\mathcal{O}_{\widehat{K}} = \overline{\mathcal{O}_K} = \varprojlim \mathcal{O}_{\widehat{K}}/\pi^n\mathcal{O}_{\widehat{K}}$ *(i.e. the DVR associated with $\widehat{v}$ is the closure of the one associated with v)*

(2) *any uniformizer for $\mathcal{O}_K$ is also one for $\mathcal{O}_{\widehat{K}}$ (i.e. if $v(x) = 1$, then $\widehat{v}(x) = 1$) - this also means that if $\mathfrak{m}_{\mathcal{O}_K} = \pi\mathcal{O}_K$, then $\mathfrak{m}_{\mathcal{O}_{\widehat{K}}} = \pi\mathcal{O}_{\widehat{K}}$, and that $\pi\mathcal{O}_{\widehat{K}} \cap K = \pi\mathcal{O}_K$.*

(3) $\widehat{\mathcal{O}_K}/\pi\widehat{\mathcal{O}_K} \cong \mathcal{O}_K/\pi\mathcal{O}_K$

Proof: (1) is because a uniformizer π for $\mathcal{O}_K$ is also uniformizes $\widehat{K}$, so that the $\pi^i\mathcal{O}_{\widehat{K}}$ form a neighborhood basis for $\mathcal{O}_{\widehat{K}}$ at 0, as we've seen in general; (3) is because the composition $\mathcal{O}_K \hookrightarrow \widehat{\mathcal{O}_K} \twoheadrightarrow \widehat{\mathcal{O}_K}/\pi\widehat{\mathcal{O}_K}$ has kernel $\pi\mathcal{O}_K$ (since for $x \in \mathcal{O}_K$ we have $x \in \pi\widehat{\mathcal{O}_K} \Leftrightarrow \widehat{v}(x) = 1 \Leftrightarrow v(x) = 1 \Leftrightarrow x \in \mathcal{O}_K$) and is surjective. (maybe add more details but idk if it's worth)

□

2.4 Extension

Given L/K, we say that v_L *extends* v_K iff $v_L|_K$ differs from v_K multiplicatively by a constant (which - assuming as usual that our valuations have image $\mathbb{Z} \cup \{\infty\}$ - must necessarily be e_K^L, since if π uniformizes K then $\pi\mathcal{O}_L = \mathfrak{m}_L^{e_K^L}$ and so $v_L(\pi) = e_K^L$).

Theorem 6. *If K is a complete discretely valued field, and L is a finite extension of K, then:*

- *$\mathcal{O}_L \triangleq \overline{\mathcal{O}_K}^L$ (denoting the integral closure of $\mathcal{O}_K$ in L) is a DVR and a free $\mathcal{O}_K$-module of rank $[L : K]$*
- *the valuation v_L that $\mathcal{O}_L$ induces on L makes L complete*
- *the valuation v_L is the unique one on L extending v_K (talk about what this means; I may have to define the ramification index earlier for it to be satisfying?)*

Proof: I will omit it, but the main idea is to use 'dévissage' to break into the separable / purely inseparable cases and combine appropriately.

We again get $e_{L/K}f_{L/K} = [L : K]$ in this case (we can't directly apply the discussion in 2.2 to get this, since there we assumed our extension to be separable, but it turns out that $\mathcal{O}_L$ being a finitely generated $\mathcal{O}_K$-module is suffices anyway). We can additionally get an explicit form of the valuation on L:

Theorem 7. *If K is a complete discretely valued field, and L is a finite extension of K, then $v_L(x) = v_K(N_K^L(x))/f_{L/K}$.*

Proof: Let $N \triangleq \mathrm{spl}(L/K)$ be the normal closure of L/K; it is a finite extension of both L and K, so v_N extends both v_K and v_L uniquely. Since $v_N \circ \sigma$ is also a valuation on N extending v_K for any $\sigma \in \mathrm{gal}(N/K)$, it must equal v_N, and so since any conjugate of $x \in L$ can be written $\sigma(x)$ for some $\mathrm{gal}(N/K)$ we have $v_N(x) = v_N(\sigma(x))$.

Then

$$
\begin{aligned}
v_K\left(\prod_{\sigma\in\mathrm{gal}(N/K)}\sigma(x)\right) &= e_{N/K}^{-1}v_N\left(\prod_{\sigma\in\mathrm{gal}(N/K)}\sigma(x)\right)\\
&= e_{N/K}^{-1}\sum_{\sigma\in\mathrm{gal}(N/K)}v_N(\sigma(x))\\
&= e_{N/K}^{-1}\sum_{\sigma\in\mathrm{gal}(N/K)}v_N(x)\\
&= \frac{|\mathrm{gal}(N/K)|}{e_{N/K}}v_N(x)\\
&= \frac{|\mathrm{gal}(N/K)|}{e_{N/K}}e_{N/L}v_L(x)\\
&= f_{N/K}v_N(x)\\
&= f_{N/K}e_{N/L}v_L(x)
\end{aligned}
$$

(actually i'm kind of confused where $f_{L/K}$ comes from skull emoji cuz it should equal $f_{N/K}e_{N/L}$ iff $e_{N/L}f_{N/L} = 1$ but this shouldn't be able to hold if $L \neq N$?)

$\square$

Here is an important comment about normalization of valuations in extensions: given L/K finite with K complete and discretely valued, the valuations v_K and v_L are related via $v_K(x) = e_K^L v_L(x)$ for all $x \in K$; the result is that v_L may not actually equal v_K on K, though they differ multiplicatively by a constant. Sometimes we wish to circumvent this by considering the valuation $v \triangleq v_L/e_K^L$; this is a singular valuation on all of L such that $v(\pi) = 1$ when π uniformizes K. In this case we say v is the valuation of L <u>normalized for K</u>. In contrast, if we take our valuation instead as just $v \triangleq v_L$, this is a singular valuation on all of L such that $v(\pi) = 1$ when π uniformizes L; in this case we say v is the valuation of L <u>normalized for L</u>.

We can really just do the same thing for arbitrary subextensions E between K and L; we say v is the valuation on L <u>normalized for E</u> iff $v = v_L/e_E^L$ (i.e. iff v differs from v_L multiplicatively by a constant, and $v(\pi) = 1$ when π normalizes E).

One consequence of all this is that we can consider a valuation on the algebraic closure $\overline{K}$, gotten by essentially taking the union over all valuations of finite extensions of K normalized for K (so in particular this valuation on $\overline{K}$ is normalized for K).

(ngl this yappy as hell pls cut this down in the final draft lolllll)

2.5 Completion and extension: all together now!

(mainly just wanna copy paste that one theorem from Serre)

2.6 Generators for extensions

Here I'll go on a brief detour to showcase two very useful facts relating to how a lower ring of integers 'downstairs' can generate a higher one 'upstairs' (which will be used a lot later):

Theorem 8. *If L/K is a finite extension of discretely valued fields, with separable residue field extension, then $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$.*

Proof: (it's an instructive proof so I should write out the details later, also cuz i wanna try and fill in the nakayama part lol)

It is sometimes useful to be able to guarantee α is a uniformizer (this will provide a nice alternative characterization of the higher ramification groups in 3.2); we can get this with slightly different hypotheses (remember that an *Eisenstein polynomial* over K is one where all coefficients but the leading one lie in $\mathfrak{m}_K$ and the constant coefficient does not lie in $\mathfrak{m}_K^2$):

Theorem 9. *If L/K is a finite totally ramified extension of discretely valued fields, then $\mathcal{O}_L = \mathcal{O}_K[\pi]$ for some uniformizer $\pi \in \mathcal{O}_L$ (which also has an Eisenstein irreducible polynomial over K).*

Proof: (it's a bit long but i guess i should at least sketch it later though)

This theorem can actually sort of be phrased as an if and only if, though I don't think we will need it (but it's still fun so I'll write it):

Theorem 10. *Let K be a discretely valued field, with v the valuation on $\overline{K}$ normalized for K; if no roots of $f(T) \in \mathcal{O}_K[T]$ have valuation 0, then $f(T)$ is an Eisenstein polynomial iff it is irreducible and the extension generated by any one of its roots is totally ramified, having said root as a uniformizer.*

Proof: ($\Leftarrow$) was done in theorem 9, so I'll do ($\Rightarrow$): Let $f(T)$ be Eisenstein with roots $\alpha_1, \ldots, \alpha_n$ and consider the valuation v on the splitting field of $f(T)$ over K, normalized for K. We have that $\prod_{i=1}^{n} \alpha_i$ is the constant coefficient of $f(T)$ up to sign, and so

$$1 = v\left(\prod_{i=1}^{n} \alpha_i\right) = \sum_{i=1}^{n} v(\alpha_i).$$

Since $v(\alpha_i) > 0$ for all i (they have valuation at least 0 since they are integral over $\mathcal{O}_K$, and they don't have valuation 0 by hypothesis), then

$$v(\alpha_i) \geq \frac{1}{e_K^{K(\alpha_i)}} \geq \frac{1}{n}$$

for all i. For both the previous lines to hold, we must have $v(\alpha_i) = 1/n$ for all i, so that $n = e_K^{K(\alpha_i)}$, implying (1) that $n = e_K^{K(\alpha_i)} \leq [K(\alpha_i) : K] \leq n$ i.e. $[K(\alpha_i) : K] = \deg(f)$ and so $f = \mathrm{irr}(\alpha_i, K)$ and (2) that $K(\alpha_i)/K$ is totally ramified, with α_i uniformizing (since it has valuation $1/e_K^{K(\alpha_i)}$).

□

---

3 Higher Ramification Groups

Throughout this section, I will assume we have a finite galois extension L/K of discretely valued fields with separable residue field extension l/k, where L has valuation v_L extending the valuation v_K of K. Remember that for $x \in K$, we have $v_L(x) = v_K(x)/e_K^L$. Additionally, using the previous section, write $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Assume from here that this generator α is fixed.

Definition 10.

- *The **inertia group** $G_0(L/K)$ of L/K (written G_0 if the extension is clear) is the subgroup*

$$\{\sigma \in \mathrm{gal}(L/K) : (\forall x \in \mathcal{O}_L)[\sigma(x) \equiv x \bmod \mathfrak{m}_L]\}$$

  of $\mathrm{gal}(L/K)$; it is sometimes denoted $\mathcal{I}_{L/K}$.

- *The **inertia field** of L/K is L_{G_0}, the fixed field of G_0 under the Galois correspondence; it is sometimes denoted $L_{\mathcal{I}}$.*

$L_{\mathcal{I}}$ is the maximal unramified subextension L of K, meaning if $K \leq E \leq L$ then $\mathfrak{m}_K$ does not ramify in E iff $E \subseteq L_{G_0}$.

Definition 11. *The i**-th ramification group** of L/K (for $i \geq 0$) is defined as*

$$G_i(L/K) \triangleq \{\sigma \in \mathrm{gal}(L/K) : (\forall x \in \mathcal{O}_L)[\sigma(x) \equiv x \bmod \mathfrak{m}_L^{i+1}]\}.$$

We also define $G_{-1}(L/K) \triangleq \mathrm{gal}(L/K)$, and as before we simply write G_i if the extension is clear.

Note that the 0-th ramification group of L/K is the same as its inertia group. The ramification groups can also be thought about in a slightly different way:

Definition 12. *Given $\sigma \in \mathrm{gal}(L/K)$, let $i_L^K(\sigma) \triangleq v_L(\sigma(\alpha) - \alpha)$.*

The upshot is that it's enough to consider just $\sigma(x) - x$ for $x = \alpha$, instead of for all $x \in \mathcal{O}_L$. The fact that i_L^K determines our ramification groups and does not depend on our choice of generator α for $\mathcal{O}_L$ over $\mathcal{O}_K$ is shown by the following theorem:

Theorem 11. *$G_i(L/K) = \{\sigma \in \mathrm{gal}(L/K) : i_L^K(\sigma) \geq i+1\}$; in other words,*

$$i_K^L(\sigma) \geq i+1 \Leftrightarrow (\forall x \in \mathcal{O}_L)[v_L(\sigma(x) - x) \geq i+1].$$

Proof: For any $r \in \mathbb{N}$ and $a_0, \ldots, a_r \in \mathcal{O}_K$ we have

$$\begin{aligned} v_L\left(\sigma\left(\sum_0^r a_i\alpha^i\right) - \sum_0^r a_i\alpha^i\right) &= v_L\left(\sum_1^r a_i(\sigma(\alpha)^i - \alpha^i)\right) \\ &= v_L\left(\sum_{i=1}^r a_i(\sigma(\alpha)-\alpha)\left(\sum_{j=0}^{i-1}\sigma(\alpha)^j\alpha^{r-1-j}\right)\right) \\ &= v_L(\sigma(\alpha)-\alpha) + v_L\left(\sum_{i=1}^r a_i\left(\sum_{j=0}^{i-1}\sigma(\alpha)^j\alpha^{r-1-j}\right)\right) \\ &\geq v_L(\sigma(\alpha)-\alpha). \end{aligned}$$

The last step is because $\sum_{i=1}^r a_i\left(\sum_{j=0}^{i-1}\sigma(\alpha)^j\alpha^{r-1-j}\right) \in \mathcal{O}_L$.

□

Here is another essential property of the ramification groups:

Theorem 12. *$G_i \trianglelefteq \mathrm{gal}(L/K)$ for all i, and there is some N such that G_i is trivial for all $i \geq N$; in summary; the G_i form a normal series for $\mathrm{gal}(L/K)$.*

Proof: Normality is because if $\sigma \in \mathrm{gal}(L/K)$ and $\tau \in G_i$, then we have $v_L(\tau(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha)) \geq i+1$, i.e. $\tau(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha) \in \mathfrak{m}_L^{i+1}$; but since $\sigma(\mathfrak{m}_L) = \mathfrak{m}_L$ (since it must map maximal ideals to maximal ideals), then $\sigma(\mathfrak{m}_L^{i+1}) = \mathfrak{m}_L^{i+1}$, so that

$$\tau(\sigma^{-1}(\alpha)) - \sigma^{-1}(\alpha) \in \mathfrak{m}_L^{i+1} \implies \sigma(\tau(\sigma^{-1}(\alpha))) - \alpha \in \mathfrak{m}_L^{i+1}$$

and so $\sigma \circ \tau \circ \sigma^{-1} \in G_i$.

The G_i stabilize because $\mathrm{gal}(L/K)$ is finite by hypothesis, so we can take N with $N \geq i_K^L(\sigma)$ for all $\sigma \in \mathrm{gal}(L/K) - \{\mathbb{1}_L\}$ (since for all nontrivial σ, $i_K^L(\sigma)$ is finite); then for each such σ we have $\sigma \notin G_N$ since $i_K^L(\sigma) \leq N < N+1$.

□

Let's now turn our attention towards studying how the ramification groups behave in towers; i.e. let's introduce an intermediate field E with $K \leq E \leq L$ and try to describe how the ramification groups of L/E and possibly E/K (if E is galois over K) interact with the ones for L/K. For L/E, the situation is quite simple:

Theorem 13. $G_i(L/E) = G_i(L/K) \cap \mathrm{gal}(L/E)$ *for all* $i \geq -1$.

Proof: Since our generator α for $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra is also a generator for it as a $\mathcal{O}_E$-algebra, then we have that, for any $\sigma \in \mathrm{gal}(L/E)$, $i_E^L(\sigma) = v_L(\sigma(\alpha) - \alpha) = i_K^L(\sigma)$. In other words, $i_E^L = i_K^L|_{\mathrm{gal}(L/E)}$, and so

$$\begin{aligned} \sigma \in G_i(L/E) &\Leftrightarrow \sigma \in \mathrm{gal}(L/E) \wedge i_E^L(\sigma) \geq i+1 \\ &\Leftrightarrow \sigma \in \mathrm{gal}(L/E) \wedge i_K^L(\sigma) \geq i+1 \\ &\Leftrightarrow \sigma \in \mathrm{gal}(L/E) \cap G_i(L/K). \end{aligned}$$

□

In particular, if $E = L_{G_0}$ (the inertia field of L/K from definition 10), then $\mathrm{gal}(L/E) = \mathrm{gal}(L/L_{G_0}) = G_0(L/K)$ by definition, so that the above theorem tells us $G_i(L/L_{G_0}) = G_i(L/K) \cap G_0(L/K) = G_i(L/K)$ when $i \geq 0$. In words, the ramification groups for L/K and L/L_{G_0} are the exact same (excluding the -1-th ramification group, which is just the whole galois group anyway).

For E/K, the situation is not so nice; we know that $G_{-1}(E/K) = \mathrm{gal}(E/K) \cong \mathrm{gal}(L/K)/\,\mathrm{gal}(L/E)$ from basic Galois theory, but the other ramification groups (i.e. $G_i(E/K)$ with $i \geq 0$) don't have so nice a description - the best we can do is the following:

Theorem 14. *Identify* $\mathrm{gal}(E/K)$ *with* $\mathrm{gal}(L/K)/\,\mathrm{gal}(L/E)$ *implicitly in the natural way; then*

$$i_K^E(\sigma\,\mathrm{gal}(E/K)) = \sum_{\tau \in \mathrm{gal}(L/K) : \tau\sigma^{-1} \in \mathrm{gal}(E/K)} i_K^L(\tau)$$

Proof: (it's not very fun :(but maybe i should sketch it)

There is a better way to express the relationship between the ramification groups of L/K and E/K, but it requires us to 'raise' our perspective, so to speak.

3.1 Hasse-Herbrand transition function

Let's keep the same notation and conventions we've been using, and make a couple 'out-of-pocket' definitions:

Definition 13. *For* $t \geq -1$*, let* $G_t(L/K) \triangleq G_{\lceil t \rceil}(L/K)$ *(so that* $\sigma \in G_t(L/K) \Leftrightarrow v_L(\sigma(\alpha) - \alpha) \geq t+1$ *holds in this case too).*

Definition 14. *The* ***Hasse-Herbrand transition function*** *of* L/K *is* $\varphi_K^L : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ *given by*

$$\varphi_K^L(t) \triangleq \int_0^t \frac{|G_t(L/K)|}{|\,\mathrm{gal}(L/K)|}\, dt.$$

The integral may seem a bit strange - I only write it because everyone else insists on doing so in the literature - but it's really just an overly cutesy way to define a piecewise linear function whose pieces are the integer intervals $[i, i+1]$ for $i \geq -1$, and whose slope on $[i, i+1]$ is simply the size of $G_{i+1}(L/K)$ normalized by the size of the whole galois group. It's literally nothing deeper than that. If we want, we can write out a very explicit formula:

$$\varphi(t) = |G_0|^{-1} \left(\sum_{i=1}^{\lfloor t \rfloor} |G_i| + (t - \lfloor t \rfloor)|G_{\lceil t \rceil}| \right).$$

In particular, this formula makes it clear that if $\varphi(t) \in \mathbb{Z}$, then $t \in \mathbb{Z}$ (because every $|G_j|$ divides every $|G_i|$ for $i \leq j$).

Note that $(\varphi_K^L)' = 1$ on $(-1, 0)$, and if $G_i(L/K)$ is trivial for $i \geq N$ then $(\varphi_K^L)' = |\mathrm{gal}(L/K)|^{-1}$ on (N, ∞). Also note that φ is a homeomorphism $[-1, \infty) \to [-1, \infty)$, so that it has a well-defined inverse ψ, which we will use to 'shift' our indexing for the ramification groups.

Definition 15. *Given $s \in [-1, \infty)$, let $G^s \triangleq G_{\psi(s)}$. The G^s are said to be the ramification groups of L/K in the **upper numbering**.*

Equivalently, we have $G_t = G^{\varphi(t)}$ for $t \in [-1, \infty)$. Symmetrically, the G_t are said to be in the **lower numbering**.

Theorem 15. *If $K \leq E \leq L$ with E/K galois, then $G^s(E/K) = G^s(L/K)\,\mathrm{gal}(L/E)/\,\mathrm{gal}(L/E)$.*

Proof: (i have notes but it's a bit long so maybe i'll summarize it?)

Serre sets up his notation so that he can write this statement very cutely as $(G/H)^s = G^s H/H$, but I write it as I did above for transparency's sake.

3.2 Factors of the ramification series

Keep the same conventions as before, but let $\mathfrak{m}$ denote $\mathfrak{m}_L$ throughout this section (because I write it way too many times in the proofs to justify putting the subscripts everywhere lol).

Since we've seen that the $G_i(L/K)$ form a normal series for the whole galois group, one natural question is what the factor groups of this series look like, since this should give us information about the G_i.

The first step is to reframe some things we've done previously in terms of multiplication. Namely, we said $\sigma \in G_i(L/K) \Leftrightarrow \sigma(\alpha) \equiv \alpha \bmod \mathfrak{m}^{i+1}$ for a generator α of $\mathcal{O}_L$ over $\mathcal{O}_K$; if we instead look at L/L_{G_0}, which we know is totally ramified, then we can take a uniformizing generator π of $\mathcal{O}_L$ over $\mathcal{O}_{L_{G_0}}$ by theorem 9. In this case we still have $\sigma \in G_i(L/K) \Leftrightarrow \sigma(\pi) \equiv \pi \bmod \mathfrak{m}^{i+1}$, and - using the fact that π has valuation $1(!)$ - this latter condition is equivalent to

$$\frac{\sigma(\pi)}{\pi} \equiv 1 \bmod \mathfrak{m}^i.$$

In other words, fixing the valuation of our generator has allowed us to control how much valuation we 'lose' when multiplying / dividing by it, which is what permits us to reframe things multiplicatively here.

We saw previously in theorem 13 that $G_i(L/K) = G_i(L/L_{G_0})$ for $i \geq 0$, so restricting to the extension L/L_{G_0} makes no difference ($G_{-1}(L/K)$ was always just the whole galois group anyway, so we are not losing generality here).

So we should be all set to introduce the unit groups now!

Definition 16. *Let $U_L^{(0)} \triangleq \mathcal{O}_L^\times$ and $U_L^{(i)} \triangleq 1 + \mathfrak{m}_L^i$ for $i \geq 1$.*

These $U_L^{(i)}$ form a descending neighborhood basis for 1 (i.e. $U_L^{(0)} \geq U_L^{(1)} \geq U_L^{(2)} \geq \dots$), and are all complete, so $\mathcal{O}_L^\times \cong \varprojlim \mathcal{O}_L^\times / U_L^{(i)}$ (?? lol i need to remember what source has this thm), and they have quite a nice structure, as the following two theorems show: (note: i should actually proofread the proofs cuz i just kinda typed them out stream of consciousness style but i don't have time rn)

Theorem 16. $\mathcal{O}_L^\times / U_L^{(1)} \cong \ell^\times$.

Proof: We can just define a map explicitly, via $x(1+\mathfrak{m}) \mapsto x + \mathfrak{m}$; this is well-defined because $x \in \mathcal{O}_L^\times$ implies $x \notin \mathfrak{m}$, so that $x + \mathfrak{m} \neq 0 + \mathfrak{m}$ (and so actually lies in $\ell^\times$), and it's clear this is a surjective homomorphism. For injectivity, note that $x + \mathfrak{m} = y + \mathfrak{m} \Leftrightarrow xy^{-1} \in 1 + \mathfrak{m} \Leftrightarrow x(1+\mathfrak{m}) = y(1+\mathfrak{m})$.

□

Theorem 17. $U_L^{(i)} / U_L^{(i+1)} \cong (\ell, +)$ *for* $i \geq 1$.

Proof: First we define a map $U_L^{(i)}/U_L^{(i+1)} \to \mathfrak{m}^i/\mathfrak{m}^{i+1}$, via $x(1+\mathfrak{m}^{i+1}) \mapsto (x-1) + \mathfrak{m}^{i+1}$ - note that this is a homomorphism because for $x, y \in 1 + \mathfrak{m}^i$ we have $(xy - 1) + \mathfrak{m}^{i+1} = (x - 1 + y - 1) + \mathfrak{m}^{i+1}$) (as $xy - x - y + 1 = (x-1)(y-1) \in \mathfrak{m}^{i+1}$, since $x - 1, y - 1 \in \mathfrak{m}^i$), and is injective since $y \in 1 + \mathfrak{m}^i$ implies y is a unit in $\mathcal{O}_L$, so that

$$\begin{aligned}
(x-1) + \mathfrak{m}^{i+1} = (y-1) + \mathfrak{m}^{i+1} &\implies x - y \in \mathfrak{m}^{i+1} \\
&\implies \frac{x}{y} - 1 \in \mathfrak{m}^{i+1} \\
&\implies xy^{-1} \in 1 + \mathfrak{m}^{i+1} \\
&\implies x(1+\mathfrak{m}^{i+1}) = y(1+\mathfrak{m}^{i+1}).
\end{aligned}$$

And surjectivity is clear.

Now let's show that $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is an ℓ-vector space, since the homomorphism $\Theta : \mathcal{O}_L \to \mathrm{aut}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$ given by $\Theta(a)(x + \mathfrak{m}^{i+1}) \triangleq ax + \mathfrak{m}^{i+1}$ is constant on every coset of $\mathfrak{m}$ (as $a \in \mathfrak{m} \implies ax \in \mathfrak{m}^{i+1} \implies ax + \mathfrak{m}^{i+1} = 0$), so it induces an action $\mathcal{O}_L/\mathfrak{m} \to \mathrm{aut}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$.

Additionally, since $1+\mathfrak{m}^{i+1}$ generates $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ (as $x+\mathfrak{m}^{i+1} = (x+\mathfrak{m})(1+\mathfrak{m}^{i+1})$), then $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is a 1-dimensional vector space over ℓ, and so is isomorphic to $(\ell,+)$ as a group. So in summary we have $U_L^{(i)}/U_L^{(i+1)} \cong \mathfrak{m}^i/\mathfrak{m}^{i+1} \cong (\ell,+)$.

□

The upshot of understanding the structure of the $U_L^{(i)}/U_L^{(i+1)}$ is that we can embed the factors G_i/G_{i+1} in them (via the map $\sigma \mapsto \sigma(\pi)/\pi : G_i(L/K) \to 1+\mathfrak{m}^i$ - note this is well-defined since $\sigma \in G_i(L/K) \implies \sigma(\pi) \equiv \pi \bmod \mathfrak{m}^{i+1} \implies \sigma(\pi)/\pi \equiv 1 \bmod \mathfrak{m}^{i+1}$), and so we get information about them from the above two theorems.

For example, if $\mathrm{char}(\ell) = 0$, then finite subgroups of $(\ell,+)$ are trivial, and so G_i/G_{i+1} is trivial for $i \geq 1$ - but since G_N is also trivial for large N, by multiplying orders / indexes we get that G_i is trivial for $i \geq 1$. Note this implies that G_0 is cyclic, since G_1 being trivial means $G_0 \cong G_0/G_1$ embeds into $\mathcal{O}_L^\times/U_L^{(1)} \cong \ell^\times$.

And if $\mathrm{char}(\ell) = p$, then subgroups of $(\ell,+)$ are vector spaces over $\mathbb{F}_p$, and so $G_i/G_{i+1} \leq (\mathbb{F}_{p^k},+) \cong \mathbb{Z}_p^k$ meaning it is elementary abelian. Since G_N is trivial for large N, again by multiplying orders / indexes we get that the G_i themselves are all p-groups (for $i \geq 1$).

4 Deligne stuff

First we need a few preliminary things, which may seem a bit random but will come into play later. The very first is that throughout this section, a *local field* will mean a complete discretely valued field with perfect residue field (not necessarily finite). The second is the following:

Definition 17. *Given an R-module M, let $M^{\otimes n}$ for $n > 0$ denote the tensor product $\bigotimes_{i=1}^{n} M$; let $M^{\otimes 0}$ denote R; let $M^{\otimes n}$ for $n < 0$ denote $\hom(M^{\otimes n}, R)$.*

The direct sum $\bigoplus_{n\in\mathbb{Z}} M^{\otimes n}$ has a natural R-algebra structure given by tensoring / function application. To convey the basic idea, for elements that have only one pure tensor in one component, we have, for $r, s > 0$:

$$(x_1 \otimes \cdots \otimes x_r)(x_{r+1} \otimes \cdots \otimes x_{r+s}) \triangleq x_1 \otimes \cdots \otimes x_{r+s}$$

and if $\varphi \in \hom(M^{\otimes r}, R)$, and $s < r$, then

$$\varphi \cdot (x_1 \otimes \cdots \otimes x_s) \triangleq \varphi(x_1, \ldots, x_s, -, \ldots, -)$$

and if $r < s$ then

$$\varphi \cdot (x_1 \otimes \cdots \otimes x_s) \triangleq \varphi(x_1, \ldots, x_r)(x_{r+1} \otimes \cdots \otimes x_{r+s})$$

and so on. I've only sketched the actual algebraic structure, but a better (more complete) picture can be gotten by the fact that, if M is free of rank 1 over R (which it always will be throughout this section), then $\bigotimes_{n\in\mathbb{Z}} M^{\otimes n}$ is isomorphic to $R[T, T^{-1}]$ via fixing a generator of M over R and mapping it to T (in fact, I suppose you could define it this way).

Definition 18. *A* ***truncated valuation ring*** *is a local principal ideal ring R whose maximal ideal $\mathfrak{m}$ is nilpotent. The smallest s such that $\mathfrak{m}^s = 0$ is the* ***length*** *of R and denoted $\lg(R)$.*

Note that because the generator of the maximal ideal is nilpotent, any truncated valuation ring is necessarily *not* an integral domain and so not a PID, even though all ideals are generated by one element.

It can be shown that an equivalent definition of a truncated valuation ring is a quotient of a complete DVR R by a power $\mathfrak{m}^s$ of its maximal ideal (where $\lg(R/\mathfrak{m}^s)$ will equal s necessarily). Then truncated valuation rings inherit a 'truncated valuation' from the ring of which they are a quotient; the truncated valuation of $R/\mathfrak{m}^s$ takes values in $[0, s-1]$, and is truncated in the sense that if for $x \in R$ we have $v_{\mathfrak{m}}(x) \in [0, s-1]$, then the truncated valuation at x equals $v_{\mathfrak{m}}(x)$, and if $v_{\mathfrak{m}}(x) \geq s$ then the truncated valuation at x is ∞.

Definition 19. *We will reserve the term "triple" for a tuple (R, M, ε) where R is a truncated valuation ring, M is a free R-module of rank 1, and $\varepsilon : R \to \mathfrak{m}_R$ is a surjective homomorphism.*

If K is a local field, for every $s \in \mathbb{Z}_+$ we can associate with it the triple $\mathrm{tr}_s(K) \triangleq (\mathcal{O}_K/\mathfrak{m}_K^s, \mathfrak{m}_K/\mathfrak{m}_K^{s+1}, \varepsilon : \mathfrak{m}_K/\mathfrak{m}_K^{s+1} \to \mathfrak{m}_K/\mathfrak{m}_K^s)$ (where ε is the natural map $x + \mathfrak{m}_K^{s+1} \mapsto x + \mathfrak{m}_K^s$)

Using the fact that any truncated valuation ring is a quotient of a complete DVR R by a power $\mathfrak{m}^s$ of its maximal ideal, it can be shown that every triple can be realized as $\mathrm{tr}_s(K)$ for some $s \in \mathbb{Z}_+$ and some local field K.

Definition 20. *Given a triple (R, M, ε), if $r < s$ then $\varepsilon_{r,s}$ is the map $M^{\otimes s} \to M^{\otimes r}$ determined by $\varepsilon_{r,s}(\alpha^{\otimes s}) \triangleq \varepsilon(\alpha)^{s-r}\alpha^{\otimes r}$, where α is a generator of M over R (so that $\alpha^{\otimes s}$ is one of $M^{\otimes s}$ over R).*

Note this map is independent of the generator we choose, since if $\beta = u\alpha$ (so that $\beta^{\otimes s} = u^s\alpha^{\otimes s}$) then $\varepsilon(\beta)^{s-r}\beta^{\otimes r} = u^s\varepsilon(\alpha)^{s-r}\alpha^{\otimes r}$.

Definition 21. *Let $\mathcal{T}$ be the category of triples, with morphisms $(R, M, \varepsilon) \to (R', M', \varepsilon')$ as tuples $(\varphi : R \to R', \eta : M \to M'^{\otimes k}, k)$ (where $k \geq 1$, φ and η are ring / R-module homomorphisms (with M' and so $M'^{\otimes e}$ given the R-module structure induced by φ via 'restriction of scalars'), and η maps a generator of M to one of $M'^{\otimes e}$) so that the following diagram commutes:*

$$\begin{tikzcd} M \arrow[r, "\eta"] \arrow[d, "\varepsilon"] & M'^{\otimes e} \arrow[d, "\varepsilon_{0,e}"] \\ R \arrow[r, "\varphi"] & R' \end{tikzcd}$$

Composition of morphisms is given $(\varphi', \eta', e') \circ (\varphi, \eta, e) \triangleq (\varphi' \circ \varphi, \eta'^{\otimes e} \circ \eta, e'e)$.

η induces an isomorphism $\overline{\eta} : M \otimes_R R' \hookrightarrow\!\!\!\!\!\rightarrow M'^{\otimes e}$ because ummm reasons (I think it's supposed to map $m \otimes_R r' \mapsto r'\eta(m)$, but I'm not sure why this is injective).

Given a finite extension L/K of local fields, with ramification index e, then for any $s \in \mathbb{Z}_+$ the inclusion $\iota : K \hookrightarrow L$ induces a morphism $\widetilde{\iota} \triangleq (e, \varphi, \eta)$ between the triples $\mathrm{tr}_s(K)$ and $\mathrm{tr}_{es}(L)$, where φ is the expected map $\mathcal{O}_K/\mathfrak{m}_K^s \to \mathcal{O}_L/\mathfrak{m}_L^{es}$ (note the inclusion $\mathcal{O}_K \to \mathcal{O}_L$ maps exactly $\mathfrak{m}_K^s$ to exactly $\mathfrak{m}_L^{es}$, since $v_L = ev_K$), and η is induced by the natural map $\mathfrak{m}_K/\mathfrak{m}_K^{s+1} \to \mathfrak{m}_L/\mathfrak{m}_L^{e(s+1)}$ and the isomorphism $\mathfrak{m}_L/\mathfrak{m}_L^{e(s+1)} \cong (\mathfrak{m}_L/\mathfrak{m}_L^{es+1})^{\otimes e}$ (maybe explain this more?)

Definition 22. *We say a morphism (e, φ, η) between two triples (R, M, ε) and (R', M', ε') is:*

- ***flat*** *iff* $\lg(R') = e \lg(R)$
- ***finite*** *iff R' is a finitely generated R-module*
- ***unramified*** *iff it is flat + finite and $e = 1$*
- ***totally ramified*** *iff* $R/\mathfrak{m}_R \cong R'/\mathfrak{m}_{R'}$

We might also say that (R', M', ε') over (R, M, ε) is the same, if the morphism is understood.

At this point you really might snap and be like erm what the sigma is all this about; the upshot is that these triples will encode certain information about the extensions of a local field, that will be useful towards proving the main theorem. Specifically, Deligne defines the following categories:

Definition 23.

- *If K is a local field, $\mathcal{E}(K)$ is the category whose objects are finite separable extensions L of K, with morphisms $L \to L'$ as K-homomorphisms $L \to L'$.*
- *If $S \triangleq (R, M, \varepsilon)$ is a triple, $\mathcal{E}(S)$ is the category whose objects are pairs (S_1, f), where S' is another triple and $f : S \to S'$ is a morphism, and whose morphisms $(S_1, f) \to (S_2, f')$ are morphisms $g : S_1 \to S_2$ with $f' = g \circ f$.*

He then constructs, given a local field K, a functor T_0 from $\mathcal{E}(K)$ to $\mathcal{E}(\mathrm{tr}_s(K))$, for each $s \in \mathbb{Z}_+$, mapping L to $\mathrm{tr}_{e_K^L s}(L)$ and mapping $\iota : L \hookrightarrow L'$ to the morphism $\mathrm{tr}_{e_K^L s}(L) \to \mathrm{tr}_{e_K^{L'} s}(L')$ described in the remarks after definition 21. Note that this morphism is both finite (since $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module) and flat (by definition, since $\lg(\mathcal{O}_K/\mathfrak{m}_K^s) = s$ and $\lg(\mathcal{O}_L/\mathfrak{m}_L^{es}) = es$).

Theorem 18. *T_0 is full and essentially surjective on objects.*

Proof: Here is a sketch: given a object $((R', M', \varepsilon'), (e, \varphi, \eta)) \in \mathcal{E}(\mathrm{tr}_s(K))$, it must be finite and flat over $\mathrm{tr}_s(K)$; we can also assume it is totally ramified (?). We have the following diagram:

$$\begin{array}{ccc} \mathfrak{m}_K/\mathfrak{m}_K^{s+1} & \xrightarrow{\eta} & M'^{\otimes e} \\ \downarrow{\scriptstyle \varepsilon} & & \downarrow{\scriptstyle \varepsilon'_{0,e}} \\ \mathcal{O}_K/\mathfrak{m}_K^s & \xrightarrow{\varphi} & R' \end{array}$$

If β is a generator of M', then R' is a free $\mathcal{O}_K/\mathfrak{m}_K^s$-module with basis $1, \varepsilon'(\beta), \ldots, \varepsilon'(\beta)^{r-1}$; then using our induced isomorphism $\overline{\eta} : \mathcal{O}_K/\mathfrak{m}_K^s \otimes_R R' \hookrightarrow\!\!\!\!\rightarrow M'^{\otimes e}$, we have a unique system of elements $-a_0, \ldots, -a_{r-1} \in \mathcal{O}_K/\mathfrak{m}_K^s$ so that $x^{\otimes} = \overline{\eta}\left(\sum\limits_0^{r-1} -a_i \otimes_R \varepsilon'(\beta)^i\right)$ i.e. so that

$$x^{\otimes} + \overline{\eta}\left(\sum_0^{r-1} a_i \otimes_R \varepsilon'(\beta)^i\right) = 0$$

Then R' can be reconstructed from the a_i, since $R' \cong (\mathcal{O}_K/\mathfrak{m}_K^s)[T]/\left\langle T^r + \sum_0^{r-1} \varepsilon(a_i)T^i \right\rangle$, M' and ε' can be reconstructed similarly by taking any free R'-module of rank 1 and mapping its generator to T, φ can be reconstructed as the canonical map $\mathcal{O}_K/\mathfrak{m}_K^s \to (\mathcal{O}_K/\mathfrak{m}_K^s)[T]/\left\langle T^r + \sum_0^{r-1} \varepsilon(a_i)T^i \right\rangle$, and η can be reconstructed as well. Then $((R', M', \varepsilon'), (e, \varphi, \eta))$ is isomorphic to $(\mathrm{tr}_{es}(L), \widetilde{\iota})$, where L is gotten by adjoining a root of the Eisenstein polynomial $T^r + \sum_0^{r-1} \widetilde{a_i}T^i$ to K, where the $\widetilde{a_i}$ reduce to the a_i modulo $\mathfrak{m}_K^{s+1}$.

It is a general fact that a functor is an equivalence between two categories iff it is full, faithful, and essentially surjective on objects (I remember doing this exercise in Leinster ...); so in order for T_s to be an equivalence of categories, we would also need it to be faithful. It is not, however, so we want to mod out the morphisms appropriately to make it so. Hence the following:

Definition 24. *Let's say two morphisms $(e_1, \varphi_1, \eta_1), (e_2, \varphi_2, \eta_2) : (R, M, \varepsilon) \to (R', M', \varepsilon)$ are equivalent modulo $R(f)$ iff $e_1 = e_2$ (call it e), φ_1 and φ_2 induce the same map on the residue fields of R, R', and $v_{R'}(\varepsilon'_{0,e}(\eta_1(x) - \eta_2(x))) \geq e(f+1)$.*

Then we have the following:

Theorem 19. *Given T_s and $L, L' \in \mathcal{E}(K)$, with $\mathrm{spl}(L/K)$ being at-most-s-upper-ramified, then T_s induces a bijection between $\mathcal{E}(K)(L, L')$ and $R(\psi_{L/K}(s))$-equivalence classes of morphisms $T_s(L) \to T_s(L')$ (i.e. $\mathrm{tr}_{e_K^L s}(L) \to \mathrm{tr}_{e_K^{L'} s}(L')$).*

Proof: —

And a corollary:

Theorem 20. *If $\mathcal{E}(K)^s$ is the category of at-most-s-upper-ramified extensions of K, and $\mathcal{E}(\mathrm{tr}_s(K))^s$ is the category of triples over $\mathrm{tr}_s(K)$ satisfying a certain condition (which I'll fill in later) and morphisms as defined by $R(\psi_*^*(s))$, then T_s induces an equivalence between these two.*

Proof: —

(sorry, i need to fill in some details in the statement, cuz i need to make more definitions first skull emoji)

The above theorem is essentially the main result from Deligne, which - roughly speaking - says that the category of at-most-s-upper-ramified extensions of a field K is determined (up to equivalence) by $K^\times/(1+\mathfrak{m}^e)$. If we define $tr_s(K)^\times$ as the invertible elements of $\bigoplus_{n\in\mathbb{Z}} M^{\otimes n}$ (where $M = \mathfrak{m}_K/\mathfrak{m}_K^{s+1}$), then a generator α for M over $\mathcal{O}_K/\mathfrak{m}_K^s$ gives an isomorphism $\mathrm{tr}_s(K)^\times \hookrightarrow\!\!\!\!\to \mathbb{Z}\times(\mathcal{O}_K/\mathfrak{m}_K^s)^\times$ (as an element of $\bigoplus_{n\in\mathbb{Z}} M^{\otimes n}$ is a unit iff it is of the form $r\alpha^{\otimes n}$ for some n and some $r\in(\mathcal{O}_K/\mathfrak{m}_K^s)^\times$). At the same time, $\mathbb{Z}\times(\mathcal{O}_K/\mathfrak{m}_K^s)^\times \hookrightarrow\!\!\!\!\to K^\times/(1+\mathfrak{m}_K^s)$ via the map $(n,r)\mapsto r\pi^n(1+\mathfrak{m}_K^s)$. And $\mathrm{tr}_s(K)$ should be recoverable from $\mathrm{tr}_s(K)^\times$? (need to think about this more)

5 Newton copolygons

(Ideally I want to tie this section back to the Deligne section, but for now here's just the reference stuff I've typed up about the Lubin paper in the bibliography).

Let K be a local field with valuation v.

Now, since the Hasse-Herbrand transition function allows us to translate between the lower and upper numberings on our ramification groups, it would be useful to have a nice way to calculate it. The Newton copolygon (or the valuation function, which is essentially the same thing) gives us a nice way to do this in certain cases:

Definition 25. *For $f(T)\in\mathcal{O}_K[T]$ (with $f(T)=\sum_{i=0}^n c_iT^i$), the **valuation function** or **Newton copolygon** of f is $\Psi_{v,f}:\mathbb{R}_{\geq 0}\to\mathbb{R}_{\geq 0}$ given by $\Psi_{v,f}(t)\triangleq \min_{0\leq i\leq n}\{it+v(c_i)\}$.*

The basic intuition behind this definition (which is where the name 'valuation function' probably stems from) is that $v(f(x)) \geq \min_{0\leq i\leq n}\{v(c_ix^i)\} = \min_{0\leq i\leq n}\{iv(x)+v(c_i)\}$, with - by theorem 1 - equality when the $iv(x)+v(c_i)$ have a unique minimum, which happens for all but finitely many values of $v(x)$ (one way to see this is that the $iv(x)+v(c_i)$ are linear functions in $v(x)$, each with different slopes). When there is such a unique minimum, this means that $v(f(x))$ depends *entirely* on $v(x)$, and $\Psi_{v,f}(v(x)) = v(f(x))$ at all but finitely many points $t_1,\dots,t_k$. Then $\Psi_{v,f}$ is linear on each interval $[t_i,t_{i+1}]$ for $1\leq i\leq k-1$, as well as on $[0,t_1]$ and $[t_k,\infty)$.

It turns out that, for certain extensions, the Hasse-Herbrand function is the Newton copolygon of a particular polynomial:

Theorem 21. *If $K_0\leq K\leq L$ are local fields, with L/K galois and L/K_0 finite, v the valuation on L normalized for K_0, π a uniformizer for L and $f(T)\triangleq \mathrm{irr}(\pi, L_{G_0(L/K)})(T+\pi)$, then*

$$\varphi_K^L(t-1)+1 = e_{K_0}^K\Psi_{v,f}\left(\frac{t}{e_{K_0}^L}\right)$$

for $t \geq 0$.

Proof: I'll prove it assuming $K_0 = K$. In this case, we have

$$\begin{aligned} v(f(T+\pi)) &= v\left(\prod_{\sigma \in \mathrm{gal}(L/K)} (T - (\sigma(\pi) - \pi))\right) \\ &= \sum_{\sigma \in \mathrm{gal}(L/K)} v(T - (\sigma(\pi) - \pi)) \\ &\geq \sum_{\sigma \in \mathrm{gal}(L/K)} \min(v(T), v(\sigma(\pi) - \pi)) \\ &= \sum_{\sigma \in \mathrm{gal}(L/K)} \min\left(v(T), \frac{i_K^L(\sigma)}{e_K^L}\right) \end{aligned}$$

with equality whenever $v(T)$ does not equal $v(\sigma(\pi) - \pi)$ for any $\sigma \in \mathrm{gal}(L/K)$. Since this only happens for finitely many values of $v(T)$, it suffices to prove the theorem when we have equality (at which point the full theorem will follow by continuity). Then the above calculation implies that, as a function of $v(T)$, $\Psi_{v,f}$ has derivative equal to the number of σ with $i_K^L(\sigma)/e_K^L$ greater than $v(T)$, which equals $|G_{e_L^K v(T)}(L/K)|$. So $\Psi'_{v,f}(t) = |G_{e_K^L t}(L/K)|$ at all but finitely many points. At the same time, $(\varphi_K^L)'(t) = |G_{t+1}(L/K)|/|G_0(L/K)|$ at all but finitely many points, as we've seen previously. Then

$$\left(\Psi_{v,f}\left(\frac{t}{e_K^L}\right)\right)' = \frac{1}{e_K^L}\Psi'_{v,f}\left(\frac{t}{e_K^L}\right) = \frac{|G_t(L/K)|}{|G_0(L/K)||} = (\varphi_K^L)'(t-1)$$

at all but finitely many points, and since the functions are continuous they must differ by a constant. Since $\Psi_{v,f}(0) = 0$ (because f is monic) and $\varphi_K^L(0-1) = -1$, then the result follows.

□

The existence of K_0 in the above theorem is literally just to scale things if we feel like it (maybe, for example, if it might be easier to calculate the ramification indexes of K and L over K_0 than of L over K?).

Definition 26. *The **altitude** of a finite separable totally ramified extension L/K is the vale of φ_K^L at its rightmost 'vertex' (discontinuity) - in other words, if t is the infimum over the ones so that $G_t(L/K)$ is trivial, then $\mathrm{alt}_K^L \triangleq \varphi_K^L(t)$.*

The altitude of a finite separable extension L/K is the altitude of L/L_{G_0}, and L^s $(s > 0)$ is the compositum of all subfields of L/K with altitude $< s$ (which also has altitude $< s$ by the theorem below).

Note that the altitude is essentially the infimum over the s such that L/K is at-most-s-upper-ramified. Lubin proves a couple useful facts about altitude:

Theorem 22. *Let L, E be finite separable over K.*

- $\mathrm{alt}_K^{LE} \leq \max(\mathrm{alt}_K^L, \mathrm{alt}_K^E)$.

- $\mathrm{alt}_K^L = \mathrm{alt}_K^{\mathrm{spl}(L/K)}$.
- $E^s = L^s \cap E$ *for all* $s > 0$.

---

6 Acknowledgements

I would like to thank the two cats who live in the vscode-pets extension in the lower left corner of my latex editor (sorry I'll put real acknowledgements in my final draft lol but I would actually like to thank those two cats)

also i'll add my blbliography later cuz it's really late right now but i only used a few sources tbh (mainly serre's local fields, lubin's elementary analytic methods in higher ramification theory, and deligne's 1984 paper)