An Introduction to Higher Ramification Groups

Zev Chonoles[1]

Submitted December 23, 2010

1 Background and Notation

Let K be a field complete with respect to a non-trivial discrete valuation v_K, and let L be a finite separable extension of K of degree $n = [L : K]$. Let A_K be the valuation ring of v_K, i.e.

$$A_K = \{\alpha \in K \mid v_K(\alpha) \geq 0\}.$$

Then the integral closure of A_K in L is a valuation ring $A_L \subseteq L$, and the valuation v_L defined by A_L[2] is the unique extension of v_K to a discrete valuation on L. Furthermore, L is complete with respect to v_L. Recall that

$$P_K = \{\alpha \in A_K \mid v_K(\alpha) > 0\} \subseteq A_K, \qquad P_L = \{\alpha \in A_L \mid v_L(\alpha) > 0\} \subseteq A_L$$

are the maximal ideals (in fact, unique prime ideals) of A_K and A_L. Because a valuation ring is a PID, we have that $P_K = (\pi_K)$ and $P_L = (\pi_L)$ for some $\pi_K \in A_K$ and $\pi_L \in A_L$. The elements π_K and π_L are called *uniformizing parameters*, and are clearly determined up to multiplication by a unit of A_K and A_L, respectively. We know that every fractional ideal of K is of the form $P_K^i = (\pi_K^i)$ for some $i \in \mathbb{Z}$, and similarly for L. Therefore, because $P_K A_L$ is a proper ideal of A_L, we have that $P_K A_L = P_L^e$ for some $e = e(L/K) \geq 1$, called the *ramification index* of L/K. Finally, let $\overline{K} = A_K/P_K$ and $\overline{L} = A_L/P_L$ be the residue fields of K and L. Then $f = f(L/K) = [\overline{L} : \overline{K}]$ is called the *residue degree* of L/K. They are related by the following result, which is Cor. 1 to Prop. 3 in Chapter 2 of [3].

Proposition 1. For K, L, n, e, f as above, $ef = n$.

Proof. This immediately follows from the prime decomposition theorem (Prop. 10 in Chapter 1 of [3]), a.k.a. the "$\sum e_i f_i = n$ theorem", and the fact that A_L has only one prime, P_L. □

[1] The author was supported by a grant from his father.

[2] cf. Prop. 2 in Chapter 1, §1 of [2]

The reason we are interested in the above setup (besides plain-old curiosity) is because it occurs when we have a Dedekind domain R, its fraction field $F = \mathrm{Frac}(R)$, a finite separable extension E/F, the integral closure S of R in E, a non-zero prime ideal $Q \subset R$ and a prime $\mathcal{Q} \subset S$ lying above it, and we set $K = \widetilde{F}$ and $L = \widehat{E}$, where the tilde and hat denote completion with respect to the discrete valuations v_Q and $v_{\mathcal{Q}}$, respectively. We would then have that $P_K = QR_Q$ and $P_L = \mathcal{Q}S_{\mathcal{Q}}$, where R_Q and $S_{\mathcal{Q}}$ are the localizations of R and S at Q and $\mathcal{Q}$, respectively.

For example, we might have $R = \mathbb{Z}$, $F = \mathbb{Q}$, E a number field, $S = \mathcal{O}_E$ its ring of integers, $q \in \mathbb{Z}$ a prime number and $\mathcal{Q} \subset S$ a prime ideal lying above it, in which case $K = \mathbb{Q}_q$ and $L = E_{\mathcal{Q}}$.

The following result, which is the Corollary to Prop. 2 in Chapter 1, §5 of [2], shows that the ramification and residue information of the prime $\mathcal{Q}$ over the prime Q in the extension E/F is transferred correctly to the completion L/K.

Proposition 2. For F, H, Q, $\mathcal{Q}$, K, L as above, $e(\mathcal{Q}/Q) = e(L/K)$ and $f(\mathcal{Q}/Q) = f(L/K)$.

In fact, more is true; by Corollary 4 to Theorem 1 in Chapter 1 of [3],

Proposition 3. If E/F is Galois with $\Gamma = \mathrm{Gal}(E/F)$, then L/K is Galois with

$$G = \mathrm{Gal}(L/K) \cong D(\mathcal{Q}/Q) \subseteq \Gamma,$$

where $D(\mathcal{Q}/Q)$ is the decomposition group of $\mathcal{Q}$ over Q in E/F, and the isomorphism is given by taking an automorphism of E and extending it to Cauchy sequences in E, i.e. elements of L.

Proof. Recall that

$$D(\mathcal{Q}/Q) = \{\gamma \in \Gamma \mid \gamma(\mathcal{Q}) = \mathcal{Q}\}.$$

The only $\gamma \in \Gamma$ such that $\gamma : E \to E$ induces an automorphism $\widehat{\gamma}$ of $L = \widehat{E}$, which is the completion with respect to $v_{\mathcal{Q}}$, are those with $v_{\mathcal{Q}}(\gamma(\alpha)) = v_{\mathcal{Q}}(\alpha)$ for all $\alpha \in E$, which is the case if and only if $\gamma(\mathcal{Q}) = \mathcal{Q}$. Thus, we get a (clearly injective) homomorphism $D(\mathcal{Q}/Q) \to G$. Because

$$|D(\mathcal{Q}/Q)| = e(\mathcal{Q}/Q)f(\mathcal{Q}/Q) = e(L/K)f(L/K) = [L : K] = |G|,$$

the homomorphism is in fact an isomorphism. □

Finally, recall the following important subgroup of Γ.

Definition 1. The *inertia group* of $\mathcal{Q}$ over Q in E/F is

$$I(\mathcal{Q}/Q) = \{\gamma \in \Gamma \mid \gamma(\alpha) \equiv \alpha \bmod \mathcal{Q} \text{ for all } \alpha \in S\}$$

Note that $\gamma(\alpha) \equiv \alpha \bmod \mathcal{Q}$ if and only if $\gamma(\alpha) - \alpha \in \mathcal{Q}$ if and only if $v_{\mathcal{Q}}(\gamma(\alpha) - \alpha) > 0$. By the definition of the isomorphism between $D(\mathcal{Q}/Q)$ and G, and by the fact that L is the completion of

E with respect to $v_{\mathcal{Q}}$, we have that the subgroup of G which is identified with $I(\mathcal{Q}/Q) \subseteq D(\mathcal{Q}/Q)$ under our isomorphism is

$$G_0 = \{\sigma \in G \mid v_{\mathcal{Q}}(\sigma(\alpha) - \alpha) > 0 \text{ for all } \alpha \in S_{\mathcal{Q}}\}.$$

In general, we define the inertia group of L/K to be

$$G_0 = \{\sigma \in G \mid v_L(\sigma(\alpha) - \alpha) > 0 \text{ for all } \alpha \in A_L\},$$

which does not require L and K to have come from some E and F. By the well-known fact that $\mathrm{Gal}(\overline{L}/\overline{K}) \cong \Gamma/I(\mathcal{Q}/Q)$, we also have that $\mathrm{Gal}(\overline{L}/\overline{K}) \cong G/G_0$.

The higher ramification groups G_i, which are the subject of this report, are obtained by generalizing the definition of the inertia group of L/K. Together, they form a filtration of G (i.e., a decreasing series of normal subgroups of G), the properties of which allow us to draw strong conclusions about the structure of G. In particular, we will be interested in determining the structure of the non-trivial factor groups.

2 Basic Properties

Let K and L, v_K and v_L, A_K and A_L, P_K and P_L, π_K and π_L be as above. From here on, we will require that L/K is Galois, with Galois group $G = \mathrm{Gal}(L/K)$, and that $\overline{L}/\overline{K}$ is separable.

Definition 2. For any $i \geq -1$, the ith ramification group G_i is defined to be

$$G_i = \{\sigma \in G \mid v_L(\sigma(\alpha) - \alpha) > i \text{ for all } \alpha \in A_L\}.$$

Note that for any $\sigma \in G$, we have that $\sigma(\alpha) - \alpha \in A_L$ for all $\alpha \in L$, and hence $v_L(\sigma(\alpha) - \alpha) \geq 0$ for all $\alpha \in L$. Because v_L is discrete, we therefore have that $G_{-1} = G$. As defined above, G_0 is the inertia group of L/K. Also note that $v_L(\sigma(\alpha) - \alpha) > i$ if and only if $\sigma(\alpha) - \alpha \in P_L^{i+1}$ if and only if $\sigma(\alpha) \equiv \alpha \bmod P_L^{i+1}$, so that

$$G_i = \{\sigma \in G \mid \sigma(\alpha) \equiv \alpha \bmod P_L^{i+1} \text{ for all } \alpha \in A_L\}.$$

The following result is Proposition 1 in Chapter 1, §9 of [2].

Proposition 4. $A_L = A_K[a]$ for some $a \in A_L$.

The proof of this important proposition requires many other results which are somewhat technical and unnecessary for the rest of our discussion, so it will be omitted. Note that this proposition is where the hypothesis that $\overline{L}/\overline{K}$ be separable is necessary.

Definition 3. For some $a \in A_L$ such that $A_L = A_K[a]$, define $i = i_{L/K} : G \to \mathbb{Z} \cup \{\infty\}$ by

$$i(\sigma) = i_{L/K}(\sigma) = v_L(\sigma(a) - a).$$

Among other things, the following proposition shows that this definition is independent of the choice of generator $a \in A_L$.

Proposition 5. For all $i \geq -1$, we have the following properties of G_i and $i : G \to \mathbb{Z} \cup \{\infty\}$:

1. G_i is a normal subgroup of G.
2. $\sigma \in G_i$ if and only if $i(\sigma) \geq i + 1$.
3. For any $\sigma, \tau \in G$, $i(\sigma\tau) \geq \inf(i(\sigma), i(\tau))$.
4. For any $\sigma, \tau \in G$, $i(\tau\sigma\tau^{-1}) = i(\sigma)$.
5. The G_i are decreasing, i.e. $G_i \subseteq G_j$ for $i \geq j$.
6. For sufficiently large i, $G_i = \{\mathrm{id}_L\}$.

Proof. For part 1, note that any $\sigma \in G$ naturally induces an automorphism of the ring A_L/P_L^{i+1} (because $\sigma(P_L^{i+1}) = P_L^{i+1}$ for all i). Because G_i is the kernel of the map $G \to \mathrm{Aut}(A_L/P_L^{i+1})$, we have that G_i is normal in G for all $i \geq -1$.

For part 2, note that $\sigma \in G_i$ if and only if $v_L(\sigma(\alpha) - \alpha) > i$ for all $\alpha \in A_L$, hence $i(\sigma) = v_L(\sigma(a) - a) > i$, hence $i(\sigma) \geq i + 1$. Conversely, if $i(\sigma) \geq i + 1$, then $v_L(\sigma(a) - a) \geq i + 1$, hence $\sigma(a) \equiv a \bmod P_L^{i+1}$. But because $\sigma \in G = \mathrm{Gal}(L/K)$, we have that $\sigma(\alpha) = \alpha$ for $\alpha \in A_K$, so that certainly $\sigma(\alpha) \equiv \alpha \bmod P_L^{i+1}$ for all $\alpha \in A_K$, and a generates A_L as an algebra over A_K, so we must have that $\sigma(\alpha) \equiv \alpha \bmod P_L^{i+1}$ for all $\alpha \in A_L$. Thus $\sigma \in G_i$.

For part 3, note that if $j = \inf(i(\sigma), i(\tau)) - 1 = \inf(i(\sigma) - 1, i(\tau) - 1)$, then $i(\sigma) \geq j + 1$ and $i(\tau) \geq j + 1$, which by part 2 implies $\sigma \in G_j$ and $\tau \in G_j$, hence $\sigma\tau \in G_j$, hence $i(\sigma\tau) \geq j + 1$, and thus $i(\sigma\tau) \geq \inf(i(\sigma), i(\tau))$.

For part 4, note that by part 1, $\sigma \in G_i$ if and only if $\tau\sigma\tau^{-1} \in G_i$ for all $\tau \in G$, so by part 2, $i(\sigma) \geq i + 1$ if and only if $i(\tau\sigma\tau^{-1}) \geq i + 1$, for all i. Thus $i(\tau\sigma\tau^{-1}) = i(\sigma)$.

Part 5 is obvious from the definition of the G_i.

For part 6, note that $i(\mathrm{id}_L) = v_L(0) = \infty$, but if we set $m = \sup_{\sigma \neq \mathrm{id}_L}(i(\sigma))$, then no $\sigma \in G$, $\sigma \neq \mathrm{id}_L$ has $i(\sigma) \geq m + 1$, so that $G_m = \{\mathrm{id}_L\}$. By part 5, we have $G_i = \{\mathrm{id}_L\}$ for all $i \geq m$. □

Part 2 of this proposition shows that, because the elements of each G_i are what they are, independent of our choice of generator $a \in A_L$ in the definition of $i = i_{L/K}$, we must have that for any choice, the function is the same. Furthermore, it shows that knowing the function $i_{L/K}$ is actually equivalent to knowing all the groups G_i.

For a subgroup $H \subseteq G = \mathrm{Gal}(L/K)$, let K' be the fixed field of H, so that L/K' is Galois with $H = \mathrm{Gal}(L/K')$. Because the residue field $\overline{K'}$ is an intermediate field of the extension $\overline{L}/\overline{K}$, which by assumption is separable, we also have that $\overline{L}/\overline{K'}$ is separable. Thus we can apply our results above, so that we get a filtration H_i on H, and a function $i_{L/K'} : H \to \mathbb{Z} \cup \{\infty\}$. The following (obvious) result shows that the H_i are easy to compute:

Proposition 6. For any subgroup $H \subseteq G$, we have $H_i = H \cap G_i$.

Proof. Because G_i is the kernel of the map $G \to \mathrm{Aut}(A_L/P_L^{i+1})$ and H_i is the kernel of the map $H \to \mathrm{Aut}(A_L/P_L^{i+1})$, we have that $H_i = H \cap G_i$. □

3 The Structure of G_i/G_{i+1}

Let $U_L = A_L - P_L$ be the unit group of A_L. We define the following subgroups:

$$U_i = 1 + P_L^i \subseteq U_L.$$

Note that $U_0 = U_L$.

Proposition 7. The quotient map $A_L \to A_L/P_L = \overline{L}$ induces an isomorphism

$$U_0/U_1 \cong \overline{L}^{\times}.$$

For each $n \geq 1$, the map $u \mapsto u - 1$ induces an isomorphism

$$U_n/U_{n+1} \cong P_L^n/P_L^{n+1}.$$

Proof. Because $U_0 = A_L - P_L$, and $A_L \to A_L/P_L$ is surjective, and P_L is its kernel, we have that the image of U_0 is $\overline{L}^{\times}$. Forgetting about the additive structure, this is a surjective homomorphism from the group U_0 to the group $\overline{L}^{\times}$. The kernel consists of those units which get sent to $1 + P_L$, which by definition is U_1.

For each $n \geq 1$, we have that the map $f : U_n/U_{n+1} \to P_L^n/P_L^{n+1}$ defined by $f(u + U_{n+1}) = (u - 1) + P_L^{n+1}$ is a homomorphism, because for any $u, v \in U_n$,

$$(uv - 1) - (u - 1) - (v - 1) = uv - u - v + 1 = (u - 1)(v - 1) \in P_L^{2n} \subseteq P_L^{n+1}$$

and therefore

$$f(u + U_{n+1}) + f(v + U_{n+1}) = ((u - 1) + P_L^{n+1}) + ((v - 1) + P_L^{n+1}) = (u - 1) + (v - 1) + P_L^{n+1} =$$

$$(uv - 1) + P_L^{n+1} = f(uv + U_{n+1}),$$

Its inverse is similarly defined and seen to be a homomorphism. □

Corollary 1. *If $\overline{L}$ is of characteristic p, then for $n \geq 1$, $U_n^p \subseteq U_{n+1}^p$.*

Proof. Because $U_n/U_{n+1} \cong P_L^n/P_L^{n+1}$, and P_L^n/P_L^{n+1} is an A_L-module which is annihilated by P_L, we have that U_n/U_{n+1} is a one-dimensional $\overline{L}$-vector space. Therefore, if $\overline{L}$ is of characteristic p, then $(u + U_{n+1})^p = u^p + U_{n+1} = 1 + U_{n+1}$ for all $u \in U_n$, hence $U_n^p \subseteq U_{n+1}$. □

Theorem 1. *Let $i \geq 0$. Then $\sigma \in G_i$ if and only if $\frac{\sigma(x)}{x} \in U_i$ for all $x \in L^\times$.*

Proof. Because $G_i \subseteq G_0$ for all $i \geq 1$, we can assume $\sigma \in G_0$. By Proposition 6, we can WLOG replace K by K_r, the fixed field of G_0, because it will have the same ramification groups (again because $G_i \subseteq G_0$ for all $i \geq 1$). The intermediate field K_r is the largest subfield such that K_r/K is unramified, and furthermore has the property that L/K_r is totally ramified. Thus, by Proposition 18 in Chapter 1, §6 of [3], we can now choose a generator a of A_L over A_{K_r} that is an element of P_L. Suppose that $\frac{\sigma(x)}{x} \in U_i$ for all $x \in L^\times$. Then in particular $\frac{\sigma(a)}{a} \in U_i$, so that $\frac{\sigma(a)}{a} - 1 \in P_L^i$, hence $v_L(\frac{\sigma(a)}{a} - 1) \geq i$, and hence

$$i(\sigma) = v_L(\sigma(a) - a) = v_L(a(\tfrac{\sigma(a)}{a} - 1)) = v_L(a) + v_L(\tfrac{\sigma(a)}{a} - 1) \geq i + 1.$$

Conversely, if $\sigma \in G_i$, then for any $x \in L^\times$, we have that

$$v_L(\tfrac{\sigma(x)}{x} - 1) = \tfrac{v_L(\sigma(x) - x)}{v_L(x)} = v_L(\sigma(x) - x) \geq i + 1$$

so that $\frac{\sigma(x)}{x} - 1 \in P_L^{i+1}$, so that $\frac{\sigma(x)}{x} \in U_{i+1} \subseteq U_i$. □

Theorem 2. *Let $i \geq 0$. Then the function defined by*

$$\theta_i(\sigma) = \frac{\sigma(\pi_L)}{\pi_L} \bmod U_{i+1}$$

is a homomorphism $\theta_i : G_i \to U_i/U_{i+1}$ which is independent of the choice of uniformizer π_L, and whose kernel is G_{i+1}.

Proof. Let $\sigma \in G_i$. By Theorem 1, $\frac{\sigma(\pi_L)}{\pi_L} \in U_i$, so θ_i is a well-defined map from G_i to U_i/U_{i+1}. Note that any other uniformizer Π for L differs from π_L by a unit, say $\Pi = u\pi_L$ for $u \in U_L$, so that

$$\frac{\sigma(\Pi)}{\Pi} = \frac{\sigma(\pi_L)}{\pi_L}\frac{\sigma(u)}{u}$$

Because $\sigma \in G_i$, we have $\sigma(u) \equiv u \bmod P_L^{i+1}$ and thus $\frac{\sigma(u)}{u} \equiv 1 \bmod U_{i+1}$. Therefore, θ_i is independent of the choice of uniformizer. To see that θ_i is a homomorphism, note that for any $\sigma, \tau \in G_i$,

$$\theta_i(\sigma\tau) = \frac{\sigma\tau(\pi_L)}{\pi_L} \bmod U_{i+1} = \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L}\frac{\sigma(\frac{\tau(\pi_L)}{\pi_L})}{\frac{\tau(\pi_L)}{\pi_L}} \bmod U_{i+1}$$

Because $\frac{\tau(\pi_L)}{\pi_L} \in U_L$, we again have that $\sigma(\frac{\tau(\pi_L)}{\pi_L}) \equiv \frac{\tau(\pi_L)}{\pi_L} \bmod U_{i+1}$, hence

$$\frac{\sigma(\frac{\tau(\pi_L)}{\pi_L})}{\frac{\tau(\pi_L)}{\pi_L}} \equiv 1 \bmod U_{i+1}$$

and thus $\theta_i(\sigma\tau) = \frac{\sigma(\pi_L)}{\pi_L}\frac{\tau(\pi_L)}{\pi_L} = \theta_i(\sigma)\theta_i(\tau)$. Finally, note that σ is in the kernel of θ_i if and only if $\frac{\sigma(\pi_L)}{\pi_L} \in U_{i+1}$, which is the case precisely when

$$i(\sigma) - 1 = v_L(\sigma(\pi_L) - \pi_L) - 1 = v_L(\frac{\sigma(\pi_L)}{\pi_L} - 1) \geq i + 1,$$

i.e. $i(\sigma) \geq i + 2$, which by Proposition 5 is equivalent to $\sigma \in G_{i+1}$. □

Lemma 1. *The group G_0/G_1 is cyclic, of order relatively prime to the characteristic of $\overline{L}$.*

Proof. By Proposition 7, $U_0/U_1 \cong \overline{L}^{\times}$. Because G_0 is finite, we have by Theorem 2 that G_0/G_1 is isomorphic to a finite subgroup of $\overline{L}^{\times}$. It is well-known that any finite subgroup of the multiplicative group of a field is cyclic, and it is clear that if the characateristic of $\overline{L}$ is $p > 0$, then the order of any finite subgroup of $\overline{L}^{\times}$ is relatively prime to p. □

Theorem 3. *If the characteristic of $\overline{L}$ is $p > 0$, then for every $i \geq 1$, the factor group G_i/G_{i+1} is a finite abelian p-group, and in fact a direct sum of cyclic groups of order p; hence G_1 is a p-group. If the characteristic of $\overline{L}$ is 0, then G_1 is trivial, and G_0 is cyclic.*

Proof. Theorem 2 shows that we have an injection from G_i/G_{i+1} into U_i/U_{i+1} for all $i \geq 0$. The corollary to Proposition 7 shows that if the characteristic of $\overline{K}$ is $p > 0$, then for $i \geq 1$, U_i/U_{i+1} is an abelian group annihilated by p, hence a direct sum of cyclic groups of order p. Because $G = \mathrm{Gal}(L/F)$ is finite and $G_i \subseteq G$ for all i, we have that for all $i \geq 1$, G_i/G_{i+1} is a finite abelian p-group, and indeed a finite direct sum of cyclic groups of order p. Thus $|G_1|$ is a power of p, and hence G_1 is a p-group.

On the other hand, if the characteristic of $\overline{L}$ is 0, then by Proposition 7, which tells us that $U_i/U_{i+1} \cong P_L^i/P_L^{i+1} \cong \overline{L}$ for $i \geq 1$, we know that U_i/U_{i+1} will have no non-trivial finite subgroups for $i \geq 1$ (because $\overline{L}$ is of characteristic 0). But every G_i is finite, hence G_i/G_{i+1} is finite, hence the image of G_i/G_{i+1} in U_i/U_{i+1} is finite, and therefore trivial. Thus, for $i \geq 1$, we have that $G_i = G_{i+1}$, and by Proposition 5 we know that eventually G_i is trivial, so that every G_i for $i \geq 1$ is trivial. Thus G_1 is trivial. Finally, because G_1 is trivial and G_0/G_1 is cyclic by the above Lemma, we have that G_0 is cyclic. □

4 An Application to Puiseux Series

The field of Puiseux series over a field k is a generalization of $k((T))$, the field of Laurent series over k, which allows for rational powers of the indeterminate T instead of just integers. Specifically, the field of Puiseux series $k\{\{T\}\}$ over k is defined to be $\bigcup_{n=1}^{\infty} K_n$, where $K_n = k((T^{1/n}))$ and the $T^{1/n}$ all live in some algebraic closure of $k((T))$. The following is Puiseux's Theorem for an arbitrary field k (when k is complete with respect to a valuation, there is a separate theorem concerning the subfield of convergent series in $k\{\{T\}\}$).

Puiseux's Theorem. Let k be an algebraically closed field of characteristic 0. Then the algebraic closure of $k((T))$ is $k\{\{T\}\}$.

Proof. We follow the proof in Proposition 8 in Chapter 4 of [3]. Let $K = k((T))$, and let K^{alg} be an algebraic closure of K. Let L/K be a finite Galois subextension of K^{alg}/K, with Galois group $G = \mathrm{Gal}(L/K)$. Clearly, the residue field of $K = k((T))$ relative to the prime ideal (T) in $k[[T]]$ is $\overline{K} = k$, which is algebraically closed by hypothesis. Because $\overline{L}/\overline{K}$ is finite, we must therefore have that $\overline{L} = \overline{K}$. Because $\mathrm{Gal}(\overline{L}/\overline{K}) \cong G/G_0$, we have that $G = G_0$. Because K is of characteristic 0, then by Theorem 3, we have that G is cyclic. Let L'/K be another finite Galois subextension of K^{alg}/K such that $[L : K]$ divides $[L' : K]$. Then LL'/K is also finite and Galois, and hence by the same argument $\mathrm{Gal}(LL'/K)$ is cyclic. Because the subgroups of a cyclic group are totally ordered by inclusion and

$$|\,\mathrm{Gal}(LL'/L')| = \frac{[LL' : K]}{[L' : K]} \leq \frac{[LL' : K]}{[L : K]} = |\,\mathrm{Gal}(LL'/L)|,$$

we must have that $\mathrm{Gal}(LL'/L') \subseteq \mathrm{Gal}(LL'/L)$ and hence $L \subseteq L'$. Thus, for any finite Galois subextension L/K of degree $n = [L : K]$, we have that $L \subseteq K_n$ because $[K_n : K] = n$, and hence $L \subseteq k\{\{T\}\} = \bigcup_{n=1}^{\infty} K_n$. Because any element $a \in K^{alg}$ is an element of a finite Galois subextension (e.g., the normal closure in K^{alg} of $K(a)$), we have that every element of K^{alg} is in $k\{\{T\}\}$, and hence $K^{alg} \subseteq k\{\{T\}\}$. But

$$k\{\{T\}\} = \textstyle\bigcup_{n=1}^{\infty} K_n = K(T^{1/2}, T^{1/3}, \ldots) \subseteq K^{alg}$$

by definition, so that $K^{alg} = k\{\{T\}\}$. □

5 The Upper Numbering

Many results about higher ramification groups depend on giving them a special renumbering, called the *upper numbering*. This is calculated via the *Herbrand function*. For example, this is used to establish Herbrand's Theorem, which describes the ramification groups of a Galois subextension F/K of L/K in terms of those of L/K itself.

The proofs of the results in this section require many lemmas which are technical and unnecessary for the rest of our discussion, so they will be omitted.

First, we extend the usual (or *lower*) numbering of the ramification groups to real numbers, by defining for any real $u \geq -1$

$$G_u = G_i, \text{ where } i = \lceil u \rceil.$$

Definition 4. The *Herbrand function* $\phi_{L/K} : [-1, \infty) \to [-1, \infty)$ is defined by

$$\phi_{L/K}(u) = \begin{cases} \displaystyle\int_0^u \frac{1}{[G_0 : G_t]}\, dt, & \text{if } 0 \leq u \\ u & \text{if } -1 \leq u \leq 0 \end{cases}$$

From this definition, it's clear that the function $\phi_{L/K}$ is continuous and strictly increasing, and therefore has an inverse $\psi_{L/K} : [-1, \infty) \to [-1, \infty)$. We then define the *upper numbering* of the ramification groups by, for any real $v \geq -1$,

$$G^v = G_{\psi_{L/K}(v)}, \text{ or equivalently, } G_u = G^{\phi_{L/K}(u)}.$$

Recall that subgroups $H \subseteq G$ correspond to extensions L/F for $K \subseteq F \subseteq L$, and that to compute the higher ramification groups of L/F, we have the simple result of Proposition 6: $H_i = H \cap G_i$. Now let $H \triangleleft G$ be a normal subgroup with fixed field F, so that F/K is a Galois extension with Galois group isomorphic to G/H. The upper numbering is necessary to state the natural analog for the higher ramification groups of F/K:

Theorem 4. *For a normal subgroup $H \triangleleft G$, we have $(G/H)^v = G^v H/H$ for all real $v \geq -1$.*

Indeed, as Serre states in [3], "the upper numbering is adapted to quotients, just as the lower numbering is adapted to subgroups." We also have the following results.

Herbrand's Theorem. If $v = \phi_{L/K}(u)$, then $G_u H/H = (G/H)_v$.

Hasse-Arf Theorem. If G is abelian and v is a jump in the filtration in the upper numbering, i.e. $G^v \neq G^{v+1}$, then v is an integer. Equivalently, if $G_u \neq G_{u+1}$, then $\phi_{L/K}(u)$ is an integer.

References

[1] J.W.S. Cassels, *Local Fields*, pp. 134–137, Cambridge University Press, Cambridge, 1986.

[2] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, 2nd ed., London Mathematical Society, London, 2010.

[3] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, New York, 1979.