COLORADO STATE UNIVERSITY MATHEMATICS

Higher Ramification Groups

Dean Bisogno

April 22, 2016

1 ABSTRACT

Studying higher ramification groups immediately depends on some key ideas from valuation theory. With that in mind we hope to layout the essential results from valuation theory before proceeding to the subject of this paper. Higher ramification groups arise when studying extensions of fields, and the ramification of primes in the base field. This in particular appears when studying the genus or fundamental group of spaces. From Riemann-Hurwitz we can calculate the genus of a space if we know the degree of the appropriate cover or extension, and ramification of such a cover. In well behaved situations, the ramification information can be known independently or just read off from the ramification index. But in more interesting situations (such as when the characteristic of your base field divides the ramification index), we need to inspect the order of higher ramification group to correct our ramification index. Another application of higher ramification groups is to study the subgroup structure of a Galois group, as the higher inertia groups will all be subgroups, and particular inertia groups will yield information about sylow p-subgroups of the Galois group in question. We hope to understand at a broad level what higher ramification groups are, and investigate a couple examples of their use.

2 PRELIMINARIES

2.1 VALUATIONS

We will primarily deal with discrete valuations, though

Definition 1 (Discrete Valuation Ring (D.V.R.))**.**
A discrete valuation ring is a principal ideal domain O with a unique maximal ideal $p \neq 0$.

Definition 2 (Uniformizing Parameter)**.**
Let $\mathfrak{p}$ be the unique maximal ideal of D.V.R. O. Since O is a PID, there exists a prime π in O such that $\mathfrak{p} = (\pi)$. We call π a uniformizing parameter.

Theorem 7, section 16.2 in (Dummit and Foote, 2004) shows that π is unique (up to multiplication by a unit) and generates the unique maximal ideal of O. Further in problem 26, in section 7.1 of Dummit and Foote, 2004 (which we proved in math 566) we showed that $O \setminus \mathfrak{p}$ is the set of units in O. Then for any $a \in O \setminus \{0\}$ we know that (a) is an ideal of O. We know (a) is a nonzero ideal of O and because (π) is maximal, and in local ring O, there exists some $n \in \mathbb{Z}$ such that $(a) = (\pi)^n$. Notice if a is a unit, then $n = 0$ because $< a >= O$.

Definition 3 (Discrete Valuation)**.**
The exponent n used above is the valuation of a denoted $v_\mathfrak{p}(a)$, it is a function $v_\mathfrak{p} : K^* \to \mathbb{Z}$ where K is the field of fractions of O. We can extend $v_\mathfrak{p}$ to K by setting $v_\mathfrak{p}(0) = \infty$. Further $v_\mathfrak{p}$ satisfies the following

I. $v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$.

II. $v_\mathfrak{p}(a+b) \geq min\{v_\mathfrak{p}(a), v_\mathfrak{p}(b)\}$.

There are also valuations which are not discrete, and we can classify all valuations as either archimedean or nonarchimedean. We call a valuation v nonarchimedean if $v(n)$ is bounded for every $n \in \mathbb{N}$. Proposition 3.6 in Neukirch, 1999 is often incorporated in the definition of discrete valuations, as every discrete valuation is nonarchimedean.

Proposition 1.
A valuaion $v(x)$ is nonarchimedean if and only if it satisfies $v(x+y) \leq max\{v(x), v(y)\}$.

Proof. ($\Leftarrow$) The reverse direction is straight forward. We just notice

$$v(n) = v(1 + \ldots + 1) \leq 1 \ \forall n \in \mathbb{N}.$$

($\Rightarrow$) Now, $v(n) \leq N$ for all $n \in \mathbb{N}$ for some $N \in \mathbb{N}$. Then for arbitrary $x, y \in K$, without loss of generality, consider $v(x) \geq v(y)$. Choose $l \geq 0$, so we get $v(x)^l v(y)^{n-l} \leq v(x)$. Now applying binomial formula we see that

$$v(x+y)^n \leq \sum_{l=0}^{n} v\binom{n}{l} v(x)^l v(y)^{n-l} \leq N(n+1)(v(x))^n$$

taking the n^{th} root of both sides yields

$$v(x+y) \leq N^{\frac{1}{n}}(1+n)^{\frac{1}{n}} v(x) = N^{\frac{1}{n}}(1+n)^{\frac{1}{n}} max\{v(x), v(y)\}$$

The result then follows if we let $n \to \infty$. We can conclude then that for any discrete valuation (which is nonarchimedean) $v(x+y) \leq max\{v(x), v(y)\}$. //

Valuations are particularly useful when studying number fields because of the following propositions

Proposition 2 (Neukirch, 1999)**.**
Let O be a noetherian integral domain. O is a Dedekind domain if and only if, for all prime ideals $\mathfrak{p} \neq 0$, the localizations $O_\mathfrak{p}$ are discrete valuation rings.

Proposition 3 (Neukirch, 1999)**.**
Every valuation of $\mathbb{Q}$ is equivalent to one of $v_p(x)$ (the nonarchimedean valuations) or $v_\infty(x)$ (the archimedean valuations).

Definition 4 (Prolongation of a valuation)**.**
If $A \subset B$ are rings with B integral over A, $\mathfrak{p}$ a prime in A, and $\mathfrak{q}$ prime in B dividing $\mathfrak{p}$ with ramification index $e_\mathfrak{q}$ then $v_\mathfrak{q}(x) = e_\mathfrak{q} v_\mathfrak{p}(x)$ is a prolongation of $v_\mathfrak{p}$ with index $e_\mathfrak{q}$ (Serre, 1995).

2.2 Field Completion

With a valuation v on a field K then for any real number $a \in (0,1)$ we can induce an absolute value on K by

$$||x|| = \begin{cases} a^{v(x)} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

which satisfies the usual conditions of a metric as outlined by. A topology is then induced on K via the absolute value metric, and we can denote the completion of K with respect to the valuation v by K_v. Note also that the metrics induced by different choices of a are topologically equivalent, so the completion is dependent only on v. Further, v extends in the completion of K to a discrete valuation (which we will continue to call v) on K_v (Serre, 1995).

3 Higher Ramification Groups

Consider now a finite Galois extension $L|K$ with Galois group Γ, associated discrete valuations ω on L and v on K with uniformizing parameters π_L and π_K respectively, and integer rings O_L and O_K.
Recall that

Definition 5 (Higher Ramification Groups, Serre, 1995)**.**
For every real number $i > -1$ we define the i^{th} ramification group of $L|K$ by

$$G_i = G_i(L|K) = \{\sigma \in \Gamma | \omega(\sigma(a) - a) \geq i+1 \ \forall a \in O_L\}.$$

The following is a proposition which helps characterize the higher ramification groups

Proposition 4.
For any $a \in O_L$ and $\sigma \in G$, $\omega(\sigma(a) - a) \geq i+1$ if and only if $\sigma(a) \equiv a \ mod \ <\pi_L>^{i+1}$.

Proof. ($\Rightarrow$)

$$v_L(\sigma(a) - a) \geq i+1 \implies \sigma(a) - a = \pi_L^{(}t)\frac{a}{b}$$

where $t \geq i+1$ and $a, b, \pi_L \in O_L$ all relatively prime. The above then implies $\sigma(a) - a \equiv 0 \ mod \ <\pi_L>^{i+1}$.
($\Leftarrow$)

$$\sigma(a) - a \equiv 0 \ mod \ \pi_L^{i+1} \implies \sigma(a) - a = \pi_L^t \frac{a}{b}$$

with the same restrictions as above. It follows then that $v_L(\sigma(a) - a) \geq i+1$. //

Clearly this induces the following filtration on G:

$$\{G_i(L|K)\}_{i\geq -1} = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \dots$$

Proposition 5.
The first two ramification groups are $G_0 = G$ and $G_1 = I$.

Proposition 6.
For $L|K$ is Galois with group Γ, $\nu_{\mathfrak{p}}(x)$ a valuation on K and $\omega_{\mathfrak{q}}(x)$ a prolongation of $\nu_{\mathfrak{p}}$, let $\widehat{L}$,$\widehat{K}$ be the completions of L and K with respect to $\omega_{\mathfrak{q}}$ and $\nu_{\mathfrak{p}}$ respectively. If $D(L|K)$ is the decomposition group of $\mathfrak{q}$ over $\mathfrak{p}$, then $\widehat{L}|\widehat{K}$ is Galois with Galois group $D(L|K)$.

4 The Upper Numbering and Ramification Jump

Definition 6 (Upper Numbering of the Higher Ramification groups)**.**
Consider the function

$$t = \varphi(s) = \int_0^s \frac{dx}{[G_0 : G_x]}$$

called the Herbrand function which has inverse map ψ. Then for any real $s \geq -1$ let $G_s = G_{\lceil s \rceil}$ and renumber the ramification groups by $G^t(L|K) = G_s(L|K)$ where $s = \psi(t)$.

Definition 7 (Ramification Jump)**.**
If $G^t(L|K) \neq G^{t+\epsilon}(L|K)$ for any $\epsilon \geq 0$ then we call t a ramification jump.

Theorem 1 (Hasse-Arf)**.**
For a finite abelian extension $L|K$, the jumps of the filtration $\{G^i(L|K)\}_{i\geq -1}$ are rational integers.

Serre gives a useful interpretation of the Hasse-Arf theorem, namely that if $G_i \neq G_{i+1}$ then $\varphi(i)$ is an integer. We can use this in the following example (Serre, 1995).

Example 1.
Suppose G is a cyclic group of order p^n where p is the characteristic of $\widehat{K}$. Let $G(i)$ be the subgroup of G with order p^{n-i}. Then there exist integers $i_0, \dots, i_{n-1}$ such that we can identify all ramification groups as follows:

$$G_0 = G_{i_0} = G = G^0 = G^{i_0}$$

$$G_{i_0+1} = \dots = G_{i_0+pi_1} = G(1) = G^{i_0+1} = \dots = G^{i_0+i_1}$$

$$G_{i_0+pi_1+1} = \dots = G_{i_0+pi_1+p^2i_2} = G(2) = G^{i_0+i_1+1} = \dots = G^{i_0+i_1+i_2}$$

$$\vdots$$

$$G_{i_0+pi_1+p^2i_2+\dots+p^{n-1}i_{n-1}+1} = 1 = G^{i_0+\dots+i_{n-1}+1}.$$

5 Applications

5.1 Cyclotomic Extensions of $\mathbb{Q}_p$

In this example we consider the p-adic completion of $\mathbb{Q}$ with respect to a valuation (and associated metric) v_p. Let $n = p^m$, and ζ be a primitive n^{th} root of unity and the extension $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ with Galois group G. We recall that $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] = \phi(n) = (p-1)p^{m-1}$ and $G \cong (\mathbb{Z}/n)^*$.
Now, if $0 \leq v \leq m$ then let G^v be the subgroup of G isomorphic to the subgroup $H \subset (\mathbb{Z}/n)^*$ such that $a \equiv 1 \ mod \ p^v$ for every $a \in H$. Since $Gal(\mathbb{Q}_p(\zeta_{p^v})|\mathbb{Q}_p) \cong (\mathbb{Z}/p^v)^*$ we can see that $Gal(\mathbb{Q}_p(\zeta_{p^m})|\mathbb{Q}_p(\zeta_{p^v})) \cong G^v$. Using this fact we can find all ramification groups G_i of G (Serre, 1995).

Proposition 7.
The ramification groups G_i of G are

$$G_u = \begin{cases} G & u = 0 \\ G^1 & 1 \leq u \leq p-1 \\ G^2 & p \leq u \leq p^2 - 1 \\ \vdots & \\ \{1\} & p^{m-1} \leq u \end{cases}$$

Proof. //

5.2 Artin-Schreier Extensions in Positive Characteristic

(example from char p appendix to Renzo's book) We can rephrase Riemann-Hurwitz such that if field $\mathbb{F}$ has characteristic p and $p|e$ where e is the ramification index of a point under a degree d covering map $\phi : X \to Y$ of curves over $\mathbb{F}$, then

$$2g_Y - 2 = d(2g_X - 2) + \sum_{x \in X} \Big(\sum_{i=0}^{\infty} |G_i(x)| - 1 \Big).$$

For a smooth compact algebraic curve $X_{p,t} : x^p - x - f(y)$ where $f(y)$ is degree t over algebraically closed field $\mathbb{F}$ of characteristic $p \neq 0$. Now consider the covering map $\psi : X_{p,t} \to \mathbb{A}^1_{\mathbb{F}}$ of the affine line over $\mathbb{F}$ such that $\psi(x,y) = y$.
Strategy (use change of variables $x = x\bar{y}^a, \bar{y} = 1/y$ so $p_\infty = (0,0)$, and $t = ap - 1$): Since ψ is clearly unramified over $\mathbb{A}^1_{\mathbb{F}}$, consider now $\psi : X_{p,t} \to \mathbb{P}^2_{\mathbb{F}}$. We see now that ψ is ramified over p_∞ and $Gal(\psi) \cong \mathbb{Z}/p =< \tau >=< x+1 >$. We want to show that there exists uniformizing parameter π such that $v_\infty(\pi) = 1$, then since $\tau = x+1$ generates G we want to check $\tau(\pi) - \pi$, and finally evaluate $t_\infty = v_\infty(\tau(\pi) - \pi)$. Because $\mathbb{Z}/p = G$ is simple $G_{t_\infty} = 1$ so we get

$$\sum_{x \in X} \Big(\sum_{i=0}^{\infty} |G_i(x)| - 1 \Big) = |\mathbb{Z}/p|(t_{p_\infty} + 1) = (p-1)(t_{p_\infty} + 1).$$

Which we can confirm by Stitchenoth, 1993 III.7.8.

REFERENCES

Cassels, J. & Frohlich, A. (1967). *Algebraic number theory*. Academic Press Inc. (London) LTD.

Chonoles, Z. (2010). An introduction to higher ramification groups. Retrieved from http://math.uchicago.edu/~chonoles/expository-notes/ramificationgroups.pdf

Clark, P. (2009). Lecture notes on local fields. Retrieved from http://math.uga.edu/~pete/local.pdf

Dummit, D. & Foote, R. (2004). *Abstract algebra*. John Wiley & Sons, Inc.

Neukirch, J. (1999). *Algebraic number theory*. Springer-Verlag Berlin Heidelberg.

Serre, J.-P. (1995). *Local fields*. Springer-Verlag New York.

Stitchenoth, H. (1993). *Algebraic function fields and codes*. Springer-Verlag Berlin Heidelberg.