Class Field Theory

Kevin Buzzard Richard Hill others

June 24, 2025

Chapter 1

Introduction

Chapter 2

Group Cohomology

2.1 Introduction

The aim of this chapter is to define the basic concepts of group cohomology and to prove the following theorem of Tate:

Theorem 1. *Let M be a representation of a finite group G over the ring $\mathbb{Z}$, and suppose that for all subgroups S of G the following two conditions hold:*

- $H^1(S, M) \cong 0$,
- $H^2(S, M) \cong \mathbb{Z}/|G| \cdot \mathbb{Z}$.

Then there is an isomorphism

$$G^{\mathrm{ab}} \cong M^G/N_G M.$$

If σ is a 2-cocycle representing a generator of $H^2(G, M)$ then the isomorphism is given by

$$\mathrm{reciprocity}(g) = \sum_{x \in G} \sigma(x, g)$$

In later chapters we shall see that the hypotheses of the theorem are satisfied in the following cases.

- If l/k is a finite Galois extension of local fields and $G = \mathrm{Gal}(l/k)$ then we may regard the group $l^\times$ as a respresentation of G. This representation satisfies the hypotheses above so we we have an isomorphism:

$$\mathrm{reciprocity} : \mathrm{Gal}(l/k)^{\mathrm{ab}} \cong k^\times/N(l^\times).$$

- If l/k is a finite Galois extension of number fields and $G = \mathrm{Gal}(l/k)$ then we may regard the idele class group $\mathrm{Cl}_l = \mathbb{A}^\times/l^\times$ as a respresentation of G. This representation satisfies the hypotheses above so we we have an isomorphism:

$$\mathrm{reciprocity} : \mathrm{Gal}(l/k)^{\mathrm{ab}} \cong \mathrm{Cl}_k/N(Cl_l).$$

2.2 Group cohomology and homology

Let G be a group and R a commutative ring. By a *representation of G over R*, we shall mean an R-module M with an action of G by R-linear maps. We shall use the notation $g \bullet m$ for the action of an element $g \in G$ on an element $m \in M$. We'll call M a *trivial* representation if for all $g \in G$ and all $m \in M$ we have $g \bullet m = m$. We'll write $\mathbf{Mod}(R)$ for the category of R-modules and $\mathbf{Rep}(R, G)$ for the category of such representations. In Mathlib these are called `ModuleCat R` and `Rep R G`.

If S is a subgroup of G and M is a representation of G then $M \downarrow S$ will mean the same R-module M, but regarded only as a representation of S. We shall write M^S for the R-submodule of S-invariant vectors in M. If the subgroup S is normal then M^S is a representation of the quotient group G/S.

riction functors

Definition 2. The map $M \mapsto M \downarrow S$ defines a functor $\mathbf{res} : \mathbf{Rep}(R, G) \to \mathbf{Rep}(R, S)$. If S is a normal subgroup of G then then map $M \mapsto M^S$ defines a functor $\mathbf{invar} : \mathbf{Rep}(R, G) \to \mathbf{Rep}(R, G/S)$. These functors are called *restriction* and *inflation* respectively.

Given a representation M of G, there is a cochain complex of R-modules

$$C^0(G, M) \xrightarrow{d^0} C^1(G, M) \xrightarrow{d^1} C^2(G, M) \xrightarrow{d^2} \cdots$$

where each term $C^n(G, M)$ is the space of functions $G^n \to M$ with some appropriately defined linear maps d^i linking them. The zeroth module $C^0(G, M)$ should be interpreted as just M. The first few of these linear maps d^i are

$$\begin{aligned}
(d^0 m)(x) &= x \bullet m - m && m \in M, \\
(d^1 f)(x, y) &= x \bullet f(y) - f(xy) + f(x) && f : G \to M, \\
(d^2 f)(x, y, z) &= x \bullet f(y, z) - f(xy, z) + f(x, yz) - f(x, y), && f : G^2 \to M.
\end{aligned}$$

The cochain complex $C^\bullet(G, M)$ is functorial in M and is defined in Mathlib as `groupCohomology.cochainsFunctor`. The cohomology groups of $C^\bullet(G, M)$ are called the cohomology groups of the G-module M, and are written $H^n(G, M)$. These are defined in Mathlib as `groupCohomology M n`, or `(groupCohomology.functor n).obj M`.

eg:H0

Example 3. *For example $H^0(G, M)$ is just the kernel of the map $d^0 : M \to (G \to M)$. Since $(d^0 m)(g) = g \bullet m - m$, an element m is in this kernel if m is in M^G, so we have $H^0(G, M) \cong M^G$.*

trivial iso Hom

Example 4. *Suppose M is a trivial representation of G. Then the map d^0 is zero, so $H^1(G, M)$ is the kernel of the map $(d^1 f)(x, y) = f(x) + f(y) - f(xy)$. A function $f : G \to M$ is in this kernel if it is a group homomorphism, so we have $H^1(G, M) \cong \mathrm{Hom}(G, M)$.*

eg:H2 unit

Example 5. *If G is the trivial group then for all $n > 0$, $H^n(G, M) \cong 0$. In this case each of the modules $C^n(G, M)$ may be identified with M, and the coboundary maps reduce to alternating sums of the form $d^n(m) = \sum_{i=0}^{n+1} (-1)^i m$. Hence d^n is the identity map for odd n, and is the zero map for even m.*

Remark. The functions $d^i : (G^i \to M) \to (G^{i+1} \to M)$ do not depend on the ring R. Consequently, the additive groups $H^n(G, M)$ do not depend on the R. More precisely there are forgetful functors $F_1 : \mathbf{Rep}(R, G) \to \mathbf{Rep}(\mathbb{Z}, G)$ and $F_2 : \mathbf{Mod}(R) \to \mathbf{Mod}(\mathbb{Z})$, and there are isomorphisms of functors

$$H^n \circ F_1 \cong F_2 \circ H^n.$$

That said, it is very little extra work to prove the cohomological results discussed here in the generality of $\mathbf{Rep}(R, G)$ rather than $\mathbf{Rep}(\mathbb{Z}, G)$.

Remark. At this point it's worth stressing one particular aspect of this theory. Many of the proofs involve showing that certain diagrams commute. When writing proofs on paper, some mathematicians don't give too much thought to the reasons why a particular diagram commutes but when formalizing theorems we need to be more careful than this. For that reason it is important to define all of our objects in as functorial a way as possible. In the example from the previous remark, saying that there is an isomorphism $H^n(G, F_1(M)) \cong F_2(H^n(G, M))$ is not as good as saying that there is an isomorphism of functors $H^n \circ F_1 \cong F_2 \circ H^n$. The isomorphism of functors implies that for every map $f : A \to B$ in $\mathbf{Rep}(R, G)$ we have a commuting square in $\mathbf{Mod}(\mathbb{Z})$.

$$\begin{array}{ccc} H^n(G, F_1(A)) & \overset{H^1(G,F_1(f))}{\to} & H^n(G, F_1(B)) \\ \downarrow & & \downarrow \\ F_2(H^n(G, M)) & \overset{F_2(H^1(G,f))}{\to} & F_2 H^n(G, B) \end{array}.$$

This commuting square might be crucial in some other proof. This is also the reason why we work with the categories `Rep R G` and `ModuleCat R`, rather than with `Representation R G M` and `Module R M` which could be more familiar.

`:restriction map`

Definition 6. If S is a subgroup of G, then we write $H^n(S, M)$ for the cohomology groups of the restricted representation $M \downarrow S$. If $f : G^n \to M$ is an element of $C^n(G, M)$, then we may restrict f to a function $S^n \to M$. Restricting functions in this way defines a map of cochain complexes $C^\bullet(G, M) \to C^\bullet(S, M)$, and hence a map of cohomology groups

$$\text{rest} : H^n(G, M) \to H^n(S, M).$$

This map is called the *restriction map*, and is a morphism of functors from $H^n(G, -)$ to $H^n(S, -) \circ$ **res**.

`ef:inflation map`

Definition 7. If S is a normal subgroup of G, then we write $H^n(G/S, M^S)$ for the cohomology groups of the representation M^S of G/S. If $f : (G/S)^n \to M^S$ is an element of $C^n(G/S, M^S)$, then we may "inflate" f to a function $G^n \to M$. This inflation process defines a map of cochain complexes $C^\bullet(G/S, M^S) \to C^\bullet(G, M)$, and hence a map of cohomology groups, called the *inflation map*:

$$\text{infl} : H^n(G/S, M^H) \to H^n(G, M).$$

More precisely, the inflation map is a morphism of functors from $H^n(S, -) \circ \mathbf{invar}$ to $H^n(G, -)$.

The following results are in a current PR.

`insFunctor exact`

Lemma 8. *The functor taking M to $C^\bullet(G, M)$ is exact. I.e. if $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then the corresponding sequence of cochain complexes is exact:*

$$0 \to C^n(G, A) \to C^n(G, B) \to C^n(G, C) \to 0.$$

As a consequence of this, we have the following (also a current PR):

`g exact sequence`

Definition 9. Given a short exact sequence $0 \to A \overset{f}{\to} B \overset{g}{\to} C \to 0$ in $\mathbf{Rep}(R, G)$, the corresponding sequence of cochain complexes is exact: $0 \to C^n(G, A) \to C^n(G, B) \to C^n(G, C) \to 0$. This implies that there exist "connecting homomorphisms" $\delta : H^n(G, C) \to H^{n+1}(G, A)$, such that the following is a long exact sequence:

$$0 \to H^0(G, A) \overset{H^0(f)}{\to} H^0(G, B) \overset{H^0(g)}{\to} H^0(G, C) \overset{\delta}{\to} H^1(G, A) \overset{H^1(f)}{\to} H^1(G, B) \overset{H^1(g)}{\to} H^1(G, C) \overset{\delta}{\to} \cdots.$$

ction naturality

Lemma 10. *Let S be a subgroup of G and suppose we have a short exact sequence $0 \to A \to B \to C \to 0$ in $\mathbf{Rep}(R, G)$. Then the sequence the sequence $0 \to A \downarrow S \to B \downarrow S \to C \downarrow S \to 0$ is exact in $\mathbf{Rep}(R, S)$. The following diagram commutes, where the rows are the long exact sequences for $0 \to A \to B \to C \to 0$ and for its restriction to S, and the vertical maps are restriction.*

$$\begin{array}{ccccccc} H^n(G,A) & \to & H^n(G,B) & \to & H^n(G,C) & \to & H^{n+1}(G,A) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^n(S,A) & \to & H^n(S,B) & \to & H^n(S,C) & \to & H^{n+1}(S,A) \end{array}$$

Suppose now that S is a normal subgroup of G. Then we have for every map $f : A \to B$ in $\mathbf{Rep}(R, G)$ a commuting square in which the vertical maps are inflation.

$$\begin{array}{ccc} H^n(G/S, A^S) & \overset{H^n(\mathbf{invar}(f))}{\to} & H^n(G/S, B^S) \\ \downarrow & & \downarrow \\ H^n(G, A) & \overset{H^n(f)}{\to} & H^n(G, B) \end{array}.$$

If $0 \to A \to B \to C \to 0$ is exact in $\mathbf{Rep}(R, G)$ and its inflation $0 \to A^S \to B^S \to C^S \to 0$ is also exact in $Rep(R, G/S)$, then we have a commutative diagram in which the rows are the corresponding long exact sequences and the vertical maps are inflation:

$$\begin{array}{ccccccc} H^n(G/S, A^S) & \to & H^n(G/S, B^S) & \to & H^n(G/S, C^S) & \overset{\delta}{\to} & H^{n+1}(G/S, A^S) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^n(G, A) & \to & H^n(G, B) & \to & H^n(G, C) & \overset{\delta}{\to} & H^{n+1}(G, A) \end{array}.$$

Proof. Most of the commuting squares have already been proved if inflation and restriction are defined as morphisms of functors. The remaining two squares are:

$$\begin{array}{ccc} H^n(G,C) & \overset{\delta}{\to} & H^{n+1}(G,A) \\ \text{rest} \downarrow & & \downarrow \text{rest} \\ H^n(S,C) & \overset{\delta}{\to} & H^{n+1}(S,A) \end{array} \quad \text{and} \quad \begin{array}{ccc} H^n(G/S, C^S) & \overset{\delta}{\to} & H^{n+1}(G/S, A^S) \\ \text{infl} \downarrow & & \downarrow \text{infl} \\ H^n(G,C) & \overset{\delta}{\to} & H^{n+1}(G,A) \end{array}.$$

Both of these can be deduced from the following statement in Mathlib:

`HomologicalComplex.HomologySequence.`δ`_naturality`

□

f:group homology

Definition 11. There is also a chain complex of R-modules:

$$\cdots \overset{d_2}{\to} C_2(G, M) \overset{d_1}{\to} C_1(G, M) \overset{d_0}{\to} C_0(G, M)$$

whose n-th term is the space of finitely supported functions $f : G^n \to_0 M$, with appropriately defined boundary maps d_n. In the literature $C_n(G, M)$ is often defined as $R[G]^{\otimes n} \otimes_R M$, to which it is canonically isomorphic. In the case $n = 0$ this is interpreted as meaning $C_0(G, M) = M$. The homology groups of $C_n(G, M)$ are called the *homology groups of M* and are written $H_n(G, M)$.

Example 12. *We'll sometimes write* $\text{single}(g, m)$ *for the function with value m at g and value zero elsewhere. The R-module $C_1(G, M)$ is spanned by the elements* $\text{single}(g, m)$ *for $g \in G$ and $m \in M$ (`Finsupp.single` in Mathlib). For such elements we have*

$$d_0(\text{single}(g, m)) = g \bullet m - m.$$

We shall write $I_G M$ for the submodule of M spanned by elements of the form $g \bullet m - m$. The quotient $M/I_G M$ is commonly called the coinvariants *of M and is written M_G; this is the largest quotient module on which G acts trivially. It follows that $H_0(G, M) \cong M_G$.*

2.3 Tate Cohomology

Throughout this section, the group G is assumed to be finite. Under this assumption, we show that the homology and cohomology groups may both be regarded as part of a bigger cohomology theory, which is called Tate cohomology.

def:norm **Definition 13.** Let G be a finite group and M a representation of G over a commutative ring R. There is a canonical linear map $N_G : M \to M$ called the *norm*, defined by

$$N_G(m) = \sum_{g \in G} g \bullet m.$$

We shall also regard the norm as a linear map from $C_0(G, M)$ to $C^0(G, M)$, both of which may be identified with M.

(We'll see in the next two lemmas that N_G commutes with the action of G, so is a morphism in $Rep(R, G)$. However, we shall only regard it as a morphism in $\mathbf{Mod}(R)$. The reason is that the chain and cochain modules $C^0(G, M)$ and $C_0(G, M)$ are regarded as R-modules rather than representations of G.)

lem:norm comm **Lemma 14.** *For any $g \in G$ and $m \in M$ we have $g \bullet N_G(m) = N_G(m)$ and $N_G(g \bullet m) = N_G(m)$.*

lem:norm comp d **Lemma 15.** *The composition $d^0 \circ N_G$ is zero.*

Proof. The map $d^0 : M \to (G \to M)$ is given by $(d^0 m)(g) = m - g \bullet m$. Using this formula, we obtain (by Lemma 14) $d^0(N_G m)(g) = N_G m - g \bullet N_G m = 0$. □

lem:d comp norm **Lemma 16.** *The composition $N_G \circ d_0$ is zero.*

Proof. Since the elements $\mathrm{single}(g, m)$ span $C_1(G, M)$, it's sufficient to check that these are all mapped to 0. We have by 14

$$N_G(d_0(\mathrm{single}(g, m))) = N_G(g \bullet m - m) = N_G(g \bullet m) - N_G(m) = 0.$$

□

:norm naturality **Lemma 17.** *For every map $f : A \to B$ in $\mathbf{Rep}(R, G)$ we have a commuting square:*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ N_G \downarrow & & \downarrow N_G. \\ A & \xrightarrow{f} & B \end{array}$$

Equivalently, N_G is an endomorphism of the forgetful functor $\mathbf{Rep}(R, G) \to \mathbf{Mod}(R)$.

Proof. For $m \in M$ we have

$$f(N_G(m)) = f\left(\sum_{g \in G} g \bullet m\right) = \sum_{g \in G} g \bullet f(m) = N_G(f(m)).$$

□

:Tate cohomology

Definition 18. Recall that we have a cochain complex $C^n(G,M)$, indexed by $n \in \mathbb{N}$, whose zeroth term may be identified with M. We also have a chain complex $C_n(G,M)$ whose zeroth term may be identified with M. By lem:norm lemma comp comp norm 15 and 16, we may glue these together with the map $N_G : M \to M$ to obtain a cochain complex indexed by $\mathbb{Z}$:

$$\cdots \to C_2(G,M) \to C_1(G,M) \xrightarrow{d_0} C_0(G,M) \xrightarrow{N_G} C^0(G,M) \xrightarrow{d^0} C^1(G,M) \to C^2(G,M) \to \cdots$$

We shall write $C^n_{\mathrm{Tate}}(G,M)$ for this cochain complex, and we normalize the indices so that for natural numbers n we have $C^n_{\mathrm{Tate}}(G,M) = C^n(G,M)$. This implies $C^{-n-1}_{\mathrm{Tate}}(G,M) = C_n(G,M)$. It follows from lem:norm naturality 17 that $C^\bullet_{\mathrm{Tate}}(G,M)$ is functorial in M.

For an integer n, we shall write $H^n_{\mathrm{Tate}}(G,M)$ for the n-th cohomology of the complex $C^n_{\mathrm{Tate}}(G,M)$; this is called the n-th Tate cohomology of M, and is often written $\hat{H}^n(G,M)$ or (confusingly) just $H^n(G,M)$ in the literature. We stress that Tate cohomology exists only in the case that G is a finite group.

logy or homology

Lemma 19. *Let G be a finite group and M a representation of G.*

- *The zeroth Tate cohomology $H^0_{\mathrm{Tate}}(G,M)$ is isomorphic to $M^G/N_G(M)$. In particular if M is a trivial representation of G then $H^0_{\mathrm{Tate}}(G,M) \cong M/|G|M$.*
- *For $n > 0$ we have (an isomorphism of functors in the variable M)*
$$H^n_{\mathrm{Tate}}(G,M) \cong H^n(G,M).$$
- *There is an isomorphism*
$$H^{-1}_{\mathrm{Tate}}(G,M) \cong \ker(N_G : M \to M)/I_G M,$$
Where $I_G M$ is the submodule of M generated by elements of the form $g \bullet m - m$. In particular if M is a trivial representation of G then $H^{-1}_{\mathrm{Tate}}(G,M)$ is isomorphic to the $|G|$-torsion in M.
- *For $n < -1$ we have (an isomorphism of functors in the variable M)*
$$H^n_{\mathrm{Tate}}(G,M) \cong H_{-1-n}(G,M).$$

Proof. This result is clear from the definition for $n > 0$ and $n < -1$. We'll discuss the two remaining cases.

The 0-cocycle submodule is the kernel of the map $d^0 : C^0(G,M) \to C^1(G,M)$. This is the same as $H^0(G,M)$, which is isomorphic to M^G. On the other hand $B^0_{\mathrm{Tate}}(G,M)$ is by definition the image of $N_G : M \to M$.

Similarly, $H_0(G,M)$ is the quotient of M by $I_G M$, and $H^{-1}_{\mathrm{Tate}}(G,M)$ is by definition the quotient of $\ker(N_G : M \to M)$ by the same submodule. □

g exact sequence

Definition 20. Since the functors $C^\bullet(G,-)$ and $C_\bullet(G,-)$ are both exact, it follows that $C^\bullet_{\mathrm{Tate}}(G,-)$ is an exact functor. Hence, given any short exact sequence in $\mathbf{Rep}(R,G)$:

$$0 \to A \to B \to C \to 0,$$

we obtain a short exact sequence of Tate complexes and therefore connecting homomorphisms $\delta : H^n_{\mathrm{Tate}}(G,C) \to H^{n+1}_{\mathrm{Tate}}(G,A)$ such that the following is a long exact sequence (for $n \in \mathbb{Z}$):

$$\cdots \to H^n_{\mathrm{Tate}}(G,A) \to H^n_{\mathrm{Tate}}(G,B) \to H^n_{\mathrm{Tate}}(G,C) \to H^{n+1}_{\mathrm{Tate}}(G,A) \to H^{n+1}_{\mathrm{Tate}}(G,B) \to \cdots$$

The exactness statements are in Mathlib in the namespace `HomologicalComplex.HomologySequence`. The connecting maps $\delta : H^n_{\mathrm{Tate}}(G,C) \to H^n_{\mathrm{Tate}}(G,A)$ coincide with those for cohomology for $n \geq 1$ and with those for homology of $n \leq -3$.

2.4 Coinduced and induced representations

ivial cohomology

Definition 21. Let M be a representation of G over a ring R.

- M is said to have *trivial cohomology* if for every subgroup $S \leq G$ and every $n > 0$, $H^n(S, M) \cong 0$.
- M is said to have *trivial homology* if for every subgroup $S \leq G$ and every $n > 0$, $H_n(S, M) \cong 0$.
- Suppose the group G is finite. Then M is said to have *trivial Tate cohomology* if for every subgroup $S \leq G$ and every $n \in \mathbb{Z}$, $H^n_{\mathrm{Tate}}(S, M) \cong 0$.

(We will later see that for a finite group G, the three concepts are equivalent.)

In this section we shall construct certain representations with trivial homology and cohomology.

def:induced

Definition 22. Let G be a group, R a commutative ring and A an R-module.

- There is a representation of G over R on the space of all functions $f : G \to A$. The action of an element $g \in G$ on f is defined by

$$(g \bullet f)(x) = f(xg).$$

  This representation is called the coinduced representation and is denoted $\mathrm{coind}_1(G, A)$.

- There is a representation of G over R on the space of all finitely supported functions $f : G \to_0 A$. The action of an element $g \in G$ on f is defined by

$$(g \bullet f)(x) = f(g^{-1}x), \qquad i.e. g \bullet \mathrm{single}(x, m) = \mathrm{single}(gx, m).$$

  This representation is called the induced representation and is denoted $\mathrm{ind}_1(G, A)$.

More precisely, $\mathrm{coind}_1(G, -)$ and $\mathrm{ind}_1(G, -)$ are both functors from $\mathbf{Mod}(R)$ to $\mathbf{Rep}(R, G)$.

ivial cohomology

Lemma 23. *The representation* $\mathrm{coind}_1(G, A)$ *has trivial cohomology.*

Proof. There is an elementary proof outlined in lean file involving cocycles which we describe here. A more intuitive method of proof would give a more general statement (Shapiro's Lemma). The proof given here is most easily stated in terms of inhomogeneous cochains, rather than the homogeneous cochains in Mathlib, so we explain the proof in that context first, before reformulating the same proof in terms of inhomogeneous cochains.

Choose any subgroup S of G and let $n > 0$; we shall prove that $H^n(S, \mathrm{coind}_1(A)) \cong 0$. Let $\{g_i\}$ be a set of coset representatives for G/S. Recall that a homogeneous n-cochain on S with values in $\mathrm{coind}_1(A)$ is a function $\sigma : S^{n+1} \to (G \to A)$ satisfying (for all $s, s_0, \dots, s_n \in S$ and $g \in G$) the following homogeneity condition:

$$\sigma(ss_0, ..., ss_n)(g) = \sigma(s_0, ..., s_n)(gs).$$

The cochain σ is a cocycle if it satisfies the following cocycle relation for all $s_i \in S$, $g \in G$:

$$\sum_i (-1)^i \sigma(s_0, ..., \widehat{s_i}, ..., s_{n+1})(g) = 0.$$

Given a homogeneous n-cocycle σ, we'll define a homogeneous $n-1$-cochain τ by

$$\tau(s_0, ..., s_{n-1})(g_i) = \sigma(s^{-1}, s_0, ..., s_{n-1})(g_i s).$$

The cocycle relation for σ implies $d^{n-1}\tau = \sigma$, so σ is a coboundary.

Let's rephrase this in terms of inhomogeneous cocycles. The inhomogeneous cocycle corresponding to σ is

$$\sigma'(s_1, ..., s_n)(g_i s) = \sigma(1, s_1, s_1 s_2, ..., s_1 \cdots s_n)(g_i s)$$

and the inhomogeneous cochain corresponding to τ is

$$\begin{aligned}\tau'(s_1, ..., s_{n-1})(g_i s) &= \tau(1, s_1, ..., s_1 \cdots s_{n-1})(g_i s) \\ &= \sigma(s^{-1}, 1, s_1, s_1 s_2, \dots, s_1 \cdots s_n)(g_i s) \\ &= \sigma(1, s, s s_1, s s_1 s_2, ..., s s_1 \cdots s_{n-1})(g_i) \\ &= \sigma'(s, s_1, \dots, s_{n-1})(g_i).\end{aligned}$$

The final formula above defines an inhomogeneous cochain $\tau' \in C^{n-1}(G, \mathrm{coind}_1(A))$, such that $d^{n-1}\tau' = \sigma'$. Therefore $H^n(S, \mathrm{coind}_1(A)) = 0$. □

coind invariants

Lemma 24. *Let S be a normal subgroup of G. Then $\mathrm{coind}_1(G, A)^S$ is isomorphic to $\mathrm{coind}_1(G/S, A)$. In particular $\mathrm{coind}_1(G, A)^S$ is has trivial cohomology as a representation of G/S.*

Proof. Let $f : G \to A$. Then f is in the subspace $\mathrm{coind}_1(G, A)^S$ if f is constant on cosets of S, i.e. it descends to a function $G/S \to A$. This gives a linear bijection $\mathrm{coind}_1(G, A)^S \cong \mathrm{coind}_1(G/S, A)$, and it's trivial to check that this map is compatible with the actions of G. □

trivial homology

Lemma 25. *The representation $\mathrm{ind}_1(G, A)$ has trivial homology.*

Proof. There is an elementary proof, similar to that of lem:coind trivial cohomology 23. □

ef:ind to coind

Definition 26. There is a morphism of representations $\mathrm{ind}_1(G, A) \to \mathrm{coind}_1(G, A)$, which takes a finitely supported function $f : G \to_0 A$ to the function

$$x \mapsto f(x^{-1}).$$

If the group G is finite then this map is an isomorphism. More precisely, this is an isomorphism of functors $\mathrm{ind}_1(G, -) \cong \mathrm{coind}_1(G, -)$.

ced trivial Tate

Lemma 27. *If the group G is finite then $\mathrm{ind}_1(G, A)$ and $\mathrm{coind}_1(G, A)$ have trivial Tate cohomology.*

Proof. These representations are isomorphic, so it's sufficient to prove that $\mathrm{ind}_1(G, A)$ has trivial Tate cohomology (this is the more convenient case to prove). We already know that $\mathrm{ind}_1(G, A)$ has trivial homology. Also, since it is isomorphic to $\mathrm{coind}_1(G, A)$, it must have trivial cohomology. It only remains to prove that $H^0_{\mathrm{Tate}}(S, \mathrm{ind}_1(M))$ and $H^{-1}_{\mathrm{Tate}}(S, \mathrm{ind}_1(M))$ are zero for all subgroups S of G.

Recall that $\mathrm{ind}_1(G, M)$ is the space of functions $G \to_0 M$, and the action of G is by left-translation:

$$g \bullet \mathrm{single}(x, m) = \mathrm{single}(gx, m).$$

To prove that $H^0_{\mathrm{Tate}}(S, \mathrm{ind}_1(G, A)) = 0$, we use the isomorphism lem:Tate cohomology is cohomology or homology 19:

$$H^0_{\mathrm{Tate}}(S, \mathrm{ind}_1(G, A)) \cong \mathrm{ind}_1(G, A)^S / N_S \mathrm{ind}_1(G, A).$$

A function $f : G \to_0 M$ is S-invariant if f is constant on cosets Sg of S. If we let $\{g_i\}$ be a set of coset representatives, then we have $f = N_S(\sum_i \text{single}(g_i, f(g_i)))$. Therefore $H^0_{\text{Tate}}(S, \text{ind}_1(G, A)) = 0$.

For the $n = -1$ case we use the isomorphism [lem:Tate cohomology is cohomology or homology 19]:

$$H^{-1}_{\text{Tate}}(S, \text{ind}_1(G, A)) \cong \ker(N_S : \text{ind}_1(G, A) \to \text{ind}_1(G, A))/I_S\text{ind}_1(M),$$

where $I_G\text{ind}_1(M)$ is generated by elements of the form $s \bullet f - f$ for $s \in S$ and $f : G \to M$. Suppose $f : G \to_0 M$ is in the kernel of N_S. This implies that the sum of the values of f over each coset of S is zero. We can then write f in the form

$$\begin{aligned} f &= \sum_i \sum_{s \in S} (\text{single}(sg_i, f(sg_i)) - \text{single}(g_i, f(sg_i))) \\ &= \sum_i \sum_{s \in S} (s \bullet \text{single}(g_i, f(sg_i)) - \text{single}(g_i, f(sg_i))). \end{aligned}$$

Therefore $f \in I_S\text{ind}_1(M)$. This shows that $H^{-1}(S, \text{ind}_1(M)) = 0$. □

2.5 Dimension-shifting

2.5.1 Shifting up

def:coind ' **Definition 28.** Let G be a group and M a representation of G over a commutative ring R. There is a representation $\text{coind}'_1(M)$ on the R-module of functions $G \to M$. The action of an element $g \in G$ on a function $f : G \to M$ is given by

$$(g \bullet f)(x) = g \bullet (f(xg)).$$

oind ' iso coind **Lemma 29.** *The representations* $\text{coind}'_1(M)$ *and* $\text{coind}_1(G, M)$ *of* G *are isomorphic. More precisely there is an isomorphism of functors* $\text{coind}'_1 \cong \text{coind}_1(G, -) \circ$ **forget**, *where* **forget** : $\mathbf{Rep}(R, G) \to \mathbf{Mod}(R)$ *is the forgetful functor.*

Proof. The map $f \mapsto (x \mapsto x \bullet f(x))$ is an isomorphism from $\text{coind}'_1(M)$ to $\text{coind}_1(G, M)$. □

ivial cohomology **Corollary 30.** *The representation* $\text{coind}'_1(M)$ *has trivial cohomology.*

Proof. This follows directly from Lemmas [lem:coind ' iso coind 29] and [lem:induced trivial cohomology 23]. □

ivial cohomology **Corollary 31.** *Let* S *be a normal subgroup of* G*. Then* $\text{coind}'_1(M)^S$ *has trivial cohomology as a representation of* G/S*.*

Proof. We've seen in Lemma [lem:coind ' iso coind 29] that $\text{coind}'_1(M)$ is isomorphic to $\text{coind}_1(M)$. Applying the functor **invar**, we obtain an isomorphism between $\text{coind}'_1(M)^S$ and $\text{coind}_1(M)^S$. The result then follows from Lemma [lem:coind trivial cohomology 23]. □

def:up **Definition 32.** There is an injective morphism $M \to \text{coind}'_1(M)$ which takes a vector $m \in M$ to the constant function on G with value m. We define a representation $\text{up}(M)$ to be the cokernel of this map, so that we have a short exact sequence

$$0 \to M \to \text{coind}'_1(M) \to \text{up}(M) \to 0.$$

This construction is functorial in M; in particular for every $f : M_1 \to M_2$ in $\mathbf{Rep}(R, G)$, there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \to & M_1 & \to & \text{coind}'_1(M_1) & \to & \text{up}(M_1) \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & M_2 & \to & \text{coind}'_1(M_2) & \to & \text{up}(M_2) \to 0 \end{array}.$$

cor:up iso

Corollary 33. *Let S be any subgroup of G and let $n \geq 1$. Then the connecting map from the long exact sequence $H^n(S, \mathrm{up}(M)) \to H^{n+1}(S, M)$ is an isomorphism. The corresponding map $H^0(S, \mathrm{up}(M)) \to H^1(S, M)$ is surjective.*

The isomorphism $H^n(G, \mathrm{up}(-)) \cong H^{n+1}(G, -)$ is an isomorphism of functors. This means that for every morphism $f : M \to N$ of representations, the following square commutes:

$$\begin{array}{ccc} H^n(G, \mathrm{up}(M)) & \cong & H^{n+1}(G, M) \\ \downarrow & & \downarrow \\ H^n(G, \mathrm{up}(N)) & \cong & H^{n+1}(G, N) \end{array}.$$

Proof. We have already shown in Corollary 30 that $\mathrm{coind}_1'(M)$ has trivial cohomology, so $H^r(S, \mathrm{coind}_1'(M)) = 0$ for all $r > 0$. This implies that the connecting maps are isomorphisms.

cor:coind ' trivial cohomology

The commuting square follows from `HomologicalComplex.HomologySequence.δ_naturality` because the short exact sequence $0 \to M \to \mathrm{coind}_1'(M) \to \mathrm{up}(M) \to 0$ is functorial in M. □

2.5.2 Shifting down

Let G be a group and M a representation of G over a commutative ring R.

def:ind '

Definition 34. There is a representation $\mathrm{ind}_1'(M)$ on the R-module of finitely supported functions $G \to_0 M$. The action of an element $g \in G$ on a function $f : G \to_0 M$ is given by

$$(g \bullet f)(x) = g \bullet (f(g^{-1}x)), \qquad \text{i.e. } g \bullet \mathrm{single}(g, m) = \mathrm{single}(gx, g \bullet m).$$

The map ind_1' is functorial in M.

em:ind ' iso ind

Lemma 35. *The representations $\mathrm{ind}_1'(M)$ and $\mathrm{ind}_1(G, M)$ are isomorphic; more precisely the functors ind_1' and $\mathrm{ind}_1(G, -) \circ$ **forget** are isomorphic.*

Proof. The data of the isomorphism is contained in the lean file; the isomorphism takes $f : G \to_0 M$ to the finitely supported function

$$x \mapsto x^{-1} \bullet f(x).$$

It remains to check linearity and naturality. □

trivial homology

Corollary 36. *The representation $\mathrm{ind}_1'(M)$ has trivial homology.*

Proof. We've shown that $\mathrm{ind}_1'(M)$ is isomorphic to $\mathrm{ind}_1(M)$, which is already known to have trivial homology. □

def:down

Definition 37. For any representation M, there is a surjective morphism $\mathrm{ind}_1'(M) \to M$, which takes a finitely supported function $f : G \to_0 M$ to the sum $\sum_{x \in G} f(x)$. We define $\mathrm{down}(M)$ to be the kernel of this map. There is therefore a short exact sequence

$$0 \to \mathrm{down}(M) \to \mathrm{ind}_1'(M) \to M \to 0.$$

Both $\mathrm{down}(M)$ and the short exact seqeunce are functors of M; this means that for every map $f : M \to N$ in $\mathbf{Rep}(R, G)$, we have a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & \mathrm{down}(M) & \to & \mathrm{ind}_1'(M) & \to & M & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathrm{down}(N) & \to & \mathrm{ind}_1'(N) & \to & N & \to & 0 \end{array}.$$

ed' trivial Tate **Lemma 38.** *If M is a representation of a finite group G then the representations $\mathrm{ind}_1'(M)$ and $\mathrm{coind}_1'(M)$ have trivial Tate cohomology.*

Proof. This follows from 27 together with the isomorphisms 26, 29 and 35. □

ate up down isos **Corollary 39.** *If the group G is finite then for every subgroup S of G and every $n \in \mathbb{Z}$ we have isomorphisms*

$$H^n_{\mathrm{Tate}}(S, \mathrm{up}(M)) \cong H^{n+1}_{\mathrm{Tate}}(S, M), \qquad H^{n+1}_{\mathrm{Tate}}(S, \mathrm{down}(M)) \cong H^n_{\mathrm{Tate}}(S, M).$$

Proof. These are the connecting homomorphisms from the short exact sequences linking $\mathrm{up}(M)$ and $\mathrm{down}(M)$ to M. They are isomorphisms because $\mathrm{coind}_1'(M)$ and $\mathrm{ind}_1'(M)$ have trivial Tate cohomology. □

As a simple example we consider the case of the trivial representation R. The induced representation is then the group ring RG, which is referred to Mathlib as `Rep.leftRegular R G`; this is a free R-module with basis $\mathrm{single}(g,1)$ for $g \in G$. For simplicity we shall write $[g]$ for the basis vector $\mathrm{single}(g,1)$. The map $\mathrm{ind}_1'(R) \to R$ takes $\sum_{g\in G} x_g[g]$ to $\sum_{g \in G} x_g$. This map is commonly called the augmentation, and its kernel $\mathrm{down}(R)$ the augmentation module. We shall write $\mathrm{aug}(R,G)$ for this kernel. The kernel $\mathrm{aug}(R,G)$ is spanned by the elements $[g]-[1]$ for $g \in G$. Note that $I_G\mathrm{aug}(R,G)$ is spanned by elements of the form $[gh]-[h]-[g]+[1]$.

m:homology 0 aug **Lemma 40.** *Let G be a finite group. Then there is an isomorphism of R-modules*

$$G^{\mathrm{ab}} \otimes_{\mathbb{Z}} R \cong H_0(G, \mathrm{aug}(R,G)),$$

which takes an element $g \otimes 1$ for $g \in G$ to the coset of $[g]-[1]$ in $\mathrm{aug}(R,G)/I_G\mathrm{aug}(R,G)$. In particular, taking $R = \mathbb{Z}$ we have an isomorphism

$$G^{\mathrm{ab}} \cong H_0(G, \mathrm{aug}(\mathbb{Z}, G)).$$

Proof. We'll first define a function $\phi : G \to H_0(G, \mathrm{aug}(G,R))$ by $\phi(g) = [g]-[1]$. The following calculation shows that ϕ is a group homomrphism.

$$\begin{aligned}\phi(gh) &= \phi(g) + \phi(h) + ([gh]-[1]) - ([g]-[1]) - ([h]-[1])\\ &= \phi(g) + \phi(h) + [gh] - [g] - [h] + [1]\\ &\equiv \phi(g) + \phi(h) \bmod I_G\mathrm{aug}(R,G).\end{aligned}$$

It follows that ϕ descends to a homomorphism $G^{\mathrm{ab}} \to H_0(G, \mathrm{aug}(R,G))$, which may be extended uniquely to a linear map $G^{\mathrm{ab}} \otimes R \to H_0(G, \mathrm{aug}(R,G))$.

Next we define a linear map $\psi : \mathrm{aug}(G,R) \to G^{\mathrm{ab}} \otimes R$ taking the generator $[g]-[1]$ to $g \otimes 1$. It's trivial to check that $I_G\mathrm{aug}(R,G)$ is in the kernel of ψ, so ψ descends to a map $H_0(G, \mathrm{aug}(R,G)) \to G^{\mathrm{ab}} \otimes R$. The two maps are easily seen to be inverses. □

Suppose now that the group G is finite. The map $N_G : \mathrm{aug}(R,G) \to \mathrm{aug}(R,G)$ in this case is zero, so we have

$$H^{-2}(G,\mathbb{Z}) \cong H^{-1}_{\mathrm{Tate}}(G, \mathrm{aug}(\mathbb{Z},G)) \cong H_0(G, \mathrm{aug}(\mathbb{Z},G)) \cong G^{\mathrm{ab}}. \tag{2.1}$$ eq:Tate -1 aug

2.6 The inflation-restriction sequence

riction sequence

Theorem 41. *Let S be a normal subgroup of a group G and let n be a positive integer. Assume that for all natural numbers $0 < i < n$ we have $H^i(S, M) \cong 0$. Then the following sequence is exact:*

$$0 \to H^n(G/S, M^S) \to H^n(G, M) \to H^n(S, M),$$

where the first map is inflation and the second is restriction.

Proof. This is already in Mathlib for $n = 1$. Assume the result is true for n; we will prove it for $n + 1$ by dimension-shifting.

Let M be a representation such that $H^i(S, M) = 0$ for all $0 < i < n + 1$. This implies $H^i(S, \mathrm{up}(M)) = 0$ for all $0 < i < n$. Hence by the inductive hypothesis the following sequence is exact:

$$0 \to H^n(G/S, \mathrm{up}(M)^S) \to H^n(G, \mathrm{up}(M)) \to H^n(S, \mathrm{up}(M)).$$

Recall that we have a short exact sequence of representations of G:

$$0 \to M \to \mathrm{coind}_1'(M) \to \mathrm{up}(M) \to 0.$$

Since $0 < 1 < n + 1$ we have $H^1(S, M) = 0$, so by taking S-invariants we obtain a short exact sequence of G/S-modules:

$$0 \to M^S \to \mathrm{coind}_1'(M)^S \to \mathrm{up}(M)^S \to 0.$$

cor:coind_' invariants trivial cohomology

By 31, $\mathrm{coind}_1'(M)^S$ has trivial cohomology, so we have an isomorphism

$$H^n(G/S, \mathrm{up}(M)^S) \to H^{n+1}(G/S, M^S).$$

We now have a diagram where the horizontal maps are inflation and restriction maps and the vertical maps are dimension-shifting isomorphisms.

$$\begin{array}{ccccccc} 0 & \to & H^n(G/S, \mathrm{up}(M)^S) & \to & H^n(G, \mathrm{up}(M)) & \to & H^n(S, \mathrm{up}(M)) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & H^{n+1}(G/S, M^S) & \to & H^{n+1}(G, M) & \to & H^{n+1}(S, M). \end{array}$$

lem:inflation_restriction_naturality

The diagram commutes by 10. The first row is exact by the inductive hypothesis. Therefore the second row is also exact. □

2.7 Corestriction

Let S be a subgroup of G. We have already discussed the restriction map $H^\bullet(G, M) \to H^\bullet(S, M)$. In the case that S has finite index in G there is also a "corestriction map" which goes in th other direction, i.e. $\mathrm{cor} : H^\bullet(S, -)$ to $H^\bullet(G, -)$. We define this now, and point out some easy consequences of the definition.

ef:corestriction

Definition 42. Let S be a subgroup of finite index in G and let $\{r_i\}$ be a set of representatives for the cosets $r_i S$. For any representation M of G there is a linear map $N_{G/S} : M^S \to M^G$ defined by

$$N_{G/S}(m) = \sum_i r_i \bullet m.$$

This map does not depend on the choince of coset representatives. Also, the map $N_{G/S}$ is a morphism of functors, i.e. for every map $f : A \to B$ in $\mathbf{Rep}(R, G)$ we have a commuting square in $\mathbf{Mod}(R)$:

$$\begin{array}{ccc} A^S & \to & B^S \\ \downarrow & & \downarrow \\ A^G & \to & B^G \end{array},$$

where the horizontal maps are induced by f and the vertical maps are $N_{G/S}$.

The corestriction maps $\mathrm{cor}^n : H^n(S, M) \to H^n(G, M)$ are defined recursively as follows:

- The map $\mathrm{cor}^0 : H^0(S, M) \to H^0(G, M)$ is defined to be $N_{G/S}$.
- Assume that we have defined cor^n. For any M we have a commutative diagram in which the rows are exact and the vertical arrows are cor^n:

$$\begin{array}{ccccccc} H^n(S, \mathrm{coind}_1'(M)) & \to & H^n(S, \mathrm{up}(M)) & \to & H^{n+1}(S, M) & \to & 0 \\ \downarrow & & \downarrow & & & & \\ H^n(S, \mathrm{coind}_1'(M)) & \to & H^n(S, \mathrm{up}(M)) & \to & H^{n+1}(S, M) & \to & 0 \end{array}.$$

  It follows that there is a unique linear map $\mathrm{cor}^{n+1} : H^{n+1}(S, M) \to H^{n+1}(G, M)$ such that the following square commutes:

$$\begin{array}{ccc} H^n(S, \mathrm{up}(M)) & \to & H^{n+1}(S, M) \\ \downarrow & & \downarrow \\ H^n(S, \mathrm{up}(M)) & \to & H^{n+1}(S, M) \end{array}.$$

The map $\mathrm{cor}^n : H^n(G, -) \to H^n(S, -)$ is a morphism of functors.

em:cor comp rest

Lemma 43. *For all $\sigma \in H^n(G, M)$ we have $\mathrm{cor}(\mathrm{rest}(\sigma)) = [G : S] \cdot \sigma$.*

Proof. We'll prove the result by induction on n. In the case $n = 0$, this follows from the relation for all $m \in M^G$:

$$N_{G/S}(m) = [G : S] \cdot m,$$

The identity above holds because each term in the sum defining $N_{G/S}(m)$ is equal to m.

Let's assume that the lemma is true for some n. We then have a diagram in which the vertical maps are the dimension shifting maps, which are all surjective:

$$\begin{array}{ccccc} H^n(G, \mathrm{up}\ M) & \overset{\mathrm{rest}}{\to} & H^n(S, \mathrm{up}\ M) & \overset{\mathrm{cor}}{\to} & H^n(G, \mathrm{up}\ M) \\ \downarrow & & \downarrow & & \downarrow \\ H^{n+1}(G, M) & \overset{\mathrm{rest}}{\to} & H^{n+1}(S, M) & \overset{\mathrm{cor}}{\to} & H^{n+1}(G, M) \end{array}.$$

By the inductive hypothesis, the composition of the maps on the top row is multiplication by $[G : S]$. The square on the left commutes by lem:inflation restriction naturality 10, and the square on the right commutes by definition of the corestriction map. Therefore the composition on the bottom row is multiplication by $[G : S]$. □

mology G-torsion

Corollary 44. *If M is a representation of a finite group G then for all $n \in \mathbb{Z}$ and all $\sigma \in H^n_{\mathrm{Tate}}(G, M)$ we have $|G| \cdot \sigma = 0$.*

Proof. By dimension-shifting it's enough to prove the result for $n > 0$, in which case Tate cohomology is the same as cohomology. Take S to be the trivial subgroup 1 of G. By lem:cor comp rest 43 it's sufficient to prove that $\mathrm{cor}(\mathrm{rest}(\sigma)) = 0$. This follows because $\mathrm{rest}(\sigma) \in H^n(1, M) \cong 0$. □

mology sub Sylow

Corollary 45. *Let M be a representation of a finite group G and let S_p be a Sylow p- subgroup of G for some prime number p. Then for any $n \in \mathbb{Z}$, $H^n_{\mathrm{Tate}}(G, M)[p^\infty]$ is isomorphic to an R-submodule of $H^n_{\mathrm{Tate}}(S_p, M)$.*

Proof. By dimension-shifting it's enough to prove the result for $n \geq 0$, in which case Tate cohomology is the same as cohomology. It follows from lem:cor comp rest 43 that the composition cor $\circ$ rest is injective on $H^n(G, M)[p^\infty]$. Therefore the restriction map is an injective map from $H^n(G, M)[p^\infty]$ to $H^n(S_p, M)$. □

2.8 Periodicity for finite cyclic groups

In this section we shall assume that G is a finite cyclic group of order n. We shall write gen for a fixed generator of G.

def:up iso down

Definition 46. Given any representation M of G, there is a map $\mathrm{map}_1 : \mathrm{coind}'_1(M) \to \mathrm{coind}'_1(M)$ which takes a function $f : G \to M$ to the function

$$x \mapsto f(x) - f(\mathrm{gen} \cdot x).$$

The kernel of map_1 consists of the constant functions $G \to M$, i.e. the image of the map $M \to \mathrm{coind}'_1(M)$. Hence by the first isomorphism theorem, the image of map_1 is isomorphic to $\mathrm{up}(M)$.

Since G is finite, the representations $\mathrm{coind}'_1(M)$ and $\mathrm{ind}'_1(M)$ are isomorphic, and we define map_2 to be the corresponding map $\mathrm{ind}'_1(M) \to \mathrm{ind}'_1(M)$. This is given by

$$\mathrm{map}_2(f)(x) = f(x) - f(x \cdot \mathrm{gen}^{-1}).$$

Lemma 47. *The image of $\mathrm{map}_2 : \mathrm{ind}'_1(M) \to \mathrm{ind}'_1(M)$ is precisely the set of functions $G \to_0 M$ which sum to zero. This is the kernel of the map $\mathrm{ind}'_1(M) \to M$, which we are calling $\mathrm{down}(M)$.*

Proof. It's clear that the values of $\mathrm{map}_2(f)$ sum to 0, so the image of map_2 is contained in the kernel. Conversely suppose $h : G \to_0 M$ satisifies $\sum_{i=0}^{n-1} h(\mathrm{gen}^i) = 0$. Then we have

$$\begin{aligned} h &= \sum_0^{n-1} \mathrm{single}(gen^i, h(\mathrm{gen}^i)) \\ &= \sum_0^{n-1} (\mathrm{single}(gen^i, h(\mathrm{gen}^i)) - \mathrm{single}(1, h(\mathrm{gen}^i))). \end{aligned}$$

Furthermore each of the terms $\mathrm{single}(gen^i, m) - \mathrm{single}(1, m)$ is in the image of map_2:

$$\mathrm{map}_2(\mathrm{single}(1, m) + \cdots + \mathrm{single}(\mathrm{gen}^{i-1}, m)) = \mathrm{single}(1, m) - \mathrm{single}(\mathrm{gen}^i, m).$$

□

We have a commutative square with vertical isomorphisms:

$$\begin{array}{ccc} \mathrm{ind}'_1(M) & \overset{\mathrm{map}_2}{\to} & \mathrm{ind}'_1(M) \\ \downarrow & & \downarrow \\ \mathrm{coind}'_1(M) & \overset{\mathrm{map}_1}{\to} & \mathrm{coind}'_1(M) \end{array}.$$

It follows that $\mathrm{im}(\mathrm{map}_1) \cong \mathrm{im}(\mathrm{map}_2)$, i.e.

$$\mathrm{up}(M) \cong \mathrm{down}(M).$$

This is an isomorphism of functors; i.e. for each map $f : M \to N$ in $\mathbf{Rep}(R, G)$ we have a commuting square:

$$\begin{array}{ccc} \mathrm{up}(M) & \overset{\mathrm{up}(f)}{\to} & \mathrm{up}(N) \\ \downarrow & & \downarrow \\ \mathrm{down}(M) & \overset{\mathrm{down}(f)}{\to} & \mathrm{down}(N) \end{array}.$$

iodic cohomology **Corollary 48.** *Let G be a finite cyclic group. For all $n > 0$ and all representations M we have an isomorphism $H^n(G, M) \cong H^{n+2}(G, M)$. Similarly for all integers n we have isomorphisms $H^n_{\mathrm{Tate}}(G, M) \cong H^{n+2}_{\mathrm{Tate}}(G, M)$.*

Proof. By the dimension-shifting isomorphisms we have $H^n(G, M) \cong H^{n+1}(G, \mathrm{down}(M)) \cong H^{n+1}(G, \mathrm{up}(M)) \cong H^{n+2}(G, M)$, and similarly for Tate cohomology. □

A very important example for us is the trivial representation of G on $\mathbb{Z}$, which we describe very precisely here:

lem:H2 cyclic Z **Lemma 49.** *Let G be a finite cyclic group of order n generated by an element* gen*. Then $H^1(G, \mathbb{Z}) \cong 0$ and $H^2(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. Explicitely, the isomorphism $\mathrm{inv}_{\mathbb{Z}} : H^2(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ is given by the map (for a 2-cocycle σ)*

$$\mathrm{inv}_{\mathbb{Z}}(\sigma) = \sum_{i=0}^{n-1} \sigma(\mathrm{gen}^i, \mathrm{gen}).$$

The pre-image of $1 \in \mathbb{Z}/n\mathbb{Z}$ is the cohomology class of the cocycle

$$\sigma_1(\mathrm{gen}^i, \mathrm{gen}^j) = \begin{cases} 1 & i + j \geq n \\ 0 & i + j < n, \end{cases} \qquad 0 \leq i, j < n.$$

Proof. It is easy to check that the formula for $\mathrm{inv}_{\mathbb{Z}}$ defines a homomorphism $H^2(G, \mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ (i.e. the coboundaries are in the kernel). Furthermore we can check that σ_1 is a 2-cocycle and is a preimage of $1 \in \mathbb{Z}/n\mathbb{Z}$. It follows that the map $\mathrm{inv}_{\mathbb{Z}} : H^2(G, \mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ is surjective.

lem:Tate cohomology is cohomo

Since the module $\mathbb{Z}$ is trivial, we have $H^1(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Z}) \cong 0$. It follows from 19 that $H^0_{\mathrm{Tate}}(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. Hence by periodicity there is an isomorphism $H^2(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. It follows that $\mathrm{inv}_{\mathbb{Z}}$ is an isomorphism. □

2.9 Herbrand quotients

erbrand quotient **Definition 50.** Let G be a finite cyclic group and M a representation of G. Recall that there are isomorphisms $H^n_{\mathrm{Tate}}(G, M) \cong H^{n+2}_{\mathrm{Tate}}(G, M)$. We define the Herbrand quotient of M to be

$$h(G, M) = \frac{|H^0_{\mathrm{Tate}}(G, M)|}{|H^1_{\mathrm{Tate}}(G, M)|}.$$

If either of the two cohomology groups are infinite then $h(G, M)$ defaults to 0.

lem:herbrand Z **Example 51.** *If G is a cyclic group and $\mathbb{Z}$ has the trivial action of G then $h(G, \mathbb{Z}) = |G|$. This follow immediately 49*

lem:H2 cyclic Z

:herbrand finite

Lemma 52. *If M is finite then $h(G, M) = 1$.*

Proof. Let gen be a generator of G. Recall that $H^0_{\mathrm{Tate}}(G, M) \cong M^G/N_G M$. Also, we can write M^G as $\ker(1 - \mathrm{gen} : M \to M)$. Similarly $H^{-1}_{\mathrm{Tate}}(G, M)$ is isomorphic to $\ker(N_G : M \to M)/\mathrm{im}(1 - \mathrm{gen} : M \to M)$. The result follows because

$$\begin{aligned} |\ker(N_G : M \to M)| \cdot |\mathrm{im}(N_G : M \to M)| &= |M| \\ &= |\ker(1 - g : M \to M)| \cdot |\mathrm{im}(1 - g : M \to M)|. \end{aligned}$$

□

lem:herbrand ses

Lemma 53. *Suppose we have a short exact sequence of representations of a finite cyclic group G:*

$$0 \to A \to B \to C \to 0.$$

If two of the representations A, B, C has non-zero Herbrand quotient then so does the third, and $h(G, B) = h(G, A) \cdot h(G, C)$.

Proof. It follows from the long exact sequence that if two of the representations A, B, C have finite cohomology groups then so does the third. Also, by periodicity, the long exact sequence reduces to an exact hexagon:

$$\begin{array}{ccccc} & & H^0_{\mathrm{Tate}}(G, B) & & \\ & \nearrow & & \searrow & \\ H^0_{\mathrm{Tate}}(G, A) & & & & H^0_{\mathrm{Tate}}(G, C) \\ \uparrow & & & & \downarrow \\ H^1_{\mathrm{Tate}}(G, C) & & & & H^1_{\mathrm{Tate}}(G, A) \\ & \nwarrow & & \swarrow & \\ & & H^1_{\mathrm{Tate}}(G, B) & & \end{array}.$$

The result follows because the alternating product of the finite group orders in the hexagon is 1. □

2.10 The Triviality Criterion

Recall that a representation M of a group G has trivial cohomology if for all subgroups H of G and all $n \in \mathbb{N}$, the cohomology groups $H^{n+1}(H, M)$ are zero.

iterion solvable

Theorem 54. *Let M be a representation of a finite solvable group G. Suppose we have positive natural numbers e and o with e even and o odd, such that for all subgroups S of G we have*

$$H^e(S, M) \cong 0, \qquad H^o(S, M) \cong 0.$$

Then M has trivial cohomology.

Proof. We must prove that $H^n(S, M) = 0$ for all S and all $n > 0$. We'll prove this by induction on S. The result is true for the trivial subgroup of G. Assume that the result is true for S, and assume that S'/S is cyclic. The inductive hypothesis implies that (for all n) the inflation restriction sequence is exact:

$$0 \to H^n(S'/S, M^S) \to H^n(S', M) \to H^n(S, M) = 0.$$

We therefore have isomorphisms $H^n(S'/S, M^S) \cong H^n(S', M)$. In particular we have $H^e(S'/S, M^S) \cong 0$ and $H^o(S'/S, M^S) \cong 0$. Using periodicity of the cohomology of a cyclic group, we have $H^n(S'/S, M^S) \cong 0$ for all $n > 0$. □

iality criterion

Theorem 55. *Let M be a representation of a finite group G (no longer assumed to be solvable). Suppose we have positive natural numbers e and o with e even and o odd, such that for all subgroups S of G we have*

$$H^e(S, M) = 0, \qquad H^o(S, M) = 0.$$

Then M has trivial cohomology.

Proof. Let S be a subgroup of G. Fix a prime number p and let S_p be a Sylow p-subgroup of S. Since S_p is solvable, thm:triviality criterion solvable 54 implies that $H^n(S_p, M) \cong 0$ for all $n > 0$. By cor:cohomology sub Sylow 45, it follows that $H^n(S, M)[p^\infty] \cong 0$. Since this holds for all primes p, cor:cohomology G-torsion 44 implies that $H^n(S, M) \cong 0$. □

ivial cohomology

Corollary 56. *If M is a representation of a finite group G and M has trivial cohomology then* $\mathrm{up}(M)$ *and* $\mathrm{down}(M)$ *have trivial cohomology.*

Proof. For each subgroup S of G we have

$$H^1(S, \mathrm{up}(M)) \cong H^2(S, M) \cong 0, \qquad H^2(S, \mathrm{up}(M)) \cong H^3(S, M) \cong 0.$$

By thm:triviality criterion 55 $\mathrm{up}(M)$ has trivial cohomology. Similarly

$$H^2(S, \mathrm{down}(M)) \cong H^1(S, M) \cong 0, \qquad H^3(S, \mathrm{up}(M)) \cong H^2(S, M) \cong 0,$$

so $\mathrm{down}(M)$ has trivial cohomology. □

Theorem 57. *Let M be a representation of a finite group G, and assume that M has trivial cohomology. Then M has trivial Tate cohomology.*

Proof. Fix an integer n and choose a natural number m such that $m+n > 0$. By cor:up and down trivial cohomology 56, $\mathrm{down}^m(M)$ has trivial cohomology. Therefore

$$H^n_{\mathrm{Tate}}(H, M) \cong H^{n+m}(H, \mathrm{down}^m(M)) \cong 0.$$

□

2.11 The splitting module of a 2-cocycle

Let $\sigma \in H^2(G, M)$. In this section we describe a representation of G called the *splitting module of σ*.

We shall write σ' for an inhomogeneous 2-cocycle representing σ. This means $\sigma' : G \times G \to M$ satisfies the following 2-cocycle relation for all $x, y, z \in G$

$$\sigma'(x, y) + \sigma'(xy, z) = \sigma'(x, yz) + x \bullet \sigma'(y, z). \tag{2.2}$$

def:2-cocycle re

splitting module

Definition 58. The splitting module of σ' is the R-module $M \times \mathrm{aug}(R, G)$, with the action of an element $g \in G$ given by

$$g \bullet (m, f) = \left(g \bullet m + \sum_{x \in G} f(x)\sigma'(g, x), g \bullet f \right), \qquad m \in M,\ f \in \mathrm{aug}(R, G).$$

(Although we don't need this fact right now, it's worth knowing that up to isomorphism, the splitting module depends only on the cohomology class σ. For this reason, we'll write $\mathrm{split}(\sigma)$ for this representation).

There is evidently a short exact sequence of representations of G.

$$0 \to M \to \mathrm{split}(\sigma) \to \mathrm{aug}(R, G) \to 0. \tag{2.3}$$

eq:split ses

splitting module

Lemma 59. *The image of σ in $H^2(G, \mathrm{split}(\sigma))$ is zero.*

Proof. We can check that the cocycle σ' is the coboundary of the 1-cochain $\tau : G \to \mathrm{split}(\sigma)$ defined by

$$\tau(x) = (x \bullet \sigma'(1,1), [x] - [1])$$

(Here we are using the notation $[x]$ to mean the function with value 1 at x and 0 elsewhere).

By definition we have

$$\begin{aligned} d\tau(x,y) &= \tau(x) + x \bullet \tau(y) - \tau(xy) \\ &= (x \bullet \sigma'(1,1), [x] - [1]) + x \bullet (y \bullet \sigma'(1,1), [y] - [1]) - (xy \bullet \sigma'(1,1), [xy] - [1]) \\ &= (x \bullet \sigma'(1,1), [x] - [1]) + (xy \bullet \sigma'(1,1) + \sigma'(x,y) - \sigma'(x,1), [xy] - [x]) - (xy \bullet \sigma'(1,1), [xy] - [1]) \\ &= (x \bullet \sigma'(1,1) + \sigma'(x,y) - \sigma'(x,1), 0). \end{aligned}$$

It remains to prove that $\sigma'(x,1) = x \bullet \sigma'(1,1)$. This follows from the 2-cocycle relation def:2-cocycle relation 2.2 in the case $y = z = 1$. □

2.12 The Reciprocity Isomorphism

undamental class

Definition 60. In this section G is a finite group; M is a representation of G over a commutative ring R. We shall call M a *finite class formation* if:

- The ring R has no additive torsion. This implies

$$H^2(G, \mathrm{aug}(R, G)) \cong H^1(G, R) \cong \mathrm{Hom}(G, R) = 0.$$

Assume also that the representation M satisfies the following conditions for all subgroups S of G:

- For all subgroups $S \leq G$ we have $H^1(S, M) \cong 0$.
- For all subgroups $S \leq G$, $H^2(S, M)$ is isomorphic as an R-module to $R/|S| \cdot R$.

If M is a finite class formation then a generator σ for $H^2(G, M)$ is called a *fundamental class.*

In this section we'll show that if M is a finite class formation over the ring $\mathbb{Z}$ then there is an isomorphism (called the *reciprocity isomorphism*)

$$G^{\mathrm{ab}} \cong H^0_{\mathrm{Tate}}(G, M).$$

The reciprocity isomorphism depends on the choice of a fundamental class.

Example 61. *If G is a finite cyclic group then the trivial representation $\mathbb{Z}$ is a finite class formation. This follows from* lem:H2 cyclic Z *49. The cocycle σ_1 defined in* lem:H2 cyclic Z *49 is a fundamental class.*

ve of surjective

Lemma 62. *Let I be an ideal of a commutative ring R and let $f : R/I \to R/I$ be a surjective R-linear map. Then f is injective.*

Proof. Without loss of generality $I = 0$, since such a map is also R/I-linear. Let $c \in R$ be a preimage of 1 and let $d = f(1)$. We have $cd = cf(1) = f(c) = 1$. The map f is given by $f(x) = dx$ and the map $x \mapsto cx$ is an inverse. □

class generates

Lemma 63. *Let $\sigma \in H^2(G, M)$ be a fundamental class. Then the restriction of σ to any subgroup S of G is a generator for $H^2(S, M)$.*

Proof. The restriction and corestriction maps are R-linear maps

$$H^2(G, M) \overset{\text{rest}}{\to} H^2(S, M) \overset{\text{cor}}{\to} H^2(G, M).$$

We need to prove that the restriction map is surjective. By the conditions on M, we can think of these maps as

$$R/|G| \to R/|S| \to R/|G|.$$

Since R has no additive torsion, the image of $R/|S|$ in $R/|G|$ is contained in the S-torsion, which is $[G : S]R/|G|$. Furthermore, since the composition is $[G : S]$, it follows that the image of cor is contains $[G : S]R/|G|$. Therefore the image of cor is precisely $[G : S]R/|G|$, which is isomorphic to $R/|S|$. Hence cor may be regarded as a surjective linear map $R/|S| \to R/|S|$. By 62, cor is injective with image $[G : S]H^2(G, M)$.

lem:linear injective of surject

Now let $b \in H^2(S, M)$. We have $\text{cor}(b) = [G : S]c$ for some $c \in H^2(G, M)$. This implies $\text{cor}(b) = \text{cor}(\text{rest}(c))$, and since cor is injective we have $b = \text{rest}(c)$. □

g module trivial

Theorem 64. *Let $\sigma \in H^2(G, M)$ be a fundamental class. Then* $\text{split}(\sigma)$ *has trivial cohomology.*

Proof. By 55, it's enough to prove for every subgroup S of G that $H^1(S, \text{split}(\sigma)) \cong 0$ and $H^2(H, \text{split}(\sigma)) \cong 0$. We have a long exact sequence with the following terms:

thm:triviality criterion

$$0 \to H^1(S, \text{split}(\sigma)) \to H^1(S, \text{aug}(R, G)) \to H^2(S, M) \to H^2(S, \text{split}(\sigma)) \to 0.$$

By 63 and 59, the map $H^2(S, M) \to H^2(S, \text{split}(\sigma))$ is zero. In particular $H^2(S, \text{split}(\sigma)) \cong 0$. The R-modules $H^1(S, \text{aug}(R, G))$ and $H^2(S, M)$ are both isomorphic to $R/|S|R$, and the map from one to the other is surjective. By 62, the map from $H^1(S, \text{aug}(R, G))$ to $H^2(S, M)$ is also injective. Therefore $H^1(S, \text{split}(\sigma)) = 0$. □

lem:rest in fund split class gen

lem:linear injective of surjective

:reciprocity iso

Definition 65. The theorem implies that we have isomorphisms for all $n \in \mathbb{Z}$ (which depend of σ):

$$H^n_{\text{Tate}}(G, \text{aug}(R, G)) \cong H^{n+1}_{\text{Tate}}(G, M).$$

In particular in the case $n = -1$, $R = \mathbb{Z}$ we have the reciprocity isomorphism

$$\begin{array}{ccccc} G^{\text{ab}} & \cong & H^{-1}_{\text{Tate}}(G, \text{aug}(\mathbb{Z}, G)) & \cong & H^0_{\text{Tate}}(G, M), \\ g & \mapsto & [g] - [1] & \mapsto & \delta([g] - [1]) \end{array}.$$

Here δ is the connecting map for the short exact sequence 2.3.

eq:split ses

We shall finish off this chapter by giving a formula for the reciprocity isomorphism in terms of a cocycle σ' representing the fundamental class σ.

iprocity formula

Lemma 66. *The reciprocity isomorphism for a fundamental class $\sigma \in H^2(G, M)$ is given by*

$$\text{reciprocity}(g) \equiv \sum_{x \in G} \sigma'(g, g) \bmod N_G M.$$

This depends only on the cohomology class σ rather than the cocycle σ'.

Proof. We have a diagram with exact rows. Note that $C^0(G,M)$ and $C^{-1}(G,M)$ are both M and the vertical maps are Tate coboundary maps, which are N_G.

$$\begin{array}{ccccccccc} 0 \to & C^{-1}(G,M) & \to & C^{-1}(G,\mathrm{split}(\sigma)) & \to & C^{-1}(G,\mathrm{aug}(R,G)) & \to 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \to & C^{0}(G,M) & \to & C^{0}(G,\mathrm{split}(\sigma)) & \to & C^{0}(G,\mathrm{aug}(R,G)) & \to 0 \end{array}$$

Choose an element $g \in G$. Recall that this element corresponds to the element $[g]-[1] \in C^{-1}(G,\mathrm{aug}(\mathbb{Z},G))$. An obvious pre-image off this element in $C^{-1}(G,\mathrm{split}(\sigma))$ is the element $(0,[g]-[1])$. The image of $(0,[g]-[1])$ in $C^0(G,\mathrm{split}(\sigma))$ is

$$N_G(0,[g]-[1]) = \left(\sum_{x\in G}(\sigma'(x,g)-\sigma'(x,1)),0\right).$$

By the cocycle relation we have $\sigma'(x,1)=\sigma'(1,1)$ for all $x \in G$. Hence the reciprocity map takes $g \in G$ to the element

$$\sum_{x\in G}\sigma'(x,g) - |G|\sigma'(1,1) \in M^G/N_G M.$$

Since every element of $H^\bullet_{\mathrm{Tate}}(G,-)$ is killed by $|G|$, this formula simplifies to

$$\mathrm{reciprocity}(g) = \sum_{x\in G}\sigma'(x,g).$$

If we modify σ' by a coboundary $d\tau$:

$$\sigma''(x,y) = \sigma'(x,y) + x\tau(y) - \tau(xy) + \tau(x),$$

then we will add the folowing term to reciprocity(g):

$$\sum_{x\in G}(x\tau(g) - \tau(xg) + \tau(x)).$$

This sum simplifies to $N_G(\tau(g))$, which is zero in $H^0_{\mathrm{Tate}}(G,M)$. □

2.13 The invariant map

For simplicity we shall work over the ring $R=\mathbb{Z}$ from now on.

Suppose S is a subgroup of G and M is a finite class formation with fundamental class σ_G. It follows immediately that $M \downarrow S$ is also a finite class formation with fundamental class $\sigma_S := \sigma_G|S$. Similarly we have :

class formation

Lemma 67. *Let S be a normal subgroup of G and let M be a class formation for G. Then M^S is a finite class formation for G/S. Furthermore there is a unique fundamental class $\sigma_{G/S} \in H^2(G/S, M^S)$ such that* $\inf(\sigma_{G/S}) = [G:S]\cdot\sigma_G$.

Proof. Consider the inflation restriction sequence:

$$0 \to H^2(G/S, M^S) \to H^2(G,M) \to H^2(S,M)$$

The result follows since the restriction map $H^2(G,M) \to H^2(S,M)$ is a surjective map from $\mathbb{Z}/|G|\cdot\mathbb{Z}$ to $\mathbb{Z}/|S|\cdot\mathbb{Z}$. □

In practice, the following is a more convenient definition of a finite class formation.

Definition 68. For all subgroups $S \leq T \leq G$ with S normal in T, there is an element $\sigma_{T/S} \in H^2(T/S, M^S)$ with the following properties:

- $\inf(\sigma_{T/S}) = [T : S] \cdot \sigma_T$,
- $\sigma_T = \mathrm{rest}\sigma_G$.

Given a class formation with fundamental classes $\sigma_{T/S}$ we define an invariant map

$$\mathrm{inv}_{T/S} : H^2(T/S, M^S) \to \mathbb{Q}/\mathbb{Z}, \qquad \sigma_{T/S} \mapsto \frac{1}{[T : S]}.$$

on compatibility **Lemma 69.** *Let $S \leq T$ be a normal subgroup. then we have*

$$\mathrm{inv}_{T/S}(\sigma) = \mathrm{inv}_{T/1}(\mathrm{infl}(\sigma)).$$

on compatibility **Lemma 70.** *Let $S \leq T \leq U \leq G$ be with S normal in U. then we have*

$$\mathrm{inv}_{U/S}(\mathrm{rest}(\sigma)) = [U : T] \cdot \mathrm{inv}_{T/S}(\sigma).$$

Chapter 3

Local Class Field Theory

In this chapter we shall consider finite Galois extensions of local fields l/k. We shall regard the multiplicative group $l^\times$ as a representation of $\mathrm{Gal}(l/k)$, where addition in the module is the operation which is usually written as multiplication. We shall always write $H^\bullet(l/k,-)$ as an abbreviation of $H^\bullet(\mathrm{Gal}(l/k),-)$. By the fundamental theorem of Galois theory we have

$$H^0(l/k,l^\times) = (l^\times)^G = l^\times.$$

The norm map $N_{\mathrm{Gal}(l/k)} : l^\times \to k^\times$ defined in def:norm 13 coincides with the usual norm map $N : l^\times \to k^\times$. This implies by lem:Tate cohomology is cohomology or homology 19 the isomorphism

$$H^0_{\mathrm{Tate}}(l/k,l^\times) \cong k^\times/N(l^\times).$$

We shall prove that $l^\times$ is a finite class formation and we shall construct a fundamental class $\sigma \in H^2(l/k,l^\times)$. This fundamental class gives a reciprocity isomorphism

$$\mathrm{Gal}(l/k)^{\mathrm{ab}} \cong k^\times/N(l^\times), \qquad g \mapsto \prod_{x\in\mathrm{Gal}(l/k)} \sigma(x,g).$$

In the case that l/k is unramified, the Galois group is generated by a Frobenius element F_k, and the reciprocity map satisfies (for any uniformizer π_k in k)

$$\mathrm{reciprocity}(F_k) = \pi_k N(l^\times).$$

The construction of this reciprocity isomorphism and its properties are known as *local class field theory*.

Recall that $l^\times$ is a finite class formation if for all subgroups $S \subset \mathrm{Gal}(l/k)$ we have isomorphisms:

$$H^1(S,l^\times) \cong 0, \qquad H^2(S,l^\times) \cong \mathbb{Z}/|S|\mathbb{Z}.$$

A more convenient to reformulation of this condition is the following. For all intermediate fields $l/m/k$ we have isomorphisms:

$$H^1(l/m,l^\times) \cong 0, \qquad H^2(l/m,l^\times) \cong \mathbb{Z}/[l:m]\mathbb{Z}.$$

The reason why this reformulation is so useful is because the base field k is no longer involved, so it's sufficient to prove the isomorphisms above for any Galois extension of local fields l/m (i.e. without considering any subgroups of the Galois group).

The proof that $l^\times$ is a clas formation is achieved in the following steps:

1. It is already proven in Mathlib that $H^1(l/k, l^\times) \cong 0$; this result is known as Hilbert's theorem 90. It remains to check that each $H^2(l/k, l^\times)$ is cyclic of order $[l : k]$, and to choose a generator.

2. In the case that l/k is cyclic, we can show that $|H^2(l/k, l^\times)| = [l : k]$ by Herbrand quotients. By inflation-restriction, this implies $|H^2(l/k, l^\times)| \leq [l : k]$ for all Galois extensions. Hence to prove that $l^\times$ is a class formation it's sufficient to find an element in $H^2(l/k, l^\times)$ of order $[l : k]$; such an element is a fundamental class.

3. Suppose l/k is unramified. In this case we have a decomposition:

$$l^\times \cong \mathcal{O}_l^\times \oplus \mathbb{Z}.$$

   The subrepresentation $\mathcal{O}_l^\times$ has trivial cohomology in this unramified case. Therefore for any intermediate field $l/m/k$ we have $H^\bullet(l/m, l^\times) \cong H^\bullet(l/m, \mathbb{Z})$. Since $\mathbb{Z}$ is a finite class formation over a cycic group, it follows that $l^\times$ is a finite class formation. The cocycle σ_1 defined in lem:H2 cyclic Z 49 is a fundamental class, where we use the Frobenius element as a generator.

4. Suppose l/k is a Galois extension which is not necessarily unramified. To define the fundamental class in this case, we let l'/k be the unramified extension with the same degree as l/k. We have already constructed the fundamental class $\sigma_1 \in H^2(l'/k, l'^\times)$. We let σ_2 be the inflation of σ_1 to $H^2(ll'/k, (ll')^\times)$. The extension ll'/l is unramified, so we already have an explicit isomorphism $H^2(ll'/l, (ll')^\times) \cong \mathbb{Z}/[ll' : l]$. Using this isomorphism, we can show that the restriction of σ_2 to $H^2(ll'/l, (ll')^\times)$ is zero. Hence by inflation restriction there there is a unique $\sigma \in H^2(l/k, l^\times)$ whose inflation is σ_2. It is then easy to check that σ is a fundamental class in $H^2(l/k, l^\times)$.

3.1 Notation and Preliminary results

The following result (called Hilbert's theorem 90) is already in Mathlib.

thm:hilbert 90

Theorem 71. *Let l/k be a finite Galois extension of fields. Then $H^1(l/k, l^\times) \cong 0$.*

ve field trivial

Theorem 72. *Let l/k be a finite Galois extension of fields. Then there is an isomorphism of* $\mathrm{Gal}(l/k)$*-representations:*

$$l \cong \mathrm{ind}_1(k).$$

In particular l has trivial cohomology as a representation of $\mathrm{Gal}(l/k)$*.*

Proof. Recall from Galois theory that there is a normal basis for l over k, i.e. a basis of the form

$$\{x \bullet b_0 : x \in \mathrm{Gal}(l/k)\}.$$

Define a map $\mathrm{ind}_1(k) \cong l$ by

$$\Phi(f : G \to_0 k) = \sum_{x \in \mathrm{Gal}(l/k)} f(x) \cdot x \bullet b_0.$$

The map Φ is clearly a linear bijection; we check that it commutes with the Galois action:

$$\Phi(g \bullet f) = \sum_x f(g^{-1}x) \cdot xb_0 = \sum_x f(x) \cdot (gx) \bullet b_0 = g \bullet \Phi(f).$$

□

3.2 The Herbrand quotient of $l^\times$

In this section we'll prove that for a cyclic extension l/k of local fields, $h(l/k, l^\times) = [l : k]$.

additive trivial

Lemma 73. *Let l/k be a Galois extension of local fields and let U be any neighbourhood of 0 in l. There is a Galois-invariant compact open subgroup $L \subseteq U$ which has trivial Tate cohomology.*

Proof. Let P be the maximal ideal of $\mathcal{O}_l$. Choose n such that $P^n \subseteq U$. Choose a normal basis for l over k contained in P^n and let L be the span of that basis over $\mathcal{O}_k$. We therefore have an isomorphism of Galois modules $L \cong \mathrm{ind}_1(\mathcal{O}_l)$, and induced representations have trivial Tate cohomology. □

ct open additive

Lemma 74. *Suppose l/k is a cyclic extension. Let $M \subset l$ be a compact open subrepresentation. Then $h(l/k, M) = 1$.*

Proof. Choose $L \subseteq M$ as in lemma lem:exists additive trivial 73. Since L has finite index in M we have $h(M) = h(L) = 1$. □

ocal isomorphism

Lemma 75. *There is a non-zero ideal $P^n \subset \mathcal{O}_l$ such that the exponential and logarithm maps give inverse isomorphisms*

$$(1 + P^n, \times) \cong (P^n, +).$$

This isomorphism commutes with the action of the Galois group.

Proof. Choose n large enough so that for all $r > 0$,

$$rn - v_l(r!) \geq n, \qquad rn - v_l(r!) \overset{r\to\infty}{\to} \infty.$$

Then $\exp(x)$ converges for all $x \in P^n$ to an element of $1 + P^n$ and $\log(1 + x)$ converges to an element of P^n. Hence both $\exp(\log(1+x))$ and $\log(\exp(x))$ converge. The identities $\exp(\log(1 + x)) = 1 + x$ etc. follow by observing that they are true as an equations of power series □

rand local units

Lemma 76. *If l/k is a cyclic extension, then $h(l/k, \mathcal{O}_l^\times) = 1$.*

Proof. Choose a subgroup $1 + P^n$ as in the lem:local isomorphism 75. Since $\mathcal{O}_l^\times/(1 + P^n)$ is finite we have

$$h(\mathcal{O}_l^\times) = h(1 + P^n) = h(P^n).$$

The right hand side is 1 by lem:herbrand compact open additive 74. □

erbrand local l*

Lemma 77. *If l/k is a cyclic extension of local fields then $h(l/k, l^\times) = [l : k]$.*

Proof. We have a short exact sequence of representations

$$0 \to \mathcal{O}_l^\times \to l^\times \to \mathbb{Z} \to 0,$$

where the second map is the valuation. We've shown in lem:herbrand local Z units 76, lem:herbrand local l units 51 that $h(l/k, \mathcal{O}^\times) = 1$ and $h(l/k, \mathbb{Z}) = [l : k]$. Therefore $h(l/k, l^\times) = [l : k]$. □

lem:local H2 l*

Lemma 78. *If l/k is a cyclic extension of local fields then $|H^2(l/k, l^\times)| = [l : k]$.*

Proof. The follows from lem:herbrand tate local 77 and lem:tate local 71. □

3.3 An upper bound for $H^2(l/k, l^\times)$

l H2 upper bound

Theorem 79. *Let l/k be a Galois extenion of local fields. Then $|H^2(l/k, l^\times)| \leq [l : k]$.*

Proof. Let p be prime number dividing the degree $[l : k]$ and let k_p be the fixed field of a Sylow p-subgroup S_p of $\mathrm{Gal}(l/k)$. By cor:cohomology sub Sylow 45 it is sufficient to prove that $|H^2(l/k_p, l^\times)| \leq [l : k_p]$, which is a special case of the theorem. In the special case, the Galois group is S_p, which is a solvable group. It is therefore sufficient to prove the theorem in the case that $\mathrm{Gal}(l/k)$ is solvable. (Note that $\mathrm{Gal}(l/k)$ is always solvable if l/k is an extension of local fields, but we do not need to prve this.)

We shall prove the theorem by induction on k, starting with $k = l$ and moving down in cyclic steps. Assume the result for l/k and let k_0 be a subfield of k with k/k_0 cyclic. It follows from thm:hilbert 90 71 that we have an inflation-restriction sequence in dimension 2:

$$0 \to H^2(k/k_0, k^\times) \to H^2(l/k_0, l^\times) \to H^2(l/k, l^\times).$$

The first term has order $[k : k_0]$ by lem:local H2 l* 78, and the last term has order at most $[l : k]$ by the inductive hypothesis. Thereofore $H^2(l/k_0, l^\times)$ has order at most $[l : k] \times [k : k_0] = [l : k_0]$. □

3.4 Fundamental classes in unramified extensions

In this section we assume that l/k is unramified. In this case $\mathrm{Gal}(l/k)$ may be identified with $\mathrm{Gal}(\mathbb{F}_l/\mathbb{F}_k)$ where $\mathbb{F}_l$ and $\mathbb{F}_k$ are the residue class fields of l and k respectively. This group is cyclic and is generated by the Frobenius element F_k. If we choose a uniformizer π_k in k (i.e. a generator for the maximal ideal in $\mathcal{O}_k$) then π_k is also a uniformizer in l, so we may identify $\mathbb{F}_l$ with $\mathcal{O}_l/\pi_k\mathcal{O}_l$.

te field trivial

Lemma 80. *The Galois modules $\mathbb{F}_l$ and $\mathbb{F}_l^\times$ have trivial cohomology.*

Proof. By periodicity, it's suffient to prove that H^1 and H^2 are trivial. Also, since $\mathbb{F}_l$ and $\mathbb{F}_l^\times$ are finite, they both have Herbrand quotient 1, so it's enough to prove that H^1 is trivial. This follows from thm:hilbert 90 71 and thm:additive field trivial 72. □

additive trivial

Lemma 81. *If l/k is unramified then there is a normal basis for $\mathcal{O}_l$ over $\mathcal{O}_k$. Hence there is an isomorphism of Galois representations $\mathcal{O}_l \cong \mathrm{ind}_1\mathcal{O}_k$. In particular $\mathcal{O}_l$ has trivial cohomology.*

Proof. By thm:additive field trivial 72 we may choose $x_0 \in \mathbb{F}_l$ such that $\{g \bullet x_0 : g \in \mathrm{Gal}(l/k)\}$ is a normal basis. Let $y \in \mathcal{O}_l$ be a lift of x_0. We claim that $\{g \bullet y\}$ is a normal basis in $\mathcal{O}_l$. It's sufficient to show that these vectors span $\mathcal{O}_l$ over $\mathcal{O}_k$. Choose any $z \in \mathcal{O}_l$. By assumption we may solve the congruence

$$z \equiv \sum \lambda_{g,0} gy \mod \pi_k. \qquad (\lambda_{g,0} \in \mathcal{O}_k).$$

Similarly we may solve the congruence

$$(z - \sum \lambda_{g,0} gy)/\pi_k \equiv \sum \lambda_{g,1} gy \mod \pi_k. \qquad (\lambda_{g,1} \in \mathcal{O}_k).$$

This implies

$$z \equiv \sum (\lambda_{g,0} + \lambda_{g,1}\pi_k) gy \mod \pi_k^2.$$

etc. Proceeding in this way, we construct convergent series $\lambda_g = \sum \lambda_{g,r}\pi_k^r \in \mathcal{O}_k$, such that $z = \sum_g \lambda_g y$. □

ed units trivial

Lemma 82. *If l/k is unramified then $\mathcal{O}_l^\times$ has trivial cohomology.*

Proof. Recall (lem:local_isomorphism 75) that for n sufficiently large we have isomorphisms of Galois modules:

$$1 + P^n \cong P^n \cong \mathcal{O}_l,$$

where the first map is the logarithm and the second map is multiplication by π_k^{-n}. Hence by lem:unramified_additive 81, the multiplictive subgroup $1 + P^n$ has trivial cohomology. The long exact sequence now gives isomorphisms

$$H^r(l/k, \mathcal{O}_l^\times) \cong H^r(l/k, \mathcal{O}_l^\times/(1 + P^n)).$$

We'll prove by induction on n that $\mathcal{O}_l^\times/(1 + P^n)$ has trivial cohomology. In the case $n = 1$ we have

$$\mathcal{O}_l^\times/(1 + P) \cong \mathbb{F}_l^\times.$$

In this case the result follows from lem:finite_field_trivial 80.

For the inductive step we note that there is a short exact sequence of Galois modules

$$0 \to \mathbb{F}_l \to \mathcal{O}_l^\times/(1 + P^{n+1}) \to \mathcal{O}_l^\times/(1 + P^n) \to 0,$$

where we have identified P^n/P^{n+1} with $\mathbb{F}_l$. By the inductive hypothesis, we assume that $\mathcal{O}_l^\times/(1+P^n)$ has tivial cohomology. By lem:finite_field_trivial 80 $\mathbb{F}_l$ has trivial cohomology. Hence by the long exact seqeunce, $\mathcal{O}_l^\times/(1 + P^{n+1})$ has trivial cohomology. □

iso cohomology Z

Corollary 83. *Let l/k be an unramified extension of local fields. Then there are isomorphisms*

$$H^\bullet_{\text{Tate}}(l/k, l^\times) \cong H^\bullet_{\text{Tate}}(l/k, \mathbb{Z})$$

defined by the valuation map $v : l^\times \to \mathbb{Z}$. The inverse map is defined by $n \mapsto \pi_k^n$, and does not depend on the choice of π_k.

Proof. This follows from the long exact sequence using lem:unramified_units_trivial 82. □

undamental class

Lemma 84. *Let l/k be an unramified cyclic extension of local fields. Then $H^2(l/k, l^\times)$ is cyclic of order $[l : k]$. It is generated by the cohomology class of the following cocycle*

$$\sigma_{l/k}(F_k^r, F_k^s) = \begin{cases} 1 & r + s < [l : k], \\ \pi_k & r + s \geq [l : k]. \end{cases}$$

Here F_k is the Frobenius element generating $\text{Gal}(l/k)$ and r and s are chosen to be integers in the range $0 \leq r, s < [l : k]$. It follows that l/k is a finite class formation and $\sigma_{l/k}$ is a fundamental class.

Proof. This follows from the previous result cor:cohomology_unramified_iso_cohomology_Z 83 together with the description of $H^2(l/k, \mathbb{Z})$ in lem:H2_cyclic_Z 49. □

We therefore have a reciprocity isomorphism $\text{Gal}(l/k) \cong k^\times/N(l^\times)$.

Lemma 85. *Let l/k be an unramified extension of local fields and let F_k be the Frobenius element in $\text{Gal}(l/k)$. Let π_k be a uniformizer of k. Then we have*

$$\text{reciprocity}(F_k) = \pi_k,$$

where the reciprocity map is defined by the fundamental class $\sigma_{l/k}$.

By lem:H2 cyclic Z 49 we have an isomorphim $H^2(l/k, l^\times) \cong \mathbb{Z}/[l:k]\cdot\mathbb{Z}$ defined by

$$\mathrm{inv}_{l/k}(\sigma) = \sum_{i=1}^{[l:k]} v_k(\sigma(F_k^i, F_k)).$$

The class $\sigma_{l/k}$ maps to $1 \in \mathbb{Z}/n\mathbb{Z}$.

Lemma 86. *Let $m/l/k$ be an unramified tower of extensions of local fields Then the restriction to m/l of $\sigma_{m/k}$ is $\sigma_{m/l}$.*

Proof. Up to cohomology, $\sigma_{l/k}$ does not depend on the choice of uniformizer, so we may assume $\pi_k = \pi_l$ in our definitions of $\sigma_{m/k}$ and $\sigma_{m/l}$. We have $F_l = F_k^f$ where $f = [l:k]$. Hence

$$\begin{aligned}
\sigma_{m/k}(F_l^r, F_l^s) &= \sigma_{m/k}(F_k^{fr}, F_k^{fs}) \\
&= \begin{cases} 1 & fr + rs < [m:k] \\ \pi_k & fr + fs \geq [m:k] \end{cases} \\
&= \begin{cases} 1 & r + s < [m:l] \\ \pi_k & r + s \geq [m:l] \end{cases} \\
&= \sigma_{m/l}(F_l^r, F_l^s).
\end{aligned}$$

□

3.5 Construction of fundamental classes

Now let l/k be a Galois extension of local fields of degree n and let l' be the unramified extension of the same degree. We shall let m be the field generated by l and l'. Let e and f be the ramification index and inertia degree of l/k. Then we have $[m:l] = e$, $v_l(\pi_k) = e$. We shall write F_l for the Frobenius element in $\mathrm{Gal}(l/m)$, which we regard as a subgroup of $\mathrm{Gal}(m/k)$. We also write F_k for the Frobenius element in l'/k. With this notation we have:

$$F_l|l' = F_k^f.$$

We have a class $\sigma_{l'/k} \in H^2(l'/k, l'^\times)$, and by inflation we can regard $\sigma_{l'/k}$ as an element of $H^2(m/k, m^\times)$. Let $\psi \in H^2(m/k, m^\times)$ be the inflation of $\sigma_{l/k}$. Since the imflation map is injectove, ψ has order exactly $[l:k]$. We also have an inflation restriction sequence

$$0 \to H^2(l/k, l^\times) \to H^2(m/k, m^\times) \to H^2(m/l, m^\times)$$

We'll calculate the restriction of ψ to $H^2(m/l, m^\times)$. Since m/l is unramified, we have an isomorphism

$$\mathrm{inv}_{m/l} : H^2(m/l, m^\times) \cong \mathbb{Z}/e.$$

We have

$$\begin{aligned}\mathrm{inv}_{m/l}(\psi) &= \sum_{i=0}^{e-1} v_l(\psi(F_l^i, F_l)) \\ &= \sum_{i=0}^{e-1} v_l(\sigma_{l'/k}((F_l|l')^i, F_l|l')) \\ &= \sum_{i=0}^{e-1} v_l(\sigma_{l'/k}(F_k^{if}, F_k^f)) \\ &= v_l(\pi_k) = e \equiv 0 \bmod [m:l].\end{aligned}$$

The first line above is the definition of $\mathrm{inv}_{m/l}$. The second line is the definition of inflation of cocycles. The calculation above shows that the image of ψ in $H^2(m/l, m^\times)$ is 0. Therefore ψ is the inflation of a unique element $\sigma_{l/k} \in H^2(l/k, l^\times)$. Since the inflation map is injective $\sigma_{l/k}$ also has order $[l:k]$. We have proved the following.

H2 local cyclic

Theorem 87. *For every finite Galois extension l/k of local fields, $H^2(l/k, l^\times)$ is a cyclic group of order $[l:k]$ generated by $\sigma_{l/k}$. In particular $l^\times$ is a class formation and $\sigma_{l/k}$ is a fundamental class. Corresponding the $\sigma_{l/k}$ there is a reciprocity isomorphism*

$$\mathrm{Gal}(l/k) \cong k^\times / N(l^\times).$$

3.6 Compatibility in towers

Let $l/m/k$ be a tower of finite Galois extensions of local fields. Then we have

$$N_{l/k}(l^\times) = N_{m/k}(N_{l/m}(l^\times)) \subseteq N_{m/k}(m^\times).$$

Hence there is a projection map

$$k^\times / N(l^\times) \to k^\times / N(m^\times).$$

Also, $\mathrm{Gal}(m/k)$ is a quotient group of $\mathrm{Gal}(l/k)$ to we have a projection map

$$\mathrm{Gal}(l/k)^{\mathrm{ab}} \to \mathrm{Gal}(m/k)^{\mathrm{ab}}.$$

bility in towers

Lemma 88. *The following square commutes:*

$$\begin{array}{ccc} \mathrm{Gal}(l/k)^{\mathrm{ab}} & \cong & k^\times / N(l^\times) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(l/k)^{\mathrm{ab}} & \cong & k^\times / N(l^\times) \end{array}$$

Proof. □

norm limitation

Theorem 89. *Let l/k be a finite Galois extension of local fields and let l^{ab} be the maximal subfield of l which is an abelian extsion of k, i.e. the fixed field of the commutator subgroup of* $\mathrm{Gal}(l/k)$. *Then $N_{l/k}(l^\times) = N_{l^{\mathrm{ab}}/k}(l^{\mathrm{ab}\times})$.*

bility in towers

Proof. This follows from because the projection $\mathrm{Gal}(l/k)^{\mathrm{ab}} \to \mathrm{Gal}(l^{\mathrm{ab}}/k)^{\mathrm{ab}}$ is an isomorphism. □

n classification

Theorem 90. *Let l_1 and l_2 be two abelian extensions of k contained in a field m. Then $l_1 \subseteq l_2$ if and only if $N_{l_1/k}(l_1^\times) \supseteq N_{l_2/k}(l_2^\times)$ and $l_1 = l_2$ if and only if $N_{l_1/k}(l_1^\times) = N_{l_2/k}(l_2^\times)$.*

Example 91. *Let l/k be an unramified extension of local field of degree f. Then $N(l^\times) = \pi_k^f \times \mathcal{O}_k^\times$.*

Proof. We have calculated the reciprocity map in this case. □

Lemma 92. *Let m_1 and m_2 be two intermediate fields between k and l such that $l = m_1 m_2$. Then we have*

$$N_{l/k}(l^\times) = N_{m_1/k}(m_1^\times) \cap N_{m_2/k}(m_2^\times).$$

Example 93. *Let $l = \mathbb{Q}_p(\zeta)$ where ζ is a primitive p^n-th root of unity for some $n > 0$. Then $N(l^\times) = p^{\mathbb{Z}} \times (1 + p^n\mathbb{Z}_p)$.*

Proof. By Eisenstein's criterion, the cyclotimic polynomial $\Phi_{p^n}(X) = \frac{X^{p^n}-1}{X^{p^{n-1}}-1}$ is irreducible over $\mathbb{Q}_p$. Hence the degree of the extension is $\phi(p^n) = p^n - p^{n-1}$. This coincides with the index:

$$\begin{aligned}[\mathbb{Q}_p^\times : p^{\mathbb{Z}} \times (1 + p^n\mathbb{Z}_p)] &= [\mathbb{Z}_p^\times : (1 + p^n\mathbb{Z}_p)] \\ &= |(\mathbb{Z}/p^n\mathbb{Z})^\times|.\end{aligned}$$

We have $p = N(1 - \zeta)$. It is therefore sufficient to show that every $x \in 1 + p^n\mathbb{Z}_p$ is the norm of an element of $\mathbb{Z}_p[\zeta]$. We split this into cases.

- Suppose p is an odd prime, so that $\exp(pz)$ converges for all $z \in \mathbb{Z}_p$. If $a \in 1 + p^n\mathbb{Z}_p^\times$ then there is an expression of a of the form

  $$a = \exp(p^n y), \qquad y \in \mathbb{Z}_p.$$

  It follows that

  $$a = \exp(p\frac{y}{p-1})^{[\mathbb{Q}(\zeta):\mathbb{Q}_p]}.$$

  In particular, $x \in N(\mathbb{Q}_p(\zeta)^\times)$.

- In the case $p^n = 2$ we have $l = \mathbb{Q}_p$, so every element of $\mathbb{Q}_p$ is a norm.

- In the case $p = 2$, $n \geq 2$, there is an intermediate field $l/\mathbb{Q}_p(i)/\mathbb{Q}_p$, and we have

  $$N_{\mathbb{Q}_p(i)/\mathbb{Q}_p}(x + iy) = x^2 + y^2.$$

  It's easy to show (for example using Hensel's lemma) that if $a \equiv 1 \bmod 4$ then a is the norm of an element of $\mathbb{Q}_p(i)$. If $a \in 1 + 2^n\mathbb{Z}_2$ then we have for some $b \in \mathbb{Z}_2$:

  $$a = \exp(2^n b) = \exp(4b)^{[l:\mathbb{Q}(i)]}.$$

  The the exponential above converges to an element of $1 + 4\mathbb{Z}_2$. In particular there is an element $b \in \mathbb{Q}_2(i)$ such that

  $$a = N_{\mathbb{Q}_p(i)/\mathbb{Q}_p}(b)^{[l:\mathbb{Q}_p(i)]} = N_{l/\mathbb{Q}_p}(b)$$

□

Kronecker Weber

Theorem 94. *Let $l/\mathbb{Q}_p$ be a finite abelian extension. Then l is (isomorphic to) a subfield of a cyclotomic extension.*

Proof. The subgroup $N_{l/\mathbb{Q}_p}(l^\times)$ is open in $\mathbb{Q}_p^\times$, so it must contain a subgroup of the form $1+p^n\mathbb{Z}_p$ for some n. Let f be the order of p in $\mathbb{Q}_p^\times/N(l^\times)$.

$$N(l^\times) \supset p^{f\mathbb{Z}} \times (1+p^n\mathbb{Z}_p).$$

□

Chapter 4

Global Class Field Theory

In this chapter we let l/k be a finite Galois extension of algebraic number fields. We shall consider the idele class group $\mathrm{Cl}_l = \mathbb{A}_l^\times / l^\times$ as a module for the Galois group $\mathrm{Gal}(l/k)$ and we shall describe the construction of fundamental classes in $H^2(l/k, \mathrm{Cl}_l)$. These classes give rise to a reciprocity isomorphism

$$\mathrm{Gal}(l/k)^{\mathrm{ab}} \cong \mathrm{Cl}_k / N(\mathrm{Cl}_l).$$

We would therefore like to prove for all intermediate fields $l/m/k$:

- $H^1(l/m, \mathrm{Cl}_l) = 0$,
- $H^2(l/m, \mathrm{Cl}_l)$ is cyclic of order $[l : m]$.

We note the following consequence of Hilbert's theorem 90:

class invariants

Lemma 95. *Let l/k be any Galois extension of number fields. The map $\mathrm{Cl}_k \to \mathrm{Cl}_l^{\mathrm{Gal}(l/k)}$ is an isomorphism.*

Proof. We have a short exact sequence

$$0 \to l^\times \to \mathbb{A}_l^\times \to \mathrm{Cl}_l \to 0.$$

Taking $\mathrm{Gal}(l/k)$-invariants gives a long exact sequence beginning with

$$0 \to k^\times \to \mathbb{A}_k^\times \to \mathrm{Cl}_l^{\mathrm{Gal}(l/k)} \to H^1(l/k, l^\times).$$

The last term is zero by thm:hilbert 90 71. This implies the result. □

By the lemma, we may regard $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ as the quotient $\mathrm{Cl}_k / N_{l/k}\mathrm{Cl}_l$. Furthmore, the inflation map for a tower of Galois extensions $l/m/k$ takes the form

$$H^\bullet(m/k, \mathrm{Cl}_m) \to H^\bullet(l/k, \mathrm{Cl}_l).$$

4.1 Choice of S

Let S be a finite set of places of k, containing all of the infinite primes and all of the primes which ramify in l. We shall use the notation

$$\mathbb{A}_{l,S} = \prod_{v \in S} \prod_{w|v} l_w \times \prod_{v \in S} \prod_{w|v} \mathcal{O}_v.$$

We also write $\mathcal{O}_{l,S}$ for the ring S-integers in l:

$$\mathcal{O}_{l,S} = \{x \in l, \forall v \notin S, \forall w|v, |x|_v \leq 1\} = k \cap \mathbb{A}_{l,S}.$$

We regard $\mathcal{O}_{l,S}$ as a subring of $\mathbb{A}_{l,S}$ and $\mathcal{O}_{l,S}^\times$ as a subgroup of $\mathbb{A}_{l,S}^\times$.

Note that the quotient $\mathbb{A}_l^\times/\mathbb{A}_{l,S}^\times$ is naturally isomorphic to the group of fractional ideals of $\mathcal{O}_{l,S}$. By adding more primes to S if necessary, we may assume that $\mathcal{O}_{k,S}$ and $\mathcal{O}_{l,S}$ are both principal ideal domains (that can be achieved by adding to S the primes P whose ideal classes generate the class groups of k and l). This implies

$$\mathbb{A}_l^\times = \mathbb{A}_{l,S}^\times l^\times, \qquad \mathbb{A}_k^\times = \mathbb{A}_{k,S}^\times k^\times,$$

and therefore

$$\mathrm{Cl}_l = \mathbb{A}_{l,S}^\times/\mathcal{O}_{l,S}^\times, \qquad \mathrm{Cl}_k = \mathbb{A}_{k,S}^\times/\mathcal{O}_{k,S}^\times.$$

The big advantage of working with $\mathbb{A}_{l,S}^\times$ and $\mathcal{O}_{l,S}$ instead of $\mathbb{A}_l^\times$ and $l^\times$ is that $\mathbb{A}_{l,S}^\times$ and $\mathcal{O}_{l,S}$ have well-defined Herbrand quotients, whereas the cohomology groups of $\mathbb{A}_l^\times$ and $l^\times$ are infinite.

4.2 The Herbrand quotient of the S-ideles

Let v be a place of k and $\hat{v}$ a place of l above v. We'll write $D_{\hat{v}}$ the decomposition group at $\hat{v}$.

Lemma 96. *Then there are isomorphisms*

$$\prod_{w|v} l_w^\times \cong \mathrm{coind}_{D_{\hat{v}}}^{\mathrm{Gal}(l/k)} l_{\hat{v}}^\times, \qquad \prod_{w|v} \mathcal{O}_w^\times \cong \mathrm{coind}_{D_{\hat{v}}}^{\mathrm{Gal}(l/k)} \mathcal{O}_{\hat{v}}^\times.$$

Proof. Define a map $\Phi : \prod_{w|v} l_w^\times \to (\mathrm{Gal}(l/k) \to l_{\hat{v}}^\times)$ by

$$\Phi(x_w) = (g \mapsto g \bullet x_{g^{-1}\hat{v}}).$$

Note that for $h \in D_{\hat{v}}$ we have

$$\Phi(x_w)(hg) = h \bullet (g x_{g^{-1}\hat{v}}) = h \bullet \Phi(x_w)(g).$$

Therefore $\Phi(x_w)$ is actually in the subspace $\mathrm{coind}_{D_v} l_{\hat{v}}$, and it's easy to check that Φ gives a group isomorphism $\prod_{w|v} l_w \cong \mathrm{coind}_{D_v} l_{\hat{v}}$. We'll check that this map intertwines the actions of G: Note that for $g \in G$, then element $g \bullet (x_w)$ has w-coordinate $g \bullet x_{g^{-1}\bullet w}$. This implies

$$\Phi(g \bullet (x_w))(h) = h \bullet (g \bullet x)_{h^{-1}\bullet\hat{v}} = hg \bullet x_{(hg)^{-1}\bullet\hat{v}} = \Phi(x_w)(hg).$$

The proof of the other isomorphism is similar. □

Lemma 97. *There are isomorphisms for all $n > 0$*

$$H^n(l/k, \mathbb{A}_{S,l}^\times) \cong \prod_{v \in S} H^n(l_{\hat{v}}/k_v, l_{\hat{v}}^\times).$$

Proof. We note that by the previous lemma we have

$$\mathbb{A}_{S,l}^\times \cong \prod_{v \in S} \mathrm{coind}_{D_{\hat{v}}} l_{\hat{v}}^\times \times \prod_{v \notin S} \mathrm{coind}_{D_{\hat{v}}} \mathcal{O}_{\hat{v}}^\times$$

By Shapiro's lemma we have

$$H^n(l/k, \mathbb{A}_{S,l}^\times) \cong \prod_{v \in S} H^n(l_{\hat{v}}/k_v, l_{\hat{v}}^\times) \times \prod_{v \notin S} H^n(l_{\hat{v}}/k_v, \mathcal{O}_{\hat{v}}^\times)$$

For $v \notin S$, the extension $l_{\hat{v}}/l_v$ is unramified, and we have proved in such cases that $\mathcal{O}_{\hat{v}}^\times$ has trivial cohomology. □

Lemma 98. *If l/k is a cyclic extension then we have*

$$h(l/k, \mathbb{A}_{S,l}^\times) = \prod_{v \in S} |D_{\hat{v}}|.$$

Proof. This follows from the previous lemma, and the calculation of Herbrand quotients for local fields. □

4.3 The Herbrand quotient of the S-units

Define the *logarithmic space* V_S to be the following finite dimensional vector space over the real numbers:

$$V_S = \prod_{v \in S} \prod_{w|v} \mathbb{R}.$$

We consider L_S as a representation of $\mathrm{Gal}(l/k)$, where the Galois action permutes the places w lying above each $v \in S$. As a Galois representation we have

$$V_S \cong \prod_{v \in S} \mathrm{ind}_{D_{\hat{v}}}^{\mathrm{Gal}(l/k)} \mathbb{R}.$$

Contained in V_S we have a lattice L_S consisting of vectors whose components are all in $\mathbb{Z}$. Here we are using the word "lattice" to mean the $\mathbb{Z}$-space of a basis for V_S. We have an isomorphism

$$L_S \cong \prod_{v \in S} \mathrm{ind}_{D_{\hat{v}}}^{\mathrm{Gal}(l/k)} \mathbb{Z}.$$

Lemma 99. *If l/k is a cyclic extension then $h(l/k, L_S) = \prod_{v \in S} |D_{\hat{v}}|$.*

Proof. This follows from Shapiro's lemma together with the calculation of the cohomology of a cyclic group with values in $\mathbb{Z}$. □

Lemma 100. *Let l/k be cyclic and let M be any Galois-invariant lattice in V_S. Then $h(l/k, M) = \prod_{v \in S} |D_{\hat{v}}|$*

Proof. The representations $M \otimes \mathbb{Q}$ and $L_S \otimes \mathbb{Q}$ have the same character (this is just the character of the representation V_S). Therefore the representations $M \otimes \mathbb{Q}$ and $L_S \otimes \mathbb{Q}$ are isomorphic. Hence M is isomorphic to subrepresentation of finite index in L_S, so thay have the same Herbrand quotient. □

The vector $(1, 1, \ldots, 1) \in V_S$ in fixed by all elements of $\mathrm{Gal}(l/k)$, so it spans a subrepresentation isomorphic to the trivial representation $\mathbb{Z}$. Recall the we have a logarithmic map

$$\log_S : \mathcal{O}_S^\times \to V_S,$$

where the w-component of $\log_S(x)$ is $\log |x|_w$. The kernel of $\log_S$ is the finite group of roots of unity in k.

let unit theorem

Theorem 101. $\log_S(\mathcal{O}_S^\times)$ *has zero intersection with* $\mathrm{Span}(1,1,\dots,1)$. *The direct sum of these subrepresentations is a lattice in* V_S.

Corollary 102. *Let* l/k *be a cyclic extension. Then*

$$h(l/k, \mathcal{O}_{l,S}^\times) = \frac{\prod_{v\in S} |D_{\hat{v}}|}{[l:k]}.$$

Proof. Since $\log_S$ has finite kernel, the Herbrand quotient of $\mathcal{O}_{l,S}^\times$ is equal to that of $\log_S(\mathcal{O}_S^\times)$. By Dirichlet's unit theorem, $\log_S(\mathcal{O}_S^\times) \oplus \mathbb{Z}$ is a lattice in V_S. We know the Herbrand quotient of $\log_S(\mathcal{O}_S^\times) \oplus \mathbb{Z}$ from the calculation above, and the Herbrand quotient of $\mathbb{Z}$ is $[l:k]$. □

Corollary 103. *If* l/k *is cyclic then* $h(\mathbb{A}_{l,S}^\times/\mathcal{O}_{l,S}^\times) = [l:k]$.

4.4 Dirichlet Density

irichlet density

Definition 104. Let M be a set of primes of $\mathcal{O}_k$. We'll say that M has a *Dirichlet density* $c \in \mathbb{R}$ if

$$\sum_{P\in M} N(P)^{-s} \overset{s\to 1+}{\sim} c \cdot \log\left(\frac{1}{s-1}\right)$$

where s tends to 1 through the real numbers $s > 1$.

Lemma 105. *Suppose* M_1 *and* M_2 *are disjoint sets of primes of* $\mathcal{O}_l$. *If two of the sets* $M_1, M_2, M_1 \cup M_2$ *have a Dirichlet density, then so does the third and we have*

$$\mathrm{density}(M_1 \cup M_2) = \mathrm{density}(M_1) + \mathrm{density}(M_2).$$

Proof. This is trivial. □

hlet density top

Lemma 106. *The set of all primes of* $\mathcal{O}_k$ *has Dirichlet density* 1.

Proof. Let P be a prime. We have

$$\left| N(P)^{-s} - \log\left(\frac{1}{1-N(P)^{-s}}\right)\right| \ll N(P)^{-2s}$$

Since $\sum N(P)^{-2s}$ is bounded in the region $s > 1$ (this follows from the convergence of the Dedekind zeta function), we have

$$\sum_P N(P)^{-s} \sim \sum_P \log\left(\frac{1}{1-N(P)^{-s}}\right) = \log \zeta_l(s),$$

where ζ_l is the Dedekind zeta function (`NumberField.dedekindZeta`). By the analytic class number formula (`NumberField.tendsto_sub_one_mul_dedekindZeta_nhdsGT`) there is a positive real number r such that

$$\zeta_l(s) = \frac{r}{s-1} + O(1) \qquad (s > 1).$$

This implies

$$\log(\zeta_l(s)) \sim \log\left(\frac{1}{s-1}\right).$$

□

nsity degree one

Lemma 107. *The set of primes of $\mathcal{O}_l$ of degree one has Dirichlet density* 1.

Proof. Let M be the set of primes of degree larger than one. It's sufficient to prove that M has Dirichlet density 0. We have

$$\sum_{P\in M} N(P)^{-s} = \sum_{n\in\mathbb{N}} A(n)n^{-s},$$

Where A is the number of primes of degree > 1 with norm n. Note that $A(n) \leq [l:\mathbb{Q}]$. Also $A(n) = 0$ unless $n = m^r$ for positive integer m and $1 \leq r \leq [l:Q]$. This implies

$$\sum_{P\in M} N(P)^{-s} \leq [l:\mathbb{Q}] \sum_{r=2}^{[l:\mathbb{Q}]} \sum_{m=1}^{\infty} m^{-rs} \leq [l:\mathbb{Q}](\zeta_{\mathbb{Q}}(2) + \cdots + \zeta_{\mathbb{Q}}([l:\mathbb{Q}])).$$

Since the sum above is bounded, the set M has Dirichlet density 0. □

et density split

Lemma 108. *Let l/k be a finite Galois extension of number fields. Then the set of degree* 1 *primes of k which split completely in l has density $\frac{1}{[l:k]}$.*

Proof. Let M_k be the set of degree 1 primes of k and M_l the set of degree 1 primes of l. Every prime Q in M_l lies above some prime $P \in M_k$. If there is a prime Q above P, then there are precisely $[l:k]$ of them; this happens when P splits completely in l.

Let M be the set of $P \in M_k$ which split completely in l. Then we have

$$\sum_{P\in M} N(P)^{-s} = \frac{1}{[l:k]} \sum_{Q\in M_l} N(Q)^{-s} \sim \frac{1}{[l:k]} \log\left(\frac{1}{s-1}\right).$$

Here we have used lem:Dirichlet density degree one 107. □

4.5 Some L-functions

Lemma 109. *$H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ is finite.*

Proof. We have

$$\begin{aligned}\mathrm{Cl}_l/N(\mathrm{Cl}_l) &\cong \mathbb{A}^\times_{k,S}/\mathcal{O}^\times_{k,S} N(\mathbb{A}^\times_{l,S}) \\ &\cong \left(\prod_{v\in S} k_v^\times/N(l_{\hat{v}}^\times)\right)/\mathcal{O}^\times_{k,S},\end{aligned}$$

where $\hat{v}$ is a place of l lying above v. The result follows because each of the groups $k_v^\times/N(l_w)$ is finite (in fact by the local reciprocity isomorphism this is isomorphic to the abelianization of the decomposition group of $\hat{v}$). □

Given any maximal ideal P of $\mathcal{O}_S$, we let π_P be an idele whose P-component is a uniformizer in k_P, and whose other components are all 1. The coset of π_P in $H^0(l/k, \mathrm{Cl}_l)$ does not depend on the choice of uniformizer since all the local units at P are local norms from l_Q for any $Q|P$ (because P is unramified in l). Equivalently, if we choose a generator $P = (\pi)$ then the coset of π_P is the inverse of the image of π in $\prod_{v\in S} k_v^\times/N(l_{\hat{v}}^\times)$. This clearly extends to a map

$$\iota : \text{non-zero fractional ideals of } \mathcal{O}_S \to H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l),$$

whose kernel is the sub group of ideals with a generator in $\prod_{v\in S} k_v^\times/N(l_{\hat{v}}^\times)$.

Definition 110. For any character $\chi : H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l) \to C^\times$ we define the L-function

$$L(s,\chi) = \sum_I \chi(I) \cdot N(I)^{-s} = \prod_P \frac{1}{1-\chi(P)\cdot N(P)^{-s}}.$$

Here s is a complex number with real part greater than 1; bith the product and the series converge absolutely in that region. In the sum, I ranges over the non-zero ideals of $\mathcal{O}_S$, and in the product P ranges over the maximal ideals of $\mathcal{O}_S$.

If χ is the trivial character, then $L(s,\chi)$ is (up to finitely many Euler factors for primes in S) equal to the Dedekind zera function of k.

It's known that $L(s,\chi)$ has a meromorphic continuation to $\mathbb{C}$ (see for example Tate's thesis, which is chapter XV of [2]). We won't need such a strong result here; we can make do with the following:

cassells frohlich

Lemma 111 (Weak lemma)**.** *If χ is a non-trivial character then $L(s,\chi)$ is bounded on the interval $(1,2)$.*

Lemma 112. *Let M be a set of primes of $\mathcal{O}_S$ whose image in $H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)$ is zero. There exists a real number c depending only on k and l, such that for all $s>0$ we have:*

$$\sum_{p\in M} N(P)^{-s} \le \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\log\left(\frac{1}{s-1}\right) + c.$$

Proof. Let $s>1$. All the series in the following calculation converge absolutely in this region. The implied constants in the $O(1)$ terms do not depend on s.

$$\begin{aligned}
\sum_{P\in M} |N(P)|^{-s} &= \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\sum_P\sum_\chi \chi(P)N(P)^{-s} \\
&= \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\sum_P\sum_\chi -\log(1-\chi(P)N(P)^{-s}) + O(1) \\
&= \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\sum_P\sum_\chi -\log|1-\chi(P)N(P)^{-s}| + O(1) \\
&= \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\sum_\chi\sum_P -\log|1-\chi(P)N(P)^{-s}| + O(1) \\
&= \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\log\left(\prod_\chi |L(s,\chi)|\right) + O(1) \\
&\le \frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}\log\left(\frac{1}{s-1}\right) + O(1).
\end{aligned}$$

Interchanging the order of summation is justified because the series converge absolutely. We need to be slightly careful about which branch of the logarithm we are using here. In the expression $\log(1-\chi(P)N(P)^{-s})$ we shall mean the branch which is continuous on the ball of radius 1, centred about 1. The imaginary parts of $\log(1-\chi(P)N(P)^{-s})$ and $\log(1-\bar\chi(P)N(P)^{-s})$ cancel out; this justifies replacing $\log(1-\chi(P)N(P)^{-s})$ by $\log|1-\chi(P)N(P)^{-s}|$. □

Remark. In fact the density of the set M in this lemma is precisely $\frac{1}{|H^0_{\mathrm{Tate}}(l/k,\mathrm{Cl}_l)|}$. This can be proved by showing that each $L(s,\chi)$ has a continuation to a neighbourhood of $s=1$, and is non-zero at $s=1$. However, proving this is more difficult than the weak lemma above, and we only need the inequality of the lemma.

4.6 The first inequality

first inequality

Theorem 113. *For any finite Galois extension l/k be have*

$$|H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)| \leq [l:k].$$

Proof. The easiest proof of this theorem is rather like that of Dirichlet's primes in arithmetic progressions result. We'll sketch the argument.

One can easily show that $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ is finite. We have a function

$$\text{primes in } \mathcal{O}_{S,k} \to H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l),$$

which takes a prime P to the coset of an idele, whose P component is a uniformizer in k_P, and whose other components are 1. This coset does not depend on the choice of uniformizer because P is unramified in l (by choice of S), and therefore every element of $\mathcal{O}_P^\times$ is a local norm in the extension.

By the method of Dirichlet's primes in arithmetic progressions theorem, we may show that the images in $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ of the primes of $\mathcal{O}_{k,S}$ are equidistributed, meaning that the set of primes in the preimage of an element of $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ has Dirichlet density $\frac{1}{|H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)|}$. The proof of this equidistribution result can be reduced to proving $L(1, \chi) \neq 0$ for each non-trivial character χ of $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ (see for example chapter VIII of [2]).

cassells frohlich

Let P be a degree one prime which splits completely in l. Then the norm map $(l \otimes k_P)^\times \to k_P$ is surjective, and therefore the image of P in $H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)$ is 0. We have shown in 108 that the set of such primes has Dirichlet density $\frac{1}{[l:k]}$. It follows that

lem:Dirichlet density split

$$\frac{1}{[l:k]} \leq \frac{1}{|H^0_{\mathrm{Tate}}(l/k, \mathrm{Cl}_l)|}.$$

This proves the result. □

clic idele class

Corollary 114. *If l/k is cyclic then $|H^2(l/k, \mathrm{Cl}_l)| = [l:k]$ and $H^1(l/k, \mathrm{Cl}_l) = 0$.*

Proof. This follows immediately from (a) the first inequality, (b) the periodicity of the cohomology for a cyclic group, and (c) the calculation of the Herbrand quotient of Cl_l. □

Theorem 115. *If l/k is any finite Galois extension then $H^1(l/k, \mathrm{Cl}_l) = 0$ and $|H^2(l/k, \mathrm{Cl}_l)| \leq [l:k]$.*

Proof. For each prime number p dividing $[l:k]$ we let k_p be the fixed field of a Sylow p-subgroup S_p of $\mathrm{Gal}(l/k)$. By 45, it's suffient to prove

cor:cohomology sub Sylow

$$H^1(l/k_p, \mathrm{Cl}_l) = 0, \qquad |H^2(l/k_p, \mathrm{Cl}_l)| \leq [l:k_p].$$

Since S_p is solvable, this reduces us to the case that $\mathrm{Gal}(l/k)$ is solvable. We'll prove the result by induction on k starting with $k = l$ and working downwards in cyclic quotients.

Clearly the result holds for $k = l$. Assume the result for a subfield m of l and let m/k by cyclic. We have an inflation restriction sequence:

$$0 \to H^1(m/k, \mathrm{Cl}_m) \to H^1(l/k, \mathrm{Cl}_l) \to H^1(l/m, \mathrm{Cl}_l).$$

The first term is zero by 114 and the last term is zero by the inductive hypothesis. Therefore $H^1(l/k, \mathrm{Cl}_l) = 0$.

cor:H1 H2 cyclic idele class

This implies that we have an inflation-restriction sequence

$$0 \to H^2(m/k, \mathrm{Cl}_m) \to H^2(l/k, \mathrm{Cl}_l) \to H^2(l/m, \mathrm{Cl}_l).$$

By the inductive hypothesis we have $|H^2(l/m, \mathrm{Cl}_l)| \leq [l : m]$ and by 114 we have $|H^2(m/k, \mathrm{Cl}_m)| \leq [m : k]$. It follows that $|H^2(l/k, \mathrm{Cl}_l)| \leq [l : k]$. □

cor:H1 H2 cyclic idele class

To complete the construction of fundamental classes and the reciprocity isomorphism, we need only show that there is an element in $H^2(l/k, \mathrm{Cl}_l)$ of order $[l : k]$. Such an element is constructed first for a cyclic cyclotomic extension l'/k with the same degree as l/k. It's then shown that the inflation of such a class to ll'/k must split on ll'/l, and must therefore be the inflation of an element of order $[l : k]$ in $H^2(l/k, \mathrm{Cl}_l)$.

Bibliography

[1] Artin Tate,

[2] Cassells Fröhlich, Algebraic number theory.

[3] Milne, Class field theory.

[4] Neukirch, Bonn notes on class field theory.

[5] Neukirch, Class field theory.