# Galois Cohomology Summary

Thomas Browning, Thomas Carr

April 2019

## 1 Kummer Theory

An abelian extension $L/K$ with $G = \mathrm{Gal}(L/K)$ is said to be of **exponent** $n$ if $\sigma^n = 1$ for all $\sigma \in G$. A **Kummer extension** is an abelian extension of exponent $n$ where $K$ contains the $n$th roots of unity.

**Example:** Let $L$ be the splitting field of $x^3 - a$ over $\mathbb{Q}$ where $a$ is not a cube, and let $K = \mathbb{Q}(\zeta_3)$. Then $L/K$ is a Kummer extension of exponent 3.

Let $L/K$ be a Kummer extension of exponent $n$, and consider the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow L^\times \xrightarrow{\cdot n} (L^\times)^n \longrightarrow 1$$

Taking Galois cohomology we have the long exact sequence

$$1 \longrightarrow \mu_n \longrightarrow K^\times \xrightarrow{\cdot n} K^\times \cap (L^\times)^n \longrightarrow H^1(G, \mu_n) \longrightarrow H^1(G, K^\times) \longrightarrow \cdots$$

We have $H^1(G, K^\times) = 1$ by Hilbert's Theorem 90. Since $G$ acts trivially on $\mu_n$, we also have that $H^1(G, \mu_n) = \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n)$. Because $\mathrm{im}(K^\times \longrightarrow K^\times \cap (L^\times)^n) = (K^\times)^n$, we have an isomorphism

$$(K^\times \cap (L^\times)^n)/(K^\times)^n \simeq \mathrm{Hom}_{\mathbb{Z}}(G, \mu_n).$$

Since $\sigma^n = 1$ for all $\sigma \in G$, the abelian group $\mathrm{Hom}_{\mathbb{Z}}(G, \mu_n)$ is just the Pontryagin dual $\chi(G)$ of $G$. Pontryagin duality gives us an inclusion reversing isomorphism of subgroup lattices of $\chi(G)$ and $G$. By Galois Theory, subgroups of $G$ correspond to finite Kummer extensions of $K$. Thus we have a correspondence between subgroups of $K^\times \cap (L^\times)^n$ containing $(K^\times)^n$ and Kummer extensions of $K$ contained in $L$.

It can be shown that there exists a maximal Kummer extension $N$ containing all other Kummer extensions of exponent $n$. Passing to this maximal extension, we have

$$(K^\times \cap (N^\times)^n)/(K^\times)^n = K^\times/(K^\times)^n \simeq \chi(G).$$

Care must be taken because the Galois group $G$ is now an infinite (profinite) group. But it is nevertheless possible to show the following correspondence:

**Theorem 1.** *There is an inclusion-preserving bijection between subgroups of $K^\times$ containing $(K^\times)^n$ and Kummer extensions of $K$ of exponent $n$. More explicitly, a Kummer extension $L/K$ corresponds to the subgroup $K^\times \cap (L^\times)^n \subset K^\times$, and a subgroup $\Delta \subset K^\times$ corresponds to the extension $K(\sqrt[n]{\Delta})$.*

This essentially says that Kummer extensions are obtained by adjoining $n$th roots of elements in $K$. This is known as **Kummer Theory**.

Note that we have been operating under the (strong) assumption that our base field $K$ contains all the $n$th roots of unity. If instead $K$ does not contain all the roots, the situation becomes significantly more complicated. Describing abelian extensions in general is the task of **class field theory**.

# 2 Global Class Field Theory

## 2.1 The Idele Class Group

For each prime $p$, we have an embedding $\mathbb{Q}^\times \hookrightarrow \mathbb{Q}_p^\times$. We also have an embedding $\mathbb{Q}^\times \hookrightarrow \mathbb{R}^\times$. This gives an embedding

$$\mathbb{Q}^\times \hookrightarrow \mathbb{R}^\times \times \prod_p \mathbb{Q}_p^\times .$$

For each $x \in \mathbb{Q}^\times$, there are only finitely many primes dividing the numerator and denominator of $x$. In particular, $v_p(x) = 0$ for all but finitely many primes $p$ so $x_p \in \mathbb{Z}_p^\times$ for all but finitely many primes $p$. Thus, we obtain an embedding to the restricted product

$$\mathbb{Q}^\times \hookrightarrow \mathbb{R}^\times \times \widehat{\prod_p}^{\mathbb{Z}_p^\times} \mathbb{Q}_p^\times .$$

More generally, for every number field $K$, we have an embedding

$$K^\times \hookrightarrow \widehat{\prod_v}^{\mathcal{O}_v^\times} K_v^\times$$

where now the restricted product runs over all nontrivial equivalence classes of valuations. There is one nontrivial equivalence class of valuations for each nonzero prime ideal of the ring of algebraic integers $\mathcal{O}_K$. There is also one nontrivial equivalence class of valuations for each of the finitely many embeddings of $K$ into $\mathbb{R}$ or $\mathbb{C}$. One formuation of Ostrowski's theorem states that this accounts for all of the nontrivial equivalence classes of valuations. The restricted product on the right is denoted by $I_K$ and is called the idele group of $K$. The quotient group $C_K = I_K/K^\times$ is called the idele class group of $K$.

## 2.2 Cohomology of the Idele Class Group

If $L/K$ is a finite extension of numbers fields, then we have inclusions

$$K^\times \subseteq L^\times, \quad I_K \subseteq I_L, \quad C_K \subseteq C_L.$$

If $L/K$ is a finite Galois extension of number fields with Galois group $G$ then we have the equalities

$$(L^\times)^G = K^\times, \quad I_L^G = I_K, \quad C_L^G = C_K.$$

In what follows, we will use the notation $H^n(L/K) = H^n(\mathrm{Gal}(L/K), C_L)$. Our next result states that the first cohomology group always vanishes. We will demonstrate how abstract cohomological results can be used to reduce this hard problem to a situation that is more amenable to number-theoretic computation.

**Theorem 2.** *Let $L/K$ be a finite Galois extension of number fields. Then $H^1(L/K) = 0$.*

*Proof Sketch.* Let $\mathrm{Gal}(L/F)$ be a Sylow $p$-subgroup of $\mathrm{Gal}(N/K)$. Recall that the composition

$$H^1(L/K) \xrightarrow{\text{res}} H^1(L/F) \xrightarrow{\text{cor}} H^1(L/K)$$

is given by multiplication by $[F : K]$ which is injective on the $p$-primary part of $H^1(L/K)$. We reduce to the case where $\mathrm{Gal}(L/K)$ is a $p$-group. Now let $\mathrm{Gal}(L/F)$ be a normal subgroup of $\mathrm{Gal}(L/K)$. We have the inflation-restriction exact sequence

$$0 \longrightarrow H^1(F/K) \xrightarrow{\text{inf}} H^1(L/K) \xrightarrow{\text{res}} H^1(L/F).$$

We reduce to the case where $\mathrm{Gal}(L/K)$ is cyclic of order $p$. We have the inflation restriction exact sequences

$$0 \longrightarrow H^1(K(\zeta_p)/K) \xrightarrow{\inf} H^1(L(\zeta_p)/K) \xrightarrow{\mathrm{res}} H^1(L(\zeta_p)/K(\zeta_p))$$

and

$$0 \longrightarrow H^1(L/K) \xrightarrow{\inf} H^1(L(\zeta_p)/K) \xrightarrow{\mathrm{res}} H^1(L(\zeta_p)/L).$$

In particular, it suffices to show that $H^1(K(\zeta_p)/K) = 0$ and $H^1(L(\zeta_p)/K(\zeta_p)) = 0$. We can compute

$$[K(\zeta_p) : K] = [K \cdot \mathbb{Q}(\zeta_p) : K] = [\mathbb{Q}(\zeta_p) : K \cap \mathbb{Q}(\zeta_p)] \leq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

so $H^1(K(\zeta_p)/K) = 0$ by induction on the degree. Also,

$$[L(\zeta_p) : K(\zeta_p)] = [L \cdot K(\zeta_p) : K(\zeta_p)] = [L : L \cap K(\zeta_p)] \leq [L : K] = p.$$

If $[L(\zeta_p) : K(\zeta_p)] \leq p - 1$ then $H^1(L(\zeta_p)/K(\zeta_p)) = 0$ by induction. We reduce to the case where $\mathrm{Gal}(L/K)$ is cyclic of order $p$ and where $K$ contains the $p$th roots of unity. At this point, it becomes a technical computation requiring more number theory. □

A similar but more complicated combination of abstract cohomological results and number-theoretic computation can be used to determine the second cohomology group.

**Theorem 3.** *Let $L/K$ be a finite Galois extension of number fields. Then $H^2(L/K)$ is cyclic of order $[L : K]$ (and these isomorphisms are nicely compatible with inflation and restriction).*

## 2.3 Tate Cohomology

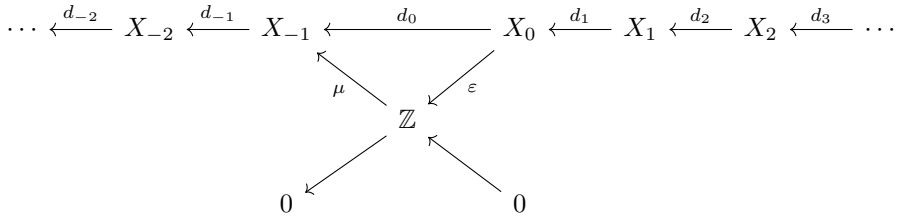
Let $G$ be a finite group and let $A$ be a $G$-module. Recall that

$$A^G = \{a \in A \colon ga = a \text{ for all } g \in G\},$$
$$A_G = A/\langle a - ga \colon a \in A,\ g \in G\rangle.$$

The element $\sum_{g \in G} g \in \mathbb{Z}G$ induces a map $N_G \colon A_G \to A^G$. The Tate cohomology groups are defined by

$$\widehat{H}^n(G, A) = \begin{cases} H^n(G, A) & n \geq 1 \\ \operatorname{coker} N_G & n = 0 \\ \ker N_G & n = -1 \\ H_{-n-1}(G, A) & n \leq -2 \end{cases}$$

This seems like a rather ad-hoc way to fuse together homology and cohomology. A more motivated construction of the Tate cohomology groups can be given by starting with a "complete free resolution" which is a commutative diagram of the form




such that each $X_i$ is a free $G$-module and such every term is exact, including the two bends. Then the Tate cohomology groups are given by

$$\widehat{H}^n(G, A) = H^n(\mathrm{Hom}_{\mathbb{Z}G}(X_\bullet, A)).$$

Here are some useful properties of the Tate cohomology groups:

1. If $0 \to A \to B \to C \to 0$ is a short exact sequence of $G$-modules then we obtain a two-sided long exact sequence of Tate cohomology groups

$$\cdots \longrightarrow \widehat{H}^{n-1}(G, C) \longrightarrow \widehat{H}^n(G, A) \longrightarrow \widehat{H}^n(G, B) \longrightarrow \widehat{H}^n(G, C) \longrightarrow \widehat{H}^{n+1}(G, A) \longrightarrow \cdots$$

2. If $G$ is cyclic and if $A$ is a $G$-module then $\widehat{H}^{n+2}(G, A) \cong \widehat{H}^n(G, A)$ for all integers $n$.

3. If $A$ and $B$ are $G$-modules then for all integers $m$ and $n$, we have a cup product

$$\widehat{H}^m(G, A) \otimes \widehat{H}^n(G, B) \to \widehat{H}^{m+n}(G, A \otimes B).$$

4. For $m \in \mathbb{Z}$, there is a $G$-module $S$ such that there are isomorphisms $\widehat{H}^n(G, A) \cong \widehat{H}^{n-m}(G, A \otimes S)$.

The last result is called dimension shifting and is very powerful. For example, if we can prove the second result for one value of $n$ then we immediately get the second result for all values of $n$. Also, dimension shifting can be used to construct the cup product in arbitrary dimensions from the cup product in dimensions $m = n = 0$.

**Theorem 4** (Tate)**.** *Let $G$ be a finite group and let $A$ be a $G$-module such that*

1. *For every subgroup $H$ of $G$, $\widehat{H}^1(H, A) = 0$.*
2. *For every subgroup $H$ of $G$, $\widehat{H}^2(H, A)$ is cyclic of order $|H|$.*

*If $a$ generates $\widehat{H}^2(G, A)$ then for every integer $n$, the map*

$$a \cup -\colon \widehat{H}^n(G, \mathbb{Z}) \to \widehat{H}^{n+2}(G, A)$$

*is an isomorphism.*

The proof uses dimension shifting. Setting $n = -2$ gives the isomorphism

$$A^G/NA = \operatorname{coker} N_G = \widehat{H}^0(G, A) \cong \widehat{H}^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}.$$

In the case of the idele class group, we obtain an isomorphism

$$C_K/N_{L/K}(C_L) \cong \mathrm{Gal}(L/K)^{\mathrm{ab}}.$$

Notice what happened here: We proved hard results about the group cohomology $H^1(G, C_L)$ and $H^2(G, C_L)$ and used dimension shifting in Tate cohomology to get a deep interpretation of the group homology $H_1(G, \mathbb{Z})$.

**Corollary 5.** *Let $K$ be a number field. There is an inclusion reversing isomorphism between abelian extensions of $K$ and norm subgroups of $C_K$.*

It turns out that the norm subgroups of $C_K$ are precisely the closed subgroups of $C_K$ of finite index.