On Galois Extensions of Local Fields with a Single Wild Ramification Jump

Samuel Goodman

May 2024

Introduction

Fix a local field K, for example a finite extension of $\mathbb{Q}_p$. A classical question is counting the number of tamely ramified extensions of K of a given degree, which in turn is done by Serre's mass formula (see [3]), giving precisely n degree n totally tamely ramified extensions (where $p \nmid n$), and then since a tamely ramified extension is uniquely a totally tamely ramified extension of its maximal unramified one and there is a unique unramified degree k extension of K for each k, we find there are $\sigma_0(n)$ tamely ramified degree n extensions, where $\sigma_0(n)$ is the sum of the divisors of n coprime to p.

Using Kummer theory and the explicit description of tamely ramified Galois extensions or more elementary techniques (see [1]), one can also obtain the following result:

Let $K/\mathbb{Q}_p$ be a finite extension and let L be a finite unramified extension of K. Set $q = |k|$. Then there are $\gcd(n, q-1)$ tamely ramified Galois extensions M/K such that $L \subset M$ and M/L is totally ramified of degree n.

This Kummer Theory approach quickly devolves into a certain counting of fixed points under the Galois group of the unramified part, something which we greatly build upon using class field theory in a broader context. In terms of ramification jumps, tamely ramified Galois extensions can be thought of as $(0, 1)$ Galois extensions since tamely ramified Galois extensions have ramification jumps only at 0 and 1. The next natural question to ask is how to count $(0, n)$ extensions for a given positive integer n; these are the extensions with only a single wild ramification jump.

In this paper, we briefly sketch the relatively straightforward $(0, 2)$ case and then give a complete treatment of the $(0, 3)$ case, effectively determining explicit formulas for the number of $(0, 3)$ extensions given a particular unramified K/K_1 setup (with K corresponding to the maximal unramified extension). In fact, we determine explicit formulas in the cases when $K_1/\mathbb{Q}_p$ is totally ramified and when it is unramified.

1 Preliminaries

We start by noting an immediate consequence of [2] (p. 67, Prop. 7):

Proposition 1.1

Let L/K be a Galois extension with Galois group G. Set $G_0 = I$ and let G_i be the ith higher ramification group for $i \geq 1$. Then we have:

1) G_0/G_1 is isomorphic to a subgroup of $l^\times$, where l is the residue field of L.

2) For $i \geq 1$, $G_i/G_{i+1} \cong (\mathbb{Z}/p\mathbb{Z})^k$ for some k, and so in particular, G_1 is a p-group.

Letting π be a uniformizer for L/K and assuming the extension L/K is totally ramified, we have that $\mathcal{O}_L = \mathcal{O}_K[\pi]$ and so the ramification groups are determined by π. More precisely, letting $\mathrm{Gal}(L/K) = G$, we have that $G_n = \{\sigma \in G, \sigma(\pi) \equiv \pi \mod \mathfrak{m}^{n+1}\}$, where $\mathfrak{m} = (\pi)$ is the maximal ideal of $\mathcal{O}_L$. We will later seek to better understand these ramification groups.

Proposition 1.2

Let $M/L/K$ be a series of finite extensions of local fields such that M/L is abelian and L/K is Galois. Let H be the norm subgroup of $L^\times$ associated to M under LCFT. Then M/K is Galois iff $\sigma(H) = H$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Proof. M/K being Galois is equivalent to $\sigma(M) = M$ for all $\sigma : M \to \bar{K}$ an embedding fixing K. Since L/K is Galois, $\sigma(L) = L$ for all such embeddings and thus $\sigma(M)/L$ is an abelian extension. Its norm group is clearly $\sigma(H)$. However, LCFT gives an order-reversing bijection between norm groups and finite abelian extensions, and so we have that $\sigma(M) = M$ for all σ iff $\sigma(H) = H$ for all σ. But $\sigma|_L$ precisely attains the elements of $\mathrm{Gal}(L/K)$, and so we conclude. □

2 Ramification Groups

We now prove some general results about ramification groups. We start with Herbrand's Theorem, which states that $G_u H/H = (G/H)_v$, where $v = \phi_{L/K}(u)$. We are interested in the case of Galois extensions where there is a single jump in the wild ramification groups. We now characterize such extensions in the context of Lubin-Tate Theory. As before, we have that $G = \mathrm{Gal}(K_{\pi,n}/K) \cong$

$\mathcal{O}_K^\times/(1+\mathfrak{m}^n)$ and so view subgroups of G in terms of subgroups of $\mathcal{O}_K^\times/(1+\mathfrak{m}^n)$. We say that an subextension L/K with corresponding subgroup H has a (lower) ramification jump at u if $(G/H)_{u-1} \neq (G/H)_u$.

Lemma 2.1

Suppose that $K_{\pi,n}/K$ is a Lubin-Tate extension with Galois group G. The subextensions L/K with a single wild ramification jump at k correspond to the proper subgroups H of G that both contain $(1+\mathfrak{m}^k)/(1+\mathfrak{m}^n)$ and have the property that the canonical map $H \to \mathcal{O}_K^\times/(1+\mathfrak{m}^{k-1})$ is surjective under the identification $G \cong \mathcal{O}_K^\times/(1+\mathfrak{m}^n)$.

Proof. Now recall from Lubin-Tate theory that if $m < q^n, q^k \leq m < q^{k+1}$, we have that $G_m = (1+\mathfrak{m}^k)/(1+\mathfrak{m}^n)$. It follows that $G^{k+1} = G_{q^k}$ for each $0 \leq k < n$.

Next note that Galois extensions with a single positive ramification jump have $G_{\phi_{L/K}(v)} = G_v$ for all v. Indeed, letting the jump be at k, we have that for $v \leq k$, $G_{\phi_{L/K}(v)} = G_v$, where $\phi_{L/K}(v) = v$ follows since $[G_0 : G_v] = 1$ for all $0 \leq v < k$. On the other hand, for $v > k$, both are trivial since then $k < \phi_{L/K}(v) < v$. Thus the upper numbering and lower numbering groups coincide for such extensions.

There being a unique jump at k is equivalent to $(G/H)^k = 1$ and $(G/H)^{k'} = (G/H)^0$ for $1 \leq k' < k$ by definition as these coincide with the lower ramification groups. By Herbrand's Theorem, this is equivalent to having $G^{k+1} = G_{q^k} \subset H$ and $G_{q^{k'}}H/H = (G/H)_0$ for $1 \leq k' < k$. The former condition is equivalent to containing $(1+\mathfrak{m}^k)/(1+\mathfrak{m}^n)$. The latter just means that $G_{q^{k'}}H$ is constant for $1 \leq k' < k$, which is equivalent to having the condition that $H \to \mathcal{O}_K^\times/(1+\mathfrak{m}^{k'})$ is surjective for $1 \leq k' < k$. However, surjectivity at $k-1$ implies surjectivity elsewhere, implying the claim. □

We now use Lemma 2.1 to say more about the H such that there is a single jump at 2 or 3. For 2, the second condition is superfluous, and so it is enough to contain $(1+\mathfrak{m}^2)/(1+\mathfrak{m}^n)$. By Proposition 2.1 and class field theory, this implies that $L \subset K_{\pi,2}$, and so these are precisely the working extensions.

If we assume that there only a single jump at q, then we must also have that the map $H \to \mathcal{O}_K^\times/(1+\mathfrak{m})$ is surjective. However, we know that H is isomorphic to a subgroup of $\mathcal{O}_K^\times/(1+\mathfrak{m}^2)$, which has p-Sylow group $(1+\mathfrak{m})/(1+\mathfrak{m}^2)$ and cyclic subgroup of order $q-1$ generated by the coset of μ_{q-1}, giving a splitting $\mathcal{O}_K^\times/(1+\mathfrak{m}^2) \cong k^+ \times k^\times$, where k is the residue field of K, where the isomorphism is induced upon fixing a uniformizer π. Any subgroup of this group will be isomorphic to the direct product of its Sylow subgroups, thus isomorphic to a product of subgroups k_1, k_2 of $k^+, k^\times$, respectively.

Surjectivity is then equivalent to k_2 being all of $k^\times$. Now let $a \in k$ and note that the coset H_a of H of elements congruent to $a \mod \mathfrak{m}$ is just $(a + (f(a) + k_1)\pi)/(1 + \mathfrak{m}^2)$ for some unique coset $f(a)$ of k^+/k_1. We must then have that $H_a H_b = H_{ab}$, which implies that $af(b) + bf(a) \equiv f(ab) \mod k_1$. Now since there a unique subgroup H with a given k_1 and every f gives a different subgroup with that corresponding k_1, we conclude that for any subgroup k_1 of k^+, the unique "differential" of the form $f : k \to k^+/k_1$ is the zero differential. Thus the 2 case is encapsulating the differential information of the residue field. The case of 3 can thus be seen as a more complicated type of differential.

Now we investigate this case. First we need some lemmas on finite fields.

3 Finite Fields

Lemma 3.1

Let k be a finite field of characteristic p and h, h' subgroups of k^+. Let $r = \dim_{\mathbb{F}_p}(h')$. Say that $h \sim h'$ if $x^2 \in h$ for each $x \in h'$. Then the number of functions $f : h' \to k^+/h$ such that $f(a+b) \equiv f(a) + f(b) + ab \mod h$ is

$$\begin{cases} 0 & p = 2, h \not\sim h' \\ p^{r(\operatorname{codim}_{\mathbb{F}_p}(h))} & \text{else} \end{cases}$$

.

Proof. From this relation and an easy induction, we deduce

$$f(\sum_{i=1}^{r} a_i) \equiv \sum_{i=1}^{r} f(a_i) + \sum_{1 \le i < j \le r} a_i a_j \mod h$$

which in particular implies that for any positive integer r, $f(ra) \equiv rf(a) + \binom{r}{2}a^2 \mod h$ upon setting all a_is equal. If $h \sim h'$ or $p \neq 2$, we find that $f(pa) \equiv 0 \mod h$ and so f is in fact well-defined. If $p = 2$ and $h \not\sim h'$, then we get a contradiction since we would need $a^2 \equiv 0 \mod h$ for all $a \in h'$, meaning that no such functions can exist.

Now let $e_1, \cdots, e_r$ be an $\mathbb{F}_p$-basis for h'. Upon choosing $f(e_i)$, the above relation gives $f(re_i) \equiv rf(e_i) + \binom{r}{2}e_i^2 \mod h$, and so $f(re_i)$ is determined by $f(e_i)$. Furthermore, we must have

$$f(\sum_{i=1}^{n} a_i e_i) \equiv \sum_{i=1}^{n} a_i f(e_i) + \binom{a_i}{2} e_i^2 + \sum_{1 \le i < j \le n} a_i a_j e_i e_j \mod h$$

and so f is completely determined by f on the basis.

The condition $f(a+b) \equiv f(a) + f(b) + ab \mod h$ is equivalent to

$$f(\sum_{i=1}^{n}(a_i+b_i)e_i) = f(\sum_{i=1}^{n} a_ie_i) + f(\sum_{i=1}^{n} b_ie_i) + (\sum_{i=1}^{n} a_ie_i)(\sum_{i=1}^{n} b_ie_i)$$

Using the known value of f, this gives

$$\sum_{i=1}^{n}(a_i+b_i)f(e_i)+\binom{a_i+b_i}{2}e_i^2+\sum_{1\leq i<j\leq n}(a_i+b_i)(a_j+b_j)e_ie_j \equiv \sum_{i=1}^{n}(a_i+b_i)f(e_i)+$$

$$(\binom{a_i}{2}+\binom{b_i}{2})e_i^2+\sum_{1\leq i<j\leq n}(a_ia_j+b_ib_j)e_ie_j+(\sum_{i=1}^{n}a_ie_i)(\sum_{i=1}^{n}b_ie_i) \mod h$$

which is an equality. Thus any choice of f on a basis determines a working f on all of k. As there are $p^{\mathrm{codim}_{\mathbb{F}_p}(h)}$ choices of coset for each basis element, this gives a total of $p^{r\mathrm{codim}_{\mathbb{F}_p}(h)}$ total choices of f. □

Lemma 3.2

Let k be a finite field of characteristic p, $k'/\mathbb{F}_p$ a subextension of $k/\mathbb{F}_p$, h a Galois invariant subgroup of k^+. Let $q = |k'|$. Then the number of Galois equivariant functions $f : k^+ \to k^+/h$ such that $f(a+b) \equiv f(a)+f(b)+ab \mod h$ is

$$\begin{cases} 0 & p=2 \\ q^{\mathrm{codim}_{\mathbb{F}_p}(h)} & p>2 \end{cases}$$

Proof. By definition, we need to have $\sigma(f(a)) = f(\sigma(a))$ for all $a \in k$. Let $e_1, \cdots, e_r$ be a Galois invariant $\mathbb{F}_p$-basis for k.

We claim that it is enough to it be equivariant on the e_is. Indeed, if it is, then representing $a = \sum_{i=1}^{r} a_ie_i$, we have

$$\sigma(f(a)) \equiv f(\sigma(\sum_{i=1}^{r} a_ie_i)) \equiv \sum_{i=1}^{s} a_i\sigma(f(e_i)) + \binom{a_i}{2}\sigma(e_i^2) + \sum_{1\leq i<j\leq r}\sigma(a_ia_je_ie_j)$$

$$\equiv \sum_{i=1}^{r} a_if(\sigma(e_i)) + \binom{a_i}{2}\sigma(e_i)^2 + \sum_{1\leq i<j\leq r} a_ia_j\sigma(e_i)\sigma(e_j) \equiv f(\sigma(a)) \mod h$$

proving the claim.

By the Galois module structure for $\mathbb{F}_{p^n}$, we can choose a basis for k over $\mathbb{F}_p$ of the form $\sigma_i(a_j), 1 \leq i \leq r, 1 \leq j \leq s$. Then given any choice of $f(\sigma_1(a_1)), \cdots, f(\sigma_1(a_r))$, we must have that $f(\sigma_k(a_j)) = \sigma_k(f(a_j))$, which determines f on the part of basis consisting of the conjugates of a_j and thus on the entire basis.

By the proof of Lemma 3.1, any choice of f on an $\mathbb{F}_p$-basis for some $p \neq 2$ uniquely determines a function satisfying $f(a+b) = f(a) + f(b) + ab$ and for $p = 2$, there are no such functions since $k^+ \not\sim h$ as h is proper and the squaring map is surjective on k. As any such function is automatically equivariant on the basis, it must be equivariant on all of k. But then there are $|k|/|h|$ choices of coset for each $f(\sigma_1(a_j))$, giving $(|k|/|h|)^s = q^{\operatorname{codim}_{\mathbb{F}_p}(h)}$ total choices. □

Lemma 3.3

Let t be the trace 0 subspace of $l = \mathbb{F}_{p^k}$, i.e. the kernel of the trace map $\mathbb{F}_{p^k} \to \mathbb{F}_p$, let $l' = \mathbb{F}_{p^{k'}}$ be a subfield, and $G = \mathrm{Gal}(l/l')$ with g a generator. Set $r = |G|$ and $s = \frac{k}{r}$. Then there is an $\mathbb{F}_p$-basis for t of the form $\{g^i \alpha_j, 0 \leq i \leq r-1, 1 \leq i \leq s-1\} \cup \{g^i(g-1)\alpha_s, 0 \leq i \leq r-2\}$.

Proof. We start with the $\mathbb{F}_p[x]$-module structure of l, where x acts as multiplication by g, which is $\prod_{i=1}^s \mathbb{F}_p[x]/(x^r - 1)$. Note that t is a G-invariant subspace since any l'-conjugate is certainly an $\mathbb{F}_p$-conjugate. Hence it also is naturally endowed with the structure of a $\mathbb{F}_p[x]$-module, and so it too has a decomposition into elementary divisors $\prod_{i=1}^m \mathbb{F}_p[x]/(p_i(x)^{e_i})$ according to the structure theorem (so that the p_is are irreducible).

Then note that multiplication by $x - 1$ on $\prod_{i=1}^s \mathbb{F}_p[x]/(x^r - 1)$ gives a submodule of t under this isomorphism, meaning that t contains the submodule $\prod_{i=1}^s (x-1)/(x^r - 1)$ and thus a submodule isomorphic to $\prod_{i=1}^s \mathbb{F}_p[x]/(\frac{x^r-1}{x-1})$. Breaking both these submodules into their invariant factor decompositions and choosing any monic irreducible $p(x) \neq x - 1$ in these decompositions, it follows that the dimension of the $p(x)^e$ is the same for both of these for any e, and so it follows that t has identical $p(x)^e$-torsion, and so in particular these elementary divisors match.

The only other possibility for a $p_i(x)$ in the decomposition for t is $x - 1$ itself, and by considering $(x-1)^e$ torsion in $\prod_{i=1}^s \mathbb{F}_p[x]/(\frac{x^r-1}{x-1})$, we see that all exponents must be at least one less than the common exponent in the decomposition of k^+. For dimension reasons, we must then have that all exponents are equal except for one which is one less. Thus we get an elementary divisor decomposition of t of the form $\prod_{i=1}^{s-1} \mathbb{F}_p[x]/(x^r - 1) \oplus \mathbb{F}_p[x]/(\frac{x^r-1}{x-1})$. The element corresponding to 1 in the last summand and 0 elsewhere is in the kernel of the trace map $\mathrm{Tr}_{l/l'}$, and thus is of the form $(g-1)\alpha_s$ for some α_s (by a counting argument or Hilbert 90), completing the proof. □

Lemma 3.4

Let k be a finite field of characteristic 2 with $[k : \mathbb{F}_2] = n$ and choose $\alpha \in k$. Let $q = 2^r$ be a prime power with $n = rm$ so that $m \geq 2$ and set $\alpha_i = \alpha^{q^i} + \alpha^{q^{i+1}}$.

Let t be the trace 0 subspace. Then $\sum_{0\le i<j<m}\alpha_i\alpha_j \equiv \alpha^{q+1}+\alpha \mod t$ if m is odd and $0 \mod t$ if m is even.

Proof. Note that $\sum_{0\le i<j<m}\alpha_i\alpha_j = \sum_{0\le i<j<m}\alpha^{q^i+q^j}+\alpha^{q^{i+1}+q^{j+1}}+\alpha^{q^{i+1}+q^j}+\alpha^{q^i+q^{j+1}}$. First note that the pairs $\mod m$ obtained by $(i+1,j+1)$ for $0\le i<j<m$ are just the pairs (i,j) for $1\le i<j\le m$. Hence these completely overlap the (i,j) pairs with $0\le i<j<m$ except for those with $i=0$ in the latter case and $j=m$ in the former. Hence this part of the sum just becomes $\sum_{0<i<m}\alpha^{1+q^i}+\sum_{1\le i<m}\alpha^{q^i+q^m}=\sum_{0<i<m}\alpha^{1+q^i}+\alpha^{q^i+q^m}=0$.

Hence we just need to determine $\sum_{0\le i<j<m}\alpha^{q^{i+1}+q^j}+\alpha^{q^i+q^{j+1}}$. The pairs $(i+1,j)$ obtained for $0\le i<j<m$ are precisely those of the form (i,j) for $1\le i\le j<m$ while the pairs $(i,j+1)$ obtained for $0\le i<j<m$ are precisely those of the form (i,j) for $0\le i<j\le m$ with $i+1<j$. The pairs (i,j) for $1\le i\le j<m$ that are not of the form (i,j) for $0\le i<j\le m$ with $i+1<j$ are precisely those with $i=j$ or $i+1=j$ while the pairs (i,j) for $0\le i<j\le m$ with $i+1<j$ that are not of the form (i,j) for $1\le i\le j<m$ are precisely those with $i=0$ or $j=m$. Hence all terms in the sum cancel out except these (since they all other pairs will have exactly 2 copies), leaving $\sum_{1\le i<m}\alpha^{2q^i}+\sum_{1\le i<m-1}a^{q^i+q^{i+1}}+\sum_{j=2}^{m}a^{1+q^j}+\sum_{i=0}^{m-2}\alpha^{q^i+q^m}-\alpha^{1+q^m}$ (since both of the latter two sums count the case $(0,m)$).

Overlapping the last two sums gives $\alpha^{1+q^{m-1}}+\alpha^2+\alpha^2+\alpha^{q+q^m}+\sum_{j=2}^{m-2}2a^{1+q^j}\equiv \alpha^{1+q^{m-1}}+\alpha^{q+q^m}-\alpha^{1+q^m}\equiv\alpha^2 \mod t$. Hence the overall sum becomes $\alpha^2+\sum_{1\le i<m}\alpha^{2q^i}+\sum_{1\le i<m-1}a^{q^i+q^{i+1}}$. Note that $\alpha^{2q^i}\equiv\alpha \mod t$ for each i, while similarly, $\alpha^{q^i+q^{i+1}}\equiv\alpha^{q+1} \mod t$ for each i (this is because the coset of t is determined by the trace and taking the trace of an $\mathbb{F}_2$-conjugate gives the same result). It follows that $\alpha^2+\sum_{1\le i<m}\alpha^{2q^i}+\sum_{1\le i<m-1}\alpha^{q^i+q^{i+1}}\equiv \alpha+(m-1)\alpha+(m-2)\alpha^{q+1}\equiv m(\alpha+\alpha^{q+1}) \mod t$, as desired. ☐

4 Main Results

Theorem 4.1

Suppose $K_1/\mathbb{Q}_p$, where $K_1\ne\mathbb{Q}_p$, is finite and totally ramified, and let K be a finite unramified extension of K_1. Let $n=[K:K_1]$. Set $f(x)=\frac{x^n-1}{(x-1)^{p^{v_p(n)}}}\in\mathbb{F}_p[x]$, $\deg(f)=n-p^{v_p(n)}=d$, and $\zeta_f(s)=\sum_{i=0}^{d}\frac{a_n}{p^{ns}}$ be the zeta function for the ring $S=\frac{\mathbb{F}_p[x]}{(f)}$ (equivalently, a_n is the number of degree n monic factors of f). Then the number of Galois extensions L/K_1 such that L/K is totally ramified with a single ramification jump at 3 is

$$\begin{cases} 0 & p=2 \\ \frac{2p^{n+1}-p^n-p^{d+1}}{p-1}\zeta_f(1) & p>2 \end{cases}$$

Proof. First note that $G = \mathrm{Gal}(L/K)$ has single wild ramification jump at 3, which means that the extension is totally wildly ramified. Thus by Proposition 1.1, we see that $G_2/G_3 \cong \mathrm{Gal}(L/K)$ is the direct sum of cyclic groups of order p. In particular, G is abelian, and so by class field theory we may attach a norm group $\mathrm{Nm}_{L/K}(L^\times)$ to it. As L/K is totally ramified, we may let $\pi \in \mathrm{Nm}_{L/K}(L^\times)$ be a uniformizer of $\mathcal{O}_K$. It then follows that $\mathrm{Nm}_{L/K}(L^\times) = \pi^{\mathbb{Z}}\mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$. Let $H = \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$. By Proposition 2.2, since G is abelian, the extension L/K_1 being Galois is equivalent to having the norm group corresponding to the abelian extension L/K under class field theory to be fixed by $\mathrm{Gal}(K/K_1)$. This means that $\pi^{\mathbb{Z}}H$ is invariant under the Galois action.

Since σ preserves valuations, $\pi^{\mathbb{Z}}H$ is invariant under $\mathrm{Gal}(K/K_1)$ iff $\pi^f H$ is for each integer f. As K/K_1 is unramified, let $\pi = \pi' u$ for some uniformizer π' of $\mathcal{O}_{K_1}$ and $u \in \mathcal{O}_K^\times$. The group $\mathcal{O}_K^\times/H$ has finite order, and so choosing $f = |\mathcal{O}_K^\times/H|$, Lagrange implies that $\pi^f H = \pi'^f H$. Thus to be Galois invariant in this case just means that H is Galois invariant. Now knowing that H is Galois invariant, we see that $\pi^{\mathbb{Z}}H$ is invariant precisely if $\sigma(u)/u \in H$ for each $\sigma \in G = \mathrm{Gal}(K/K_1)$. Thus for a given Galois invariant H, it suffices to find the number of classes $u \in \mathcal{O}_K^\times/H$ that are also Galois invariant. As H is Galois invariant, $\mathcal{O}_K^\times/H$ naturally obtains the structure of a G-module.

In order for the extension to be Galois, we just need two things to happen. First, we need that h is fixed under the Galois action. Indeed, given $x \in \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times) \cap (1+\mathfrak{m}^2)$ and $\sigma \in \mathrm{Gal}(K/K_1)$, we have that $\sigma(x) \in \mathrm{Nm}_{L/K}(L^\times)$ by Proposition 2.2 since L/K_1 is Galois. Furthermore, $1+\mathfrak{m}^2$ is Galois invariant since it $\mathfrak{m}$ is the unique maximal ideal of $\mathcal{O}_K$. Thus $\sigma(x) \in \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times) \cap (1+\mathfrak{m}^2)$. As σ has finite order, this implies that h is Galois invariant.

Then given such a subgroup h, we need to have that the fibers under the projection map onto $(1+\mathfrak{m})/(1+\mathfrak{m}^2)$ are fixed under the Galois action. This means that $\sigma(H_a) = H_{\sigma(a)}$ for all $\sigma \in \mathrm{Gal}(K/K_1)$ and a among our lifts.

We will now introduce a framework for understanding our lifts. Choose a $\mathrm{Gal}(k/k')$-invariant $\mathbb{F}_p$-basis for k (using the $\mathbb{F}_p$-module structure of $\mathbb{F}_{p^m}$), say $e_1, \cdots, e_m$ and lift these basis elements to roots of unity $\omega_1, \cdots, \omega_m$ in $\mathcal{O}_K^\times$. Each $a \in k$ can uniquely written as $\sum z_i e_i$, where $z_i \in \mathbb{F}_p$, and so there is a unique lift of a of the form $\sum z_i \omega_i$, where $0 \le z_i \le p-1$. Let $a' = \sum a_i \omega_i$ be this lift of a. Notice that $a' + b' = \sum a_i\omega_i + \sum b_i \omega_i = \sum (a_i + b_i)\omega_i$. On the other hand, the lift $(a+b)' = \sum (a+b)_i \omega_i$ is equal to $\sum(a_i+b_i)\omega_i$, so we have that $a_i + b_i = (a+b)_i$ in $\mathbb{F}_p$, which implies that $a_i + b_i \equiv (a+b)_i \mod p$. But since $K/\mathbb{Q}_p$ is totally ramified of degree > 1, we know that $a_i + b_i \equiv (a+b)_i \mod \pi^2$ and so $a' + b' \equiv (a+b)' \mod \pi^2$.

Now set $H_a = (1 + a'\pi + f(a)\pi^2)(1+\mathfrak{m}^3)$ for some coset $f(a)$ of h in k. The key idea is that

$$H_aH_b = ((1+a'\pi+f(a)\pi^2)(1+\mathfrak{m}^3))((1+b'\pi+f(b)\pi^2)(1+\mathfrak{m}^3)) =$$

$$(1+(a'+b')\pi+(f(a)+f(b)+ab)\pi^2)(1+\mathfrak{m}^3) = (1+(a+b)'\pi+(f(a)+f(b)+ab)\pi^2)(1+\mathfrak{m}^3)$$

It follows that $H_{a+b} = H_aH_b$ is equivalent to $f(a+b) \equiv f(a)+f(b)+ab \mod h$, which defines our group structure. By Galois invariance of our basis, we have that $\sigma(a') = (\sigma(a))'$, and so $\sigma(H_a) = (1+(\sigma(a))'\pi+\sigma(f(a))\pi^2)(1+\mathfrak{m}^3)$. Thus in order to have $\sigma(H_a) = H_{\sigma(a)}$ we just need to have that $\sigma(f(a)) = f(\sigma(a))$ for all $a \in k$. In other words, we want the map f to be Galois equivariant. By Lemma 3.2, the number of functions satisfying these two conditions is $(|k|/|h|)^s$.

Now since the projection map $H \to \mathcal{O}_K^\times/(1+\mathfrak{m}^2)$ is surjective, any element of $\mathcal{O}_K^\times/H$ has a coset representative of the form $1+\pi'^2x$. We want to compute the number of G-invariant points of $\mathcal{O}_K^\times/H$ given a choice of H. We may view x as an element of k since shifting x by something in $\mathfrak{m}$ does not change its coset. Such an element x is then precisely defined by its coset in k/h. The action of G on k/h restricts to the action of $G_1 = \mathrm{Gal}(k/k_1)$ on k/h, and so we just seek the number of G_1 invariant fixed points of k/h for a given choice of h.

Now note that its coset $x+h$ is invariant under G_1 iff it is invariant under a generator σ, meaning that we just need $x^q - x \in h$. Thus we seek the number of elements $x+h$ of k/h such that $x^q - x \equiv 0 \mod h$, where $q = |k_1|$. The map $x \to x^q - x$ is a linear map $k \to k$ with kernel consisting of the elements of $\mathbb{F}_q$ and image t, where t' is the trace 0 subspace (i.e. the kernel of Tr_{k/k_1}), since anything in the image is in the kernel of the trace map and t and the image have the same order. The subspace of h in the image of this map is then $h \cap t$. Each of these images is attained q times, so the total number of images in h is $q|h \cap t'|$. The total number of cosets of h is then $q|h\cap t'|/|h|$, and so this is the number of fixed points.

Now fix $|h|$. We want to determine $\sum |h \cap t'|$ over all subspaces h of k with $|h|$ of a given size. For this, we use the Galois module structure. Since $K'/\mathbb{Q}_p$ is totally ramified, $\mathbb{F}_{p^n}$ naturally has a structure as a $\mathbb{F}_p[x]$-module, decomposing as $\mathbb{F}_p[x]/(x^n-1)$. The virtue of this is that $\mathbb{F}_p[x]$-submodules, i.e. Galois invariant $\mathbb{F}_p$-subspaces, correspond precisely to ideals of $R = \mathbb{F}_p[x]/(x^n-1)$.

Under this correspondence, the subspace t' is just the ideal $(x-1)R$, and so $|h \cap t'| = |(x-1)\cap I|$. But now Is is necessarily a principal ideal corresponding to a monic factor f of x^n-1 in $\mathbb{F}_p[x]$. Let $I = (f(x))$. If $x-1|f(x)$, then $I \subset (x-1)$ and so $|(x-1)\cap I| = |I|$. Otherwise, $(x-1)\cap I = (f(x)(x-1))$ and so $|(x-1)\cap I| = |I|/p$. But then $|h| = |I|$ and so the sum we seek is $|h|\sum_{i=0}^{1} \frac{N_{i,t}}{p^i}$. Let $|h| = p^t$. Thus the total sum over h with $|h| = p^t$ becomes $p(\sum_{i=0}^{1} \frac{N_{i,t}}{p^i})$.

Now this is the total number of fixed points for a given choice of $|h|$. For each h with $|h| = p^t$, there are p^{n-t} ways to extend it to a G-invariant subgroup H of $\mathcal{O}_K^\times$ that is surjective on the projection map, and so by Lemma 3.2, to get the total number of extensions, we sum this over all possible t, meaning that we get

$$p^{n+1} \sum_{t=0}^{n-1} \sum_{i=0}^{1} \frac{N_{i,t}}{p^{i+t}}$$

as desired. Now we determine $N_{i,t}$ more explicitly. Firstly, if $i = 1$, then $N_{1,t}$ counts the number of degree t factors indivisible by $x-1$, which is $a_{d-t} = a_t$. If $i = 0$, then we now restrict to those divisible by $x-1$, which is $a_{t-1} + a_{t-2} + \cdots + a_{t-p^{v_p(n)}}$. Setting $b_t = 2a_t + \sum_{i=1}^{p^{v_p(n)}-1} a_{t-i}$, we get $p^n \sum_{t=0}^{n-1} \frac{b_t}{p^t}$, which can also be rewritten $p^n(2 + \sum_{i=1}^{n-d-1} \frac{1}{p^i})(\sum_{t=0}^{d} \frac{a_t}{p^t})$, as desired. □

In Theorem 4.1, we crucially assumed that $K/\mathbb{Q}_p$ was ramified in order for our coset machinery to work properly. However, the approach will work for any ramified $K/\mathbb{Q}_p$, with the only fallback in general being that the fixed point counts have a less pleasant expression when $K/\mathbb{Q}_p$ is not totally ramified. In fact, the count depends entirely on the content of the residue field extension k/k', and so it depends entirely on the residue field extension. In particular, for K/K_1 of fixed degree, only the residue degree of $K_1/\mathbb{Q}_p$ will impact the count. We will now treat the unramified case.

Theorem 4.2

Suppose $K_1/\mathbb{Q}_p$ is unramified of degree n and let K be a finite unramified extension of K_1. Then the number of finite Galois extensions L/K_1 such that L/K is totally ramified with a single ramification jump at 3 is

$$\begin{cases} 2^{n+1} & p = 2, \\ 0 & \text{else} \end{cases}$$

Proof. Set $[K : K_1] = r$.

By Proposition 1.1, $G_2/G_3 \cong \mathrm{Gal}(L/K)$ is the direct sum of cyclic groups of order p. By Artin reciprocity and noting that L/K is totally ramified, we have that $\mathrm{Gal}(L/K) \cong \mathcal{O}_K^\times/\mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$. This means that $(\mathcal{O}_K^\times)^p \subset \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times)$.

Now we suppose that $p > 2$. We claim that $1 + p^2\mathcal{O}_K \subset (\mathcal{O}_K^\times)^p$.

Indeed, note that $(1+py)^p \equiv 1 + p^2y \mod p^3$ if $p > 2$, which implies that for the polynomial $f(x) = x^p - (1+p^2y)$, $|f(1+p^2y)| \le p^{-3}$. On the other hand, $f'(1+p^2y) = p(1+p^2y)^{p-1}$, and so $|f'(1+p^2y)| = p^{-1}$, which shows that $|f(1+p^2y)| \le |f'(1+p^2y)|^2$. Thus by Hensel's Lemma, we can find a solution $z \in \mathcal{O}_K$ to $x^2 - (1+p^2y) = 0$, which shows that $1 + p^2\mathcal{O}_K \subset (\mathcal{O}_K^\times)^p$. Thus

$1+p^2\mathcal{O}_K \subset \mathrm{Nm}_{L/K}(\mathcal{O}_L^\times) = H$. However, to have a single ramification jump at 3, we need the map $H \to \mathcal{O}_K^\times/(1+p^2\mathcal{O}_K)$ to be surjective, which implies that $H = \mathcal{O}_K^\times$, contradicting Lemma 2.1.

Next we handle the case of $p = 2$. We will determine precisely $(\mathcal{O}_K^\times)^2$. Note that $(1+2z)^2 = 1+4(z^2+z)$. If we can find x such that $z^2+z = y$, then we have that $1+2z$ is a solution to $x^2-(1+4y) = 0$, and so as before, Hensel's Lemma implies that we can find w with $w^2 = 1+4y$. Thus the squares in $1+2\mathcal{O}_K$ are precisely those of the form $1+4(z^2+z) \mod 8$. In particular, we deduce that if h is the image of $H \cap (1+4\mathcal{O}_K) \to (1+4\mathcal{O}_K)/(1+8\mathcal{O}_K) \cong k^+$, then h contains the subspace consisting of all values $z^2+z, z \in k$. The map $z \to z^2+z$ is a homomorphism on k with kernel $0, 1$, and thus the image has size $\frac{|k|}{2}$, meaning that this subspace is an index 2 subgroup of k^+. In particular, we must have that h is precisely this subspace or else h would be the whole of k^+ which would imply as before that $H = \mathcal{O}_K^\times$, which is again not proper, contradicting Lemma 2.1.

By Lemma 3.3, we can choose an $\mathbb{F}_2$-basis for t of the form $\{g^i\alpha_j, 0 \le i \le r-1, 1 \le j \le n-1\} \cup \{g^i(g-1)\alpha_n, 0 \le i \le r-2\}$, where g is a generator of $\mathrm{Gal}(k/k_1)$. Denote these elements as $e_1, \cdots, e_{rn-1}$. Lift these basis elements to roots of unity $\omega_1, \cdots, \omega_{rn-1}$ in $\mathcal{O}_K^\times$. Each $a \in k$ can uniquely written as $\sum f_i e_i$, where $z_i \in \mathbb{F}_2$, and so there is a unique lift of a of the form $\sum z_i\omega_i$, where $0 \le z_i \le 1$. Let $a' = \sum a_i\omega_i$ be this lift of a.

Now set $H_a = (1+2a'+4f(a))(1+\mathfrak{m}^3)$ for some coset $f(a)$ of t in k. Getting a subgroup structure is equivalent to having $H_aH_b = H_{a+b}$ for all $a, b \in k$.

First suppose that $a, b \in t$. The lift $(a+b)'$ for $a+b$ will differ from $a'+b'$ by $2(\sum e_i')$, where the sum ranges over some subset of $e_1', \cdots, e_{rn-1}'$. Thus $1+2(a'+b')+4ab+4f(a)+4f(b) = 1+2(a+b)'+4(\sum e_i')+4ab+4f(a)+4f(b)$. The key point is that now $\sum e_i'$ will be an element of h and thus will not change the coset of h dictated by the values of f, and thus $1+2(a+b)'+4f(a+b) = 1+2(a'+b')+4ab+4f(a)+4f(b) = 1+2(a+b)'+4(\sum e_i')+4ab+4f(a)+4f(b) = 1+2(a+b)'+4ab+4f(a)+4f(b)$, and so we deduce that $f(a+b) \equiv f(a)+f(b)+ab \mod t$ for all $a, b \in t$.

Case 1: r is odd.

In this case, take some element β of k_1 such that $\mathrm{Tr}_{k_1/\mathbb{F}_2}(\beta) = 1$ and let $e_{rn} = \beta$. Then note that $\mathrm{Tr}_{k/\mathbb{F}_2}(\beta) = [K : K_1]\mathrm{Tr}_{k_1/\mathbb{F}_2}(\beta) = 1$, and so $\beta \notin t$, showing that β completes the basis. Then if both $a, b \notin t$, the element $(a+b)'-(a'+b')$ will now be of the form $2(\sum e_i')$, where it includes e_{rn}', and so now $\sum e_i'$ will indeed change the coset. Hence we deduce that $f(a+b) \equiv f(a)+f(b)+ab+e_{rn} \mod h$. Let l be the subspace of k spanned by $e_1, \cdots, e_{r(n-1)}$. Applying Lemma 3.1 upon noting that l has a Galois invariant basis and stays in t upon squaring (since t maps to itself upon squaring), meaning that $l \sim t$, we conclude that there are 2^{n-1} Galois equivariant functions satisfying $f(a+b) \equiv f(a)+f(b)+ab \mod t$ on l.

We will now show that each of these equivariant functions has exactly two extensions to k^+. First note that $f((g-1)\alpha_n) = f(\alpha_n^q + \alpha_n)$. In order for the functional equation to be satisfied and to have Galois equivariance, we must have that $f(\alpha_n^q + \alpha_n) \equiv 2f(\alpha_n) + \alpha_n^{q+1} \equiv \alpha_n^{q+1} \mod h$ if $\alpha_n \in t$ and $f(\alpha_n^q + \alpha_n) \equiv 2f(\alpha_n) + \alpha_n^{q+1} + \alpha_n \equiv \alpha_n^{q+1} + \alpha_n \mod h$ if $\alpha_n \notin t$. Note that the former is just $\alpha_n^{q+1} + \alpha_n$ since $\alpha_n \in t$, so we have that $f(\alpha_n^q + \alpha_n) = \alpha_n^{q+1} + \alpha_n$ in all cases. Then since the Galois group preserves t, Galois equivariance forces $f(\alpha_n^{q^i} + \alpha_n^{q^{i-1}}) \equiv \alpha_n^{q+1} + \alpha_n \mod h$ for each i. Finally, we let $f(\beta)$ be either of the two possibilities. This defines f on all of k^+ via the functional equation, and by the proof of Lemma 3.1, will give a well-defined function.

Hence we just need to check that each such function is Galois equivariant. Write $a = a_{rn}\beta + \sum_{i=1}^{n(r-1)} a_i e_i + c$ and let $b = a_{rn}\beta + \sum_{i=1}^{n(r-1)} a_i e_i$. Note that $\sigma(f(a)) = \sigma(f(b)) + \sigma(f(c)) + \sigma(bc)$. Since the basis elements in the expansion of b form a Galois invariant set, the proof of Lemma 3.2 implies that $\sigma(f(b)) = f(\sigma(b))$. Since we know that f satisfies the functional equation, we must have that $f(\sigma(a)) = f(\sigma(b)) + f(\sigma(c)) + \sigma(b)\sigma(c)$. Hence it suffices to show that $\sigma(f(c)) = f(\sigma(c))$.

By definition and Galois equivariance on the basis, we have $c = \sum_{i=r(n-1)}^{rn-1} a_i e_i = \sum_{i=0}^{r-2} a_i' g^i (g-1)\alpha_n$ and so

$$g(f(c)) = \sum_{i=0}^{r-2} a_i' g(f(g^i(g-1)\alpha_n)) + \sum_{0\le i<j\le r} g(a_i' a_j'(g^i(g-1)\alpha_n)(g^j(g-1)\alpha_n)) =$$

$$\sum_{i=0}^{r-2} a_i'(f((g-1)\alpha_n)) + \sum_{0\le i<j\le r-2} a_i' a_j'(g^{i+1}(g-1)\alpha_n)(g^{j+1}(g-1)\alpha_n))$$

Next note that $gc = a_{r-2}'(g-1)\alpha_n + \sum_{i=0}^{r-3}(a_i' + a_{r-2}')g^{i+1}(g-1)\alpha_n$ and so

$$f(gc) = f(\sum_{i=0}^{r-3} a_i' g^{i+1}(g-1)\alpha_n) + a_{r-2}' f(\sum_{i=0}^{r-2} g^i(g-1)\alpha_n) +$$

$$a_{r-2}'(\sum_{i=0}^{r-3} a_i' g^{i+1}(g-1)\alpha_n)(\sum_{i=0}^{r-2} g^i(g-1)\alpha_n)$$

Now we know that

$$f(\sum_{i=0}^{r-3} a_i' g^{i+1}(g-1)\alpha_n) = (\sum_{i=0}^{r-3} a_i' f(g^{i+1}(g-1)\alpha_n)) +$$

$$\sum_{0\le i<j\le r-3} a_i' a_j'(g^{i+1}(g-1)\alpha_n)(g^{j+1}(g-1)\alpha_n))$$

Combining everything, it remains to show that $f(\sum_{i=0}^{r-2} g^i(g-1)\alpha_n) \equiv f((g-1)\alpha_n) \mod h$. Expanding out the left hand side gives $(r-1)f((g-1)\alpha_n) + \sum_{0\le i<j\le r-2} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n)$, and so since $f((g-1)\alpha_n) \equiv \alpha^{q+1}+\alpha \mod h$, it remains to show that $\sum_{0\le i<j\le r-2} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n) \equiv r(\alpha^{q+1}+\alpha) \mod h$. By Lemma 3.4, we have that $\sum_{0\le i<j\le r-1} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n) = r(\alpha_n^{q+1}+\alpha_n)$. But then rewriting the sum gives

$$\sum_{0\le i<j\le r-2} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n) + (\sum_{i=0}^{r-2} g^i(g-1)\alpha_n)(g^{r-1}(g-1)\alpha_n) =$$

$$\sum_{0\le i<j\le r-2} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n) + ((1+g^{r-1})\alpha_n)(g^r-g^{r-1})\alpha_n$$

However, $((1+g^{r-1})\alpha_n)(g^r-g^{r-1})\alpha_n \equiv (\alpha+\alpha^{q^{r-1}})(\alpha^{q^r}+\alpha^{q^{r-1}}) \equiv (\alpha+\alpha^{q^{r-1}})^2 = \alpha+\alpha^{q^{r-1}} \equiv 0 \mod h$, and so we conclude that $\sum_{0\le i<j\le r-2} g^i(g-1)\alpha_n(g^j(g-1)\alpha_n) \equiv r(\alpha_n^{q+1}+\alpha_n) \mod h$, completing the proof.

Case 2: r is even.

Consider our basis $\{g^i\alpha_j, 0\le i\le r-1, 1\le j\le n-1\} \cup \{g^i(g-1)\alpha_n, 0\le i\le r-2\}$ for t coming from Lemma 3.3. This corresponds to the $\mathbb{F}_2[x]$-module decomposition $t \cong \bigoplus_{i=1}^{n-1} \mathbb{F}_2[x]/(x^r-1) \oplus \mathbb{F}_2[x]/(x^{r-1}+\cdots+1)$. We claim that $\alpha_n \notin t$. Suppose that $\alpha_n \in t$. Then we can write $\alpha_n = (g-1)b$ for some b, and so then $(g-1)\alpha_n = (g-1)^2 b$. Since r is even, we know that $x-1 | x^{r-1}+\cdots+1$, and so it follows that $(g-1)^2 b$ is annihilated by the element $\frac{g^{r-1}+\cdots+1}{g-1}$, contradiction since $(g-1)\alpha_n$ corresponds to 1 in the last component under the $\mathbb{F}_2[x]$-module isomorphism.

Now using the exact same reasoning as in Case 1, we can define our function f on the subspace l corresponding to the Galois equivariant part of the basis for t and note that that $f((g-1)\alpha_n) \equiv f(\alpha_n^q+\alpha_n) \equiv \alpha_n^{q+1}+\alpha_n \mod h$, this time using that $\alpha_n \notin t$. Furthermore, since $\alpha_n \notin t$, we can use it to complete our basis for k^+. There are then 2 choices for $f(\alpha_n)$, each defining f on all of k^+ via the functional equation, and by the proof of Lemma 3.1 implies that we get a well-defined function in each case.

Hence we just need to check that each function is Galois equivariant. The proof of equivariance in the case when the α_n coefficient is 0 is identical to the proof in Case 1. Hence we just need to show equivariance in the case where the α_n coefficient is 1. Write $a = a'+\alpha$ so that $a' \in t$. Noting that we already have equivariance on t, we have that $\sigma(f(a)) \equiv \sigma(f(a'))+\sigma(f(\alpha))+\sigma(a'\alpha) \equiv f(\sigma(a')+\sigma(a')\sigma(\alpha)+\sigma(f(\alpha)) \mod h$. Hence we just need to show that $\sigma(f(\alpha)) \equiv f(\sigma(\alpha)) \mod h$. Note that

$$f(g(\alpha)) \equiv f(\alpha+(g-1)\alpha)) \equiv f(\alpha)+f((g-1)\alpha)+\alpha(g-1)\alpha \equiv$$

$$f(\alpha) + \alpha^{q+1} + \alpha + \alpha(\alpha^q + \alpha) \equiv f(\alpha) + \alpha^2 + \alpha \equiv f(\alpha) \mod h$$

completing the proof.

Hence in each case, we have 2^n Galois equivariant functions for $h = t$, which shows that there 2^n possibilities for h in each case. Now since the quotient k/t consists of two cosets and each is fixed (since t itself is), we conclude that there are 2 fixed points. Hence following the proof of Theorem 4.1, we conclude that there are precisely 2^{n+1} extensions, as desired. □

With the main theorems proven, we now determine the cohomology of our subgroups H of $\mathcal{O}_K^\times$ and the quotients $\mathcal{O}_K^\times/H$ since H and thus $\mathcal{O}_K^\times/H$ are equipped with the structures of G-modules, building off our calculation of fixed points.

Theorem 5.1

We have that $\hat{H}^0(G, H) \cong \hat{H}^1(G, H) \cong (\mathbb{Z}/p\mathbb{Z})^b$, where $p^b = |h \cap k_1||h \cap t'|/|h|$.

Proof. We begin with the exact sequence $1 \to H \to \mathcal{O}_K^\times \to \mathcal{O}_K^\times/H \to 1$. Taking cohomology and using the 2-periodicity of cyclic cohomology gives the exact sequences

$$\hat{H}^0(G, \mathcal{O}_K^\times) \to \hat{H}^0(G, \mathcal{O}_K^\times/H) \to \hat{H}^1(G, H) \to \hat{H}^1(G, \mathcal{O}_K^\times)$$

and

$$\hat{H}^1(G, \mathcal{O}_K^\times) \to \hat{H}^1(G, \mathcal{O}_K^\times/H) \to \hat{H}^0(G, H) \to \hat{H}^0(G, \mathcal{O}_K^\times)$$

Now since K/K_1 is unramified, $\hat{H}^1(G, \mathcal{O}_K^\times)$ vanishes by Hilbert 90 and $\hat{H}^0(G, \mathcal{O}_K^\times)$ vanishes since $\mathrm{Nm}_{K/K_1}(\mathcal{O}_K^\times) = \mathcal{O}_{K_1}^\times$. Thus the exact sequences become

$$1 \to \hat{H}^0(G, \mathcal{O}_K^\times/H) \to \hat{H}^1(G, H) \to 1$$

and

$$1 \to \hat{H}^1(G, \mathcal{O}_K^\times/H) \to \hat{H}^0(G, H) \to 1$$

inducing isomorphisms $\hat{H}^0(G, \mathcal{O}_K^\times/H) \cong \hat{H}^1(G, H)$ and $\hat{H}^1(G, \mathcal{O}_K^\times/H) \cong \hat{H}^0(G, H)$. As $\mathcal{O}_K^\times/H$ is a finite G-module and G is cyclic, the theory of the Herbrand quotient implies that $h(\mathcal{O}_K^\times/H) = 1$, which shows that $|\hat{H}^1(G, \mathcal{O}_K^\times/H)| = |\hat{H}^0(G, \mathcal{O}_K^\times/H)|$. We now compute $|\hat{H}^0(G, \mathcal{O}_K^\times/H)|$ explicitly. Note that

$$|\hat{H}^0(G, \mathcal{O}_K^\times/H)| = |(\mathcal{O}_K^\times/H)^G|/|\mathrm{Nm}_{K/K_1}(\mathcal{O}_K^\times/H)|$$

We have shown that $|(\mathcal{O}_K^\times/H)^G| = q|h \cap t'|/|h|$, and so it remains to compute $\mathrm{Nm}_{K/K_1}(\mathcal{O}_K^\times/H)$. Again, we may view this as $\mathrm{Tr}_{k/k_1}(k/h)$. The number of elements $x \in k$ with $\mathrm{Tr}_{k/k_1}(x) = 0$ is $|k|/q$ by surjectivity of Tr_{k/k_1}. Thus there are $|k||h \cap k_1|/q$ with image in h, and so this means that $q/|h \cap k_1|$ cosets are reached, showing that the image has order $q/|h \cap k_1|$. Hence

$$|\hat{H}^0(G, \mathcal{O}_K^\times/H)| = |h \cap k_1||h \cap t'|/|h|$$

Now since the $\mathcal{O}_K^\times/H$ is p-torsion, so are $\hat{H}^i(G, \mathcal{O}_K^\times/H)$, and this immediately implies the claim. □

References

[1] Hasse, Helmut. Number Theory, Berlin, Boston: De Gruyter, 1979.

[2] Serre, Jean-Pierre, Local fields, Springer-Verlag, 1979.

[3] Serre, J.-P.: Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local. Comptes Rendus 286, 1031–1036 (1978)