MATH 223A: UPPER NUMBERING RAMIFICATION GROUPS

SAM LICHTENSTEIN

Motivation

Standard setup.

$$\begin{array}{ccccc} \ell & = & B/\mathfrak{P} = B/\Pi B & \leftarrow & B & \hookrightarrow & L \\ | & & & & | & & | \\ k & = & A/\mathfrak{p} = A/\pi A & \leftarrow & A & \hookrightarrow & K \end{array}$$

Let K be a complete DVF, let L/K be a finite separable extension of degree n, with $G = \mathrm{Gal}(L/K)$, and suppose the residue extension is separable.

Recall from class the definition of the (lower indexed) **ramification groups**, a filtration of G defined by

$$0 \to G_i \to G \to \mathrm{Aut}(B/\mathfrak{P}^{i+1}) \to 0.$$

That is, G_i is the subgroup of G fixing $B/\mathfrak{P}^{i+1}$.

Properties.

(1) Easy to define;

(2) Suppose we have the setup

$$\begin{array}{ccc} L & & \\ {\scriptstyle H \lhd G}\,\big| & \big| & \\ K' & \big| & G \\ {\scriptstyle G/H}\,\big| & \big| & \\ K & & \end{array}$$

The **filtration index** $i_{L/K}(\sigma) = v_L(\sigma x - x)$ [where x is a monogenerator for $\mathfrak{o}_L$ as an $\mathfrak{o}_K$-algebra] plays well with restriction from $G = \mathrm{Gal}(L/K)$ to $H = \mathrm{Gal}(L/K') \lhd G$ when we have a tower of Galois extensions $K \subset K' \subset L$;

(3) But, $i_{L/K}$ plays (somewhat) poorly with quotients: the *unindexed* filtration on $G/H = \mathrm{Gal}(K'/K)$ comprises the same groups we get by projecting the filtration on G to G/H, but - as Mazur put it - "the bad news" is that the filtration indexing expressed by the compicated formula

$$(\star) \qquad i_{K'/K}(\overline{\sigma}) = \frac{1}{e(L/K')} \sum_{G \ni \sigma \mapsto \overline{\sigma}} i_{L/K}(\sigma).$$

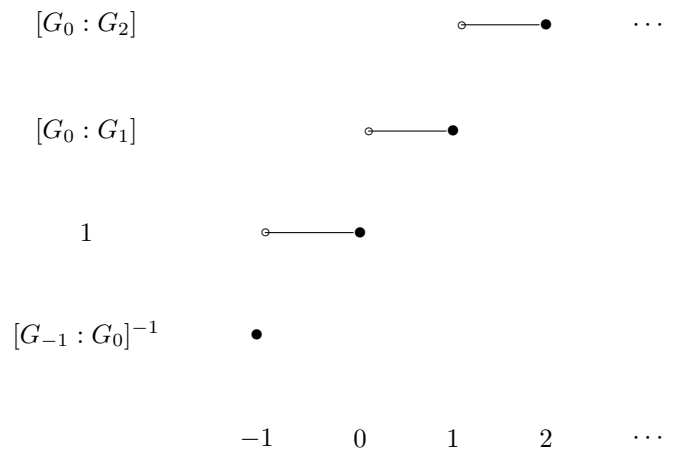
Goal. Figure out how to re-express the ramification filtration in a way that is adapted to quotients. We'll index our new filtration with *raised* indices to distinguish it from the existing lower-indexed filtration, and - suggestively - call the groups G^i the **upper numbering ramification groups**.

It should go without saying that the reference for all this material is *Local Fields*.

Definitions

The function φ. We extend the map $G_\bullet : \{-1, 0, 1, 2, \ldots\} \to \{subgroups \subset G\}$ to a map from $\mathbb{R}_{\geq -1} \to \{subgroups\}$ by setting $G_u = G_{\lceil u \rceil}$ for any $u \geq -1$.

Using this convention, we extend the map $[G_0 : G_\bullet] : \{0, 1, 2, \ldots\} \to \mathbb{N}$ to $[G_0 : G_\bullet] : \mathbb{R}_{\geq -1} \to \{[G_{-1} : G_0]^{-1}\} \cup \mathbb{N}$ by setting $[G_0 : G_{-1}] = [G_{-1} : G_0]^{-1}$. Graph of $[G_0 : G_\bullet]$:



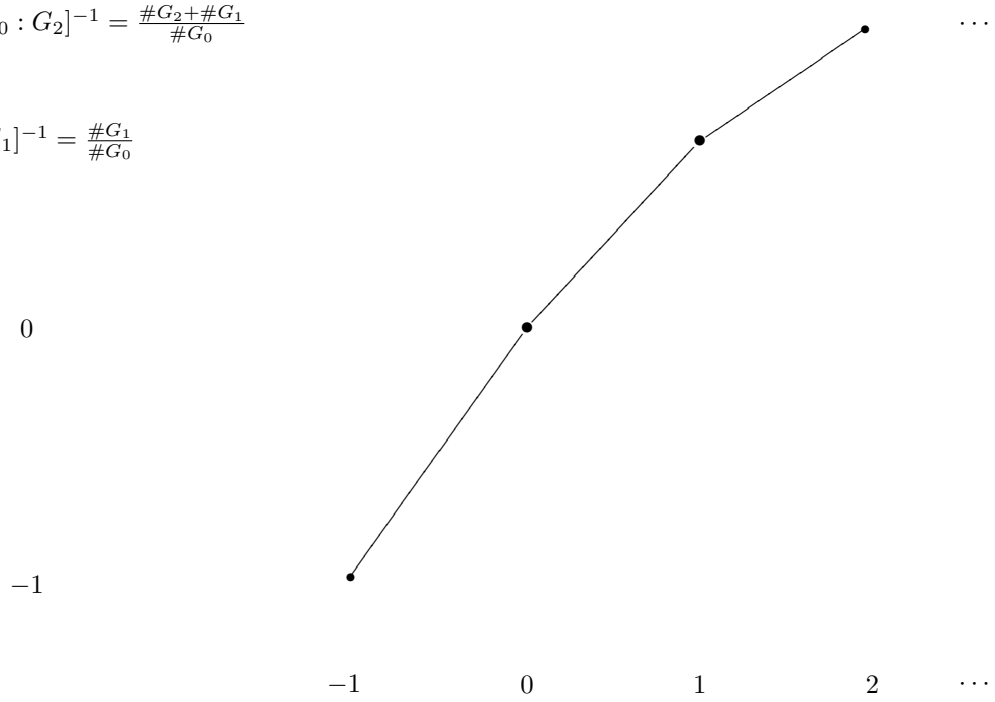
Now define $\varphi : \mathbb{R}_{\geq -1} \to \mathbb{R}$ by the integral

$$\varphi(u) = \varphi_{L/K}(u) := \int_0^u \frac{\mathrm{d}\, t}{[G_0 : G_t]}.$$

All this notation is just Serre's silly way of writing a piecewise linear definition

$$\varphi(u) = \begin{cases} -u, & -1 \leq u \leq 0; \\ \frac{1}{\#G_0}(\#G_1 + \cdots + \#G_m + (u-m)\#G_{m+1}), & m \leq u \leq m+1, m \in \mathbb{N}. \end{cases}$$

The graph of φ looks like



Main Lemma. Recalling that $i_{L/K}(\sigma) \geq i+1 \Leftrightarrow \sigma \in G_i$, it is not difficult to see that

$$\varphi(u) = \left(\frac{1}{\#G_0} \sum_{\sigma \in G} \min(i_{L/K}(\sigma), u+1) \right) - 1.$$

Proof. Stare. □

The function ψ. So φ is continuous, piecewise linear, monotonic increasing, and concave. Moreover $\varphi'(u) = [G_0 : G_u]^{-1}$ for $u \notin \mathbb{Z}$. So φ gives a homeomorphism of the half-line $[-1, \infty)$ onto itself; let the continuous inverse be $\psi : \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 1}$. Then ψ is also continuous, piecewise linear, and increasing, but convex. Moreover $\psi'(\varphi(u)) = 1/\varphi'(u)$ takes on only integer values.

Suppose $v \in \mathbb{Z}_{\geq -1}$; set $u = \psi(v)$ and suppose $u \in [m, m+1]$. Then

$$\#G_0 \cdot v = \#G_1 + \cdots + \#G_m + (u - m) \cdot \#G_{m+1}.$$

Since $\#G_{m+1} | \#G_i$ for $0 \leq i \leq m$, we can divide through by it to conclude that $(u - m)$, and hence u, is an integer.

***Upper Numbering* of the ramification gorups.** This is defined by

$$G^v = G_{\psi(v)} \iff G^{\varphi(u)} = G_u.$$

Quotients

Theorem. The following **transitivity formulas** hold:

$$\varphi_{L/K} = \varphi_{K'/K}\varphi_{L/K'} \text{ and } \psi_{L/K} = \psi_{L/K'}\psi_{K'/K}.$$

Moreover, the upper numbering is adapted to quotients: if $H \lhd G$ then

$$(G/H)^v = G^v H/H$$

for all v.

Lemma (omit). $i_{L/K}(st) \geq \min(i_{L/K}(s), i_{L/K}(t))$.

Proof. Use the fact that $i_{L/K}(g) \geq i + 1 \Leftrightarrow g \in G_i$, together with the fact that $G_{\min(i_{L/K}(s)-1, i_{L/K}(t)-1)} = G_{i_{L/K}(s)-1} \cap G_{i_{L/K}(t)-1}$ (since we're dealing with a filtration) and st is in this intersection. □

Lemma (omit proof). Fix $\overline{\sigma} \in G/H$ and define $j(\overline{\sigma}) = \max\limits_{G \ni \sigma \mapsto \overline{\sigma}} i_{L/K}(\sigma)$. Then

$$i_{K'/K}(\overline{\sigma}) = 1 + \varphi_{L/K'}(j(\overline{\sigma}) - 1).$$

Proof. Let $G \ni s \mapsto \overline{\sigma}$ such that $i_{L/K}(s) = j(\overline{\sigma}) =: m$ be where the maximum defining $m = j(\overline{\sigma})$ is obtained. If $t \in H_{m-1} = H \cap G_{m-1}$ then $i_{L/K}(t) \geq m$ so $i_{L/K}(st) \geq \min(i_{L/K}(s), i_{L/K}(t)) \geq m$. But $st \mapsto \overline{\sigma}$ so by the maxmiality of m we have $i_{L/K}(st) = m$. If $t \notin H_{m-1}$ then $i_{L/K}(t) < m$, and as a consequence $i_{L/K}(st) = i_{L/K}(t) < m$.

(Proof: If x is a monogenerator for $\mathfrak{o}_L$ as an $\mathfrak{o}_K$-algebra, we have $v_L(s(t(x)) - x) = v_L(s(t(x)) - t(x) + t(x) - x) = \min(v_L(s(t(x)) - t(x)), v_L(t(x) - x))$. Since $i_{L/K}(s) = m$ we have $v_L(s(t(x)) - t(x)) > m$, so this minimum is $v_L(t(x) - x) = i_{L/K}(t)$.)

Thus we see $i_{L/K}(st) = \min(i_{L/K}(t), m)$. So by formula $(\star)$ we have

$$i_{K'/K}(\overline{\sigma}) = \frac{1}{e(L/K')} \sum_{t \in H} \min(i_{L/K}(t), m).$$

But by the Main Lemma we have

$$\varphi_{L/K'}(m-1) + 1 = \frac{1}{\#H_0} \sum_{t \in H} \min(i_{L/K'}(t), m).$$

We showed in class that $i_{L/K'} = i_{L/K}|_H$ and we know that by definition $e(L/K') = \#H_0$. (Recall that $H_0 = \ker(H \twoheadrightarrow \mathrm{Gal}(\ell, k'))$ has order $[L : K']/[\ell, k'] = e(L/K')$.)

So we can conclude that

$$i_{K'/K}(\overline{\sigma}) = 1 + \varphi_{L/K'}(m-1),$$

as claimed. □

Lemma (Herbrand's theorem). if $v = \varphi_{L/K'}(u)$ then $G_u H/H = (G/H)_v$.

Proof. This follows right from the definitions and the last lemma: $\overline{\sigma} \in G_u H/H \Leftrightarrow (\exists s \in G_u, t \in H) st \mapsto \overline{\sigma} \Leftrightarrow (\exists s \in G_u, s \mapsto \overline{\sigma}) i_{L/K}(s) \geq \lceil u \rceil + 1 \Leftrightarrow j(\overline{\sigma}) - 1 \geq u \Leftrightarrow \varphi_{L/K'}(j(\overline{\sigma}) - 1) \geq \varphi_{L/K'}(u) \Leftrightarrow i_{K'/K}(\overline{\sigma}) - 1 \geq \varphi_{L/K'}(u) \Leftrightarrow \overline{\sigma} \in (G/H)_v$. □

Proof of theorem. To prove the transitivity formulas, it suffices by continuity to show them on the dense subsets of their domains upon which the functions ψ and φ are differentiable. Suppose $u > -1$ is a non-integer. Then setting $v = \varphi_{L/K'}(u)$ we have by the chain rule

$$(\varphi_{K'/K}\varphi_{L/K'})'(u) = \varphi'_{K'/K}(v)\varphi'_{L/K'}(u).$$

Since we know that $\varphi'_{K'/K}(v) = [(G/H)_0 : (G/H)_v]^{-1} = \#(G/H)_v/\#(G/H)_0 = \#(G/H)_v/e(K'/k)$ and similarly $\varphi'_{L/K'}(u) = \#H_u/e(L/K')$, we get

$$(\varphi_{K'/K}\varphi_{L/K'})'(u) = \frac{\#(G/H)_v}{e(K'/K)} \cdot \frac{\#H_u}{e(L/K')} = \frac{\#(G_uH/H)}{e(K'/K)} \cdot \frac{\#(H \cap G_u)}{e(L/K')} = \frac{\#G_u}{e(L/K)} = \varphi'_{L/K}(u)$$

since the ramification indices are multiplicative and $\#G_uH = \#G_u \cdot \#H/\#H_u$ because $H_u = G_u \cap H$. Since the derivatives agree identically (where they are defined) and the maps agree at 0, by continuity this proves the desired identity for the φs. Inverting it gives the desired identity for the ψs.

Now we have

$$(G/H)^v = (G/H)_{\psi_{K'/K}(v)} = G_{\psi_{L/K'}\psi_{K'/K}(v)}H/H = G_{\psi_{L/K}v}H/H = G^vH/H,$$

as desired.

Example: $G = Q_8$ the quaternion group

We have $G = \{\pm 1, \pm i, \pm j, \pm k\}$ with the usual relations, $Z(G) = \pm 1$.

Theorem. *There exists a totally ramified extension L/K such that $G = \mathrm{Gal}(L/K)$ and $G_4 = 1$.*

With just this knowledge we can deduce the structure of the ramification groups.

First, since L/K is totally ramified we must have $G = G_0$. Second, recall from class that G_0/G_1 injects into the units of the residue field of K, so is cyclic. The only normal subgroups of $G_0 = G$ are $1, Z, G_0$. Since G and $G/Z \cong V$ are not cyclic, w emust have $G_1 = G_0 = G$. This means that L/K is *wildly ramified*, and the residue characteristic must therefore be 2.

Lemma. The integers $i \geq 1$ such that $G_i \neq G_{i+1}$ are all congruent to one another mod p where p is the residue characteristic.

Proof. See Serre, §IV.2, Prop. 11. □

So we know that G_2, G_3 are either (G, G), (Z, Z), or $(1, 1)$.

Lemma. If $i \geq 1$ and $s \in G_0, t \in G_i$ then $[s, t] \in G_{i+1}$ if and only if $s^i \in G_1$ or $t \in G_{i+1}$.

Moreover, if $i, i' \geq 1$ and $s \in G_i, t \in G_{i'}$ then $[s, t] \in G_{i+i'}$.

Proof. loc. cit. Cor. 1., Prop. 10. (Proof involves using the maps $G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1}$.) □

Since $i \in G_0$ and $j \in G_1$ this gives $[i, j] = -1 \in G_2 \Leftrightarrow i \in G_1$ or $j \in G_2$. Since $i \in G_1$, in fact we have $-1 \in G_2$. So $(G_2, G_3) = (G, G)$ or (Z, Z).

Moreover if $j \in G_3$ then $[i, j] = -1 \in G_4$, which is false. So the lower indexing is $G_{-1} = G_0 = G_1 = G, G_2 = G_3 = Z, G_4 = \cdot = 1$.

Now we can figure out the upper indexing. Working it out using the funciton $\varphi_{L/K}$ we find

$$G^v = \begin{cases} G & v \leq 1 \\ Z & 1 < v \leq \frac{3}{2} \\ 1 & v \geq \frac{3}{2} \end{cases}$$

So the upper indices "jump" at 1 and $\frac{3}{2}$. Note that one of the jumps is not an integer! This is a non-abelian phenomenon:

Theorem (Hasse-Arf)**.** *If G is abelian and v is a jump in the upper numbering filtration of the ramification groups, then v is an integer.*