Group cohomology, Brauer groups, and algebraic K-theory

Joshua Ruiter

May 14, 2019

Origin and purpose of these notes

These notes originally began as a way for me to organize all the material I needed to know for my comprehensive exam into one place. The process of making it was a good way to study and locate parts of the material I needed to study better, and once made it served as a useful reference.

Now, my goal is that they will be useful to other people as a source of exposition and a way to learn. To that end, I have tried to add commentary and background where it was previously left out. However, my goal is not to be thorough in every detail. I have often left out proofs where my primary sources have one, especially if I think the proof is not that interesting or necesary to understand. When a proof is omitted, I refer to another source if I know of one.

My goal is never to be concise or terse. While it is admirable to avoid being wordy, too often mathematical texts swing far the other way and leave out too many details or explanations. At the risk of being wordy or repetitive, I try to be as explicit and verbose as possible in any details I deem important. It is less frustrating for a reader to skip over material they already understand than to spend hours of time trying to work through an "exercise for the reader" for every example.

Another goal is that these notes be thoroughly internally cross-referenced. Since LaTex so conveniently allows me to link and reference other parts of the document, I take advantage of this wherever possible.

Note on the author: I am a graduate student at Michigan State University. I take sole responsibility for any errors in this material. If you have questions or corrections, feel free to contact me by email at ruiterj2@msu.edu.

Overview of content

These notes serve primarily as an introduction to group cohomology, and then one of the main applications, which is to the Brauer group of a field. The early material on homological algebra and galois theory for infinite extensions is just background, and could reasonably be skipped or skimmed and looked up later as needed.

The primary source for most of the group cohomology material is Sharifi's notes [15]. If the reader really just wants to learn group cohomology, that is also a good way to learn, possibly better than reading these notes. The primary source for material on Brauer groups is Rapinchuk's notes [12], and the main source for algebraic K-theory is Milnor's book [10].

Contents

Chapter 1

Some homological algebra and category theory

In this section, we cover various background material for the more category-theoretic aspects of group cohomology. The main tools developed here to be used for group cohomology are the snake lemma (Proposition 1.1.4), and the long exact sequence on homology induced by a short exact sequence of chain complexes (Proposition 1.3.1).

We do not give full background on abelian categories, or derived functors, or even just the Ext functor. Weibel [**?**] is the standard source for this sort of thing, or see Dummit and Foote [3] for a less category-theoretic approach to defining Ext. We do freely use the language of abelian categories on occasion, but also attempt to give thorough element-wise arguments when possible.

1.1 Snake lemma

We begin with a very pedestrian lemma about kernels and cokernels.

Lemma 1.1.1. *Let R be a ring, and suppose we have a commutative square of R-modules*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} \\ A' & \xrightarrow{f'} & B' \end{array}$$

Then the natural maps

$$f|_{\ker a} : \ker a \to \ker b \qquad x \mapsto f(x)$$

and

$$\overline{f'} : \operatorname{coker} a \to \operatorname{coker} b \qquad \overline{x'} \mapsto \overline{f'(x')}$$

are well defined, and the following diagram commutes.

$$\begin{array}{ccc}
\ker a & \xrightarrow{f|_{\ker a}} & \ker b \\
\downarrow & & \downarrow \\
A & \xrightarrow{f} & B \\
\downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} \\
A' & \xrightarrow{f'} & B' \\
\downarrow & & \downarrow \\
\operatorname{coker} a & \xrightarrow{\overline{f'}} & \operatorname{coker} b
\end{array}$$

Proof. For the first, we just have to show that if $x \in \ker a$, then $f(x) \in \ker b$.

$$x \in \ker a \implies a(x) = 0 \implies 0 = f'a(x) = bf(x) = 0 \implies f(x) \in \ker b$$

For the second, we need to show that $\overline{f'(x')}$ doesn't depend on the representative $x' \in A'$ of $\overline{x'} \in \operatorname{coker} a$. Let $x', y' \in A$ be representatives of $\overline{x'}$. Then $x' - y' \in \operatorname{im} a$, so choose $z \in A$ with $a(z) = x' - y'$. We need to show that $f'(x') - f'(y') \in \operatorname{im} b$, but this is clear because

$$f'a(z) = f'(x' - y') = f'(x') - f'(y')$$

Hence $\overline{f'}$ is well defined. □

While the previous construction was nice and concrete, the same result holds in the general setting of an abelian category. In fact, the proof simpler and more interesting in this context.

Lemma 1.1.2. *Let $\mathcal{A}$ be an abelian category, with a commutative square in $\mathcal{A}$.*

$$\begin{array}{ccc}
A & \xrightarrow{f} & B \\
\downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} \\
A' & \xrightarrow{f'} & B'
\end{array}$$

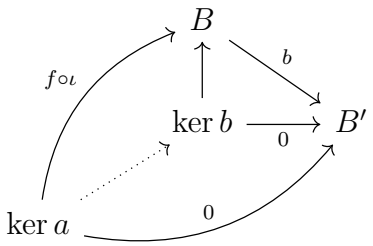
Then there are unique maps

$$\ker a \to \ker b \qquad \operatorname{coker} a \to \operatorname{coker} b$$

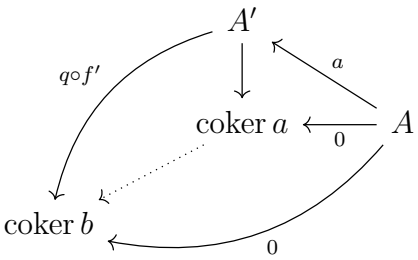
making the following diagram commute.

$$\begin{array}{ccc}
\ker a & \longrightarrow & \ker b \\
\downarrow & & \downarrow \\
A & \xrightarrow{f} & B \\
\downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} \\
A' & \xrightarrow{f'} & B' \\
\downarrow & & \downarrow \\
\operatorname{coker} a & \longrightarrow & \operatorname{coker} b
\end{array}$$

Proof. Let $\iota : \ker a \to A$ be the morphism associated to the kernel of a. By the universal property of the kernel, there is a unique morphism $\ker a \to \ker b$ making the following diagram commute.



Let $q : B' \to \operatorname{coker} b$ be the morphism associated to the cokernel of b. By the universal property of the cokernel, there is a unique morphism $\operatorname{coker} a \to \operatorname{coker} b$ making the following diagram commute.



□

We can also piece together a couple of squares of this type as in the next lemma.

Lemma 1.1.3. *Suppose we have a commutative diagram of R-modules with exact rows.*

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

The natural maps $\ker a \to \ker b$ *etc. make exact sequences*

$$\ker a \to \ker b \to \ker c \qquad \operatorname{coker} a \to \operatorname{coker} b \to \operatorname{coker} c$$

Proof. For the kernels, this is immediately obvious since $\ker a \to \ker b$ is just the restriction of f. For cokernels, it is obvious from the description of $\overline{f'}$ that $\overline{g'} \circ \overline{f'} = 0$. If $\overline{x'} \in \ker \overline{g'}$, there is a lift $x' \in \ker g' = \operatorname{im} f'$, so there is $y \in A'$ with $f'(y) = x'$. Hence $\overline{f}'(\overline{y}) = \overline{f'(y)} = \overline{x'}$, so $\ker \overline{g'} \in \operatorname{im} \overline{f'}$, which proves exactness for the cokernel sequence as well. □

Proposition 1.1.4 (Snake lemma)**.** *Let R be a ring, and suppose we have the following commutative diagram of R-modules with exact rows.*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

Then there is an R-module homomorphism $\delta : \ker c \to \operatorname{coker} a$ making an exact sequence

$$\ker a \longrightarrow \ker b \longrightarrow \ker c \xrightarrow{\delta} \operatorname{coker} a \longrightarrow \operatorname{coker} b \longrightarrow \operatorname{coker} c$$

Furthermore, if the original diagram can be extended with exact rows to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

the the exact sequence can be extended to

$$0 \longrightarrow \ker a \longrightarrow \ker b \longrightarrow \ker c \xrightarrow{\delta} \operatorname{coker} a \longrightarrow \operatorname{coker} b \longrightarrow \operatorname{coker} c \longrightarrow 0$$

Proof. Perhaps there should be a construction of the map δ which is more categorical in nature, but the simplest way to construct it is by a diagram chase. Let $x \in \ker c$. By surjectivity of $B \to C$, there is a lift $\widetilde{x} \in B$, $g(\widetilde{x}) = x$. By commutativity,

$$g'b(\widetilde{x}) = cg(\widetilde{x}) = c(x) = 0$$

hence $b(\widetilde{x}) \in \ker g' = \operatorname{im} f'$, so by exactness of the bottom row, $b(\widetilde{x}) \in \operatorname{im} f'$, so there is $y \in A'$ with $f'(y) = b(\widetilde{x})$. Define $\delta(x)$ to be the class of y in $\operatorname{coker} a = A'/\operatorname{im} a$. That is,

$$\delta(x) = \overline{(f')^{-1}\big(b(\widetilde{x})\big)}$$

We need to check that $\delta(x)$ doesn't depend on the lift $\widetilde{x}$. Let $\widetilde{x}, \widetilde{x}'$ be lifts of $x \in \ker c$. Let $y, y' \in A'$ with $f'(y) = b(\widetilde{x})$ and $f'(y') = b(\widetilde{x}')$. (The elements y, y' are unique by injectivity of f'.) We need to show $y - y' \in \operatorname{im} a$. Note that $g(\widetilde{x} - \widetilde{x}') = 0$, so by exactness of the top row, there is $z \in A$ of so that $f(z) = \widetilde{x} - \widetilde{x}'$. By commutativity,

$$bf(z) = \widetilde{x} - \widetilde{x}' = b(\widetilde{x}) - b(\widetilde{x}') = f'(y - y') = f'a(z)$$

Then by injectivity of f', we conclude that $a(z) = y - y'$, hence $y - y' \in \operatorname{im} a$. Thus δ is well defined. The sequence is exact except possibly at $\ker c$ and $\operatorname{coker} a$ by Lemma 1.1.3.

We first consider exactness at $\ker c$. Let $x \in \ker b$. Then $\delta g(x)$ is found by taking a lift of $g(x)$, for which we can choose x, then taking the image under b, which is zero since $x \in \ker b$, then taking the class in $\operatorname{coker} a$, so $\operatorname{im} g \subset \ker \delta$.

For the reverse inclusion, suppose $y \in \ker \delta \subset \ker c$. We choose a lift $x \in B$ with $g(x) = y$, and since $y \in \ker \delta$, the class of $b(y)$ in $\operatorname{coker} a$ is zero (we are identifying A' with its image in B' since f' is injective). That is, $b(y) \in \operatorname{im} a$, so there is $z \in A$ so that $b(x) = f'a(z)$. Then

$$b(x) = f'a(z) = bf(z) \implies x - f(z) \in \ker b$$

and

$$g(x - f(z)) = g(x) - gf(z) = y - 0 = y$$

Thus $x - f(z) \in \ker b$ maps to y under g, so $y \in \operatorname{im} g$. Thus $\ker \delta \subset \operatorname{im} g$, and we have proven exactness at $\ker c$. Now we prove exactness at $\operatorname{coker} a$. Let $x \in \ker c$, and let $\widetilde{x} \in B$ be a lift of x. Then

$$\overline{f'}\delta(x) = \overline{f'}\left(\overline{(f')^{-1}}\big(b(\widetilde{x})\big)\right) = \overline{f'(f')^{-1}b(\widetilde{x})} = \overline{b(\widetilde{x})} = 0 \in \operatorname{coker} b$$

Thus $\operatorname{im} \delta \subset \ker \overline{f'}$. For the reverse inclusion, suppose $\overline{y} \in \ker \overline{f'} \subset \operatorname{coker} a$ with representative $y \in A'$. Then

$$\overline{f'}\overline{y} = \overline{f'(y)} = 0 \in \operatorname{coker} b \implies f'(y) \in \operatorname{im} b$$

Thus there is $\widetilde{x} \in B$ so that $b(\widetilde{x}) = f'(y)$. Then $\delta(g(\widetilde{x})) = \overline{y}$ basically by definition of δ. Thus $\ker \overline{f'} \subset \operatorname{im} \delta$, proving exactness at $\operatorname{coker} a$.

The final remark about extending the exact sequences to zeros is mostly obvious. □

The snake lemma is surprisingly useful. Our main application will be using it to obtain a long exact sequence on the homology of a chain complex, in Proposition 1.3.1. But it also comes up in defining cup products for group cohomology, for example.

1.2 Homology of chain complexes

Definition 1.2.1. A **chain complex** of R-modules is a sequence $(C_n)_{n\in\mathbb{Z}}$ of R-modules with R-module homomorphisms $d_n : C_n \to C_{n-1}$ such that $d_{n-1}d_n = 0$ for all $n \in \mathbb{Z}$.

$$\cdots \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \xrightarrow{d_{n-1}} C_{n-2} \xrightarrow{d_{n-2}} \cdots$$

This may alternatively be written with indices ascending such as $d_n : C_n \to C_{n+1}$ or drawn with arrows going to the left, or the indices may be shifted so that $d_{n-1} : C_n \to C_{n-1}$, but these are not important distinctions.

This may also be defined in a general context of a abelian category or even just a category with some notion of a zero map.

Remark 1.2.2. A chain complex generalizes the notion of an exact sequence. In an exact sequence im = ker at each term, while a chain complex weakens this to im $\subset$ ker.

Definition 1.2.3. Let $C = (C_n, d_n)$ be a chain complex of R-modules. To each term C_n we have associated submodules

$$\begin{aligned} Z_n &= \ker d_n = n\text{-cycles} \\ B_n &= \operatorname{im} d_{n+1} = n\text{-boundaries} \\ H_n &= Z_n/B_n \end{aligned}$$

The submodule $H_n(C) = H_n$ is the **nth homology group** of C. Depending on the context, sometimes we add the prefix "co-" to all of these, making Z_n cocycles, B_n coboundaries, H_n cohomology.

Usually "co" denotes reversing arrows in category theory, but since reversing arrows doesn't change any structurally for chain complexes, "cohomology of cochain complex" is not meaningfully different than "homology of a chain complex" in a general context.

Definition 1.2.4. Let (C_n, d_n) and (D_n, ∂_n) be chain complexes of R-modules. A **chain map** between them is a sequence of R-module homomorphisms $f_n : C_n \to D_n$ making the following diagram commute.

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \xrightarrow{d_{n-1}} & C_{n-2} & \xrightarrow{d_{n-2}} & \cdots \\
 & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \downarrow{\scriptstyle f_{n-2}} & & \\
\cdots & \xrightarrow{\partial_{n+1}} & D_n & \xrightarrow{\partial_n} & D_{n-1} & \xrightarrow{\partial_{n-1}} & D_{n-2} & \xrightarrow{\partial_{n-2}} & \cdots
\end{array}$$

Remark 1.2.5. There is a category with objects being chain complexes over R and chain maps for morphisms. There are various notations for this, common ones include $\mathrm{Ch}(R)$ and $\mathrm{Kom}(R)$.

$\mathrm{Ch}(R)$ is an abelian category (no proof given here). Products, kernels, and cokernels are all constructed by taking the product/kernel/cokernel at each term (again, no proof given here). Thus the notion of exact sequences makes sense for chain complexes.

Lemma 1.2.6. *Let $A = (A_n), B = (B_n), C = (C_n)$ be chain complexes of R-modules. A sequence $A \to B \to C$ of chain complexes is exact if and only if each $A_n \to B_n \to C_n$ is exact.*

Proof. Omitted. □

If the concept of abelian category is foreign to the reader, they should just take the previous lemma as a definition for when a sequence of chain complexes is exact.

Remark 1.2.7. (This is somewhere between a definition and theorem.) Let $C = (C_n, d_n^C), D = (D_n, d_n^D)$ be chain complexes and $f = (f_n)$, $f_n : C_n \to D_n$ be a chain map. Then f induces maps

$$H_n(C) \to H_n(D) \qquad \overline{x} \mapsto \overline{f_n(x)}$$

These are called the **induced maps on homology**. We verify that this is well defined. Let $\overline{x} \in H_n(C)$ with representative $x \in Z_n(C) = \ker d_n^C$. Since f is a chain map, we have the following commutative square.

$$\begin{array}{ccc}
C_n & \xrightarrow{d_n^C} & C_{n-1} \\
\downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} \\
D_n & \xrightarrow{d_n^D} & D_{n-1}
\end{array}$$

Thus

$$d_n^D f_n(x) = f_{n-1} d_n^C(x) = 0 \implies f_n(x) \in \ker d_n^D = Z_n(D)$$

so it makes sense to take the class of $f_n(x)$ in $H_n(D)$. If x, x' are both representatives of $\overline{x} \in H_n(C)$, then $x - x' \in B_n(C)$, hence there is $y \in C_{n+1}$ with $d_{n+1}^C(y) = x - x'$. Using the chain map property of f again,

$$f_n(x) - f_n(x') = f_n(x) - f_n(x') = f_n(x - x') = f_n d_{n+1}^C(y) = d_{n+1}^D f_{n+1}(y)$$

hence $f_n(x) - f_n(x')$ lies in the image of d_{n+1}^D, which is to say, it represents the zero class in $H_n(D)$. Thus the induced map $H_n(C) \to H_n(D)$ is well defined.

1.3 Short exact sequence of complexes gives long exact sequence of cohomology

Apologies for the weird letters W, X, Y in the next proposition. A, B, C were not allowed due to possible confusion with boundaries B_n and similarly X, Y, Z would not work because of possible confusion with coboundaries Z_n.

Proposition 1.3.1 (LES induced by SES of chain complexes)**.** *Let $0 \to W \to X \to Y \to 0$ be a short exact sequence of chain complexes. Then there is a long exact sequence*

$$\cdots \to H_n(W) \to H_n(X) \to H_n(Y) \to H_{n-1}(W) \to H_{n-1}(X) \to H_{n-1}(Y) \to H_{n-2}(W) \to \cdots$$

where $H_n(W) \to H_n(X) \to H_n(Y)$ are the maps induced by the chain maps $W \to X \to Y$, and the "connecting homomorphisms" $H_n(Y) \to H_{n-1}(W)$ come from the snake lemma.

Proof. We already have the maps $H_n(W) \to H_n(X) \to H_n(Y)$. We need to construct the connecting homomorphisms $H_n(Y) \to H_{n-1}(W)$ so that everything is exact. To do this, we apply the snake lemma to the following commutative diagram.

$$\begin{array}{ccccccc} & & W_n/B_n(W) & \longrightarrow & X_n/B_n(X) & \longrightarrow & Y_n/B_n(Y) \longrightarrow 0 \\ & & \downarrow{\scriptstyle \overline{d_n^W}} & & \downarrow{\scriptstyle \overline{d_n^X}} & & \downarrow{\scriptstyle \overline{d_n^Y}} \\ 0 & \longrightarrow & Z_{n-1}(W) & \longrightarrow & Z_{n-1}(X) & \longrightarrow & Z_{n-1}(Y) \end{array} \tag{1.3.1}$$

The vertical arrows are induced by the boundary maps from the complexes, and the horizontal maps are induced by the maps $W \to X \to Y$, and the rows are exact because $0 \to W_n \to X_n \to Y_n \to 0$ is exact for all n.

We claim that the kernel of $\overline{d_n^W}$ is exactly $H_n(W)$, and the cokernel is $H_{n-1}(W)$. As justification for this, we just provide the commutative following diagram, where $B_n = B_n(W), Z_n = Z_n(W), H_n = H_n(W)$.

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & Z_n & \hookrightarrow & W_n & \xrightarrow{d_n^W} & W_{n-1} & \twoheadrightarrow & W_{n-1}/B_{n-1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & Z_n/B_n = H_n & \hookrightarrow & W_n/B_n & \xrightarrow{\overline{d_n^W}} & Z_{n-1} & \longrightarrow & Z_{n-1}/B_{n-1} = H_{n-1} & \longrightarrow & 0 \end{array}$$

By the snake lemma applied to diagram 1.3.1, we have an exact sequence

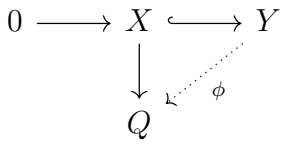
$$H_n(W) \to H_n(X) \to H_n(Y) \to H_{n-1}(W) \to H_{n-1}(X) \to H_{n-1}(Y)$$

Doing this same for each n gives the long exact sequence. There is some mild thinking to verify that the maps $H_n(W) \to H_n(X)$ induced by the snake lemma on 1.3.1 give the same as the induced maps $H_n(W) \to H_n(X)$ by usual means, but this is not very interesting. □

The reader who wants to learn group cohomology should probably skip from here to the start of the section on group cohomology. The rest of this section is not closely related.

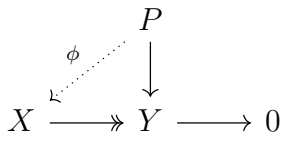
1.4 Injectives and projectives

Definition 1.4.1. An R-module Q is **injective** if every diagram as below can be completed to a commutative diagram by choosing some ϕ.



Equivalently, Q is injective if the functor $\mathrm{Hom}_R(-, Q)$ is exact, or if every short exact sequence $0 \to Q \to X \to Y \to 0$ splits (proof of equivalence omitted, see Lang [6]).

Definition 1.4.2. An R-module P is **projective** if every diagram as below can be completed to a commutative diagram by choosing some ϕ.



Equivalently, P is projective if the functor $\mathrm{Hom}_R(P, -)$ is exact, or if every short exact sequence $0 \to X \to Y \to P \to 0$ splits (proof of equivalence omitted, see Lang [6]).

Definition 1.4.3. An abelian category $\mathcal{A}$ has **enough injectives** if for every object X in $\mathcal{A}$, there is an injective object I and a monomorphism $X \to I$. (In the category of R-modules, monomorphism is equivalent to injective map.)

Definition 1.4.4. An abelian category $\mathcal{A}$ has **enough projectives** if for every object X in $\mathcal{A}$, there is a projective object P and an epimorphism $P \to X$. (In the category of R-modules, epimorphism is equivalent to surjective map.)

Definition 1.4.5. Let $\mathcal{A}$ be a category. An **projective resolution** of an object X (in $\mathcal{A}$) is an exact sequence

$$\cdots \to P_1 \to P_0 \to X \to 0$$

where each P_i is projective (in $\mathcal{A}$). Analogously, an **injective resolution** of X is an exact sequence

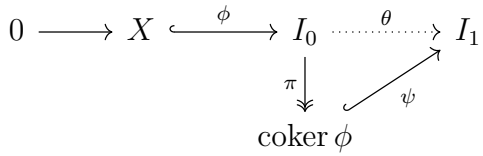
$$0 \to X \to Q_0 \to Q_1 \to \cdots$$

where each Q_i is injective (in $\mathcal{A}$).

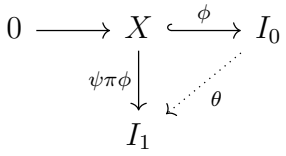
Philosophically speaking, why should we care whether a category has enough injectives or projectives? The main reason is that having enough injectives (resp. projectives) means that every object has an injective (resp. projective) resolution, and that having such resolutions is necessary to define derived functors, such as Ext.

Proposition 1.4.6. *Let $\mathcal{A}$ be an abelian category with enough injectives (projectives). Then every object X has an injective (projective) resolution in $\mathcal{A}$.*

Proof. As $\mathcal{A}$ has enough injectives, choose an injective object I_0 with a monomorphism $\phi : X \hookrightarrow I_0$. Let $\pi : I_0 \to \operatorname{coker}\phi$ be the cokernel map. Choose a monomorphism $\psi : \operatorname{coker}\phi \hookrightarrow I_1$ with I_1 injective. We want $\theta : I_0 \to I_1$ extending our exact sequence.



Since I_1 is injective, there exists θ making the following diagram commute.



Since ϕ is a monomorphism, $\theta\phi = \psi\pi\phi$ implies $\theta = \psi\pi$, hence θ makes our original diagram commute.

To check exactness of this sequence, we need $\ker\theta = \operatorname{im}\phi$. By definition, $\operatorname{im}\phi = \ker\operatorname{coker}\phi$, which is then equal to $\ker\pi$. On the other hand, $\ker\theta = \ker\psi\pi$, but since ψ is a monomorphism, this is just $\ker\pi$. Thus the sequence is exact.

We then iterate this construction to contiue extending the exact sequence, and obtain an injective resolution of X. The corresponding statement about projective resolutions may be proved using the exact same argument with all arrows reversed. Alternatively, it follows from the statement about injectives by considering the opposite category $\mathcal{A}^{\mathrm{op}}$. (Note that $\mathcal{A}^{\mathrm{op}}$ is also abelian, and injective objects in $\mathcal{A}$ correspond to projective objects in $\mathcal{A}^{\mathrm{op}}$.) □

Theorem 1.4.7. *Let R be a ring. The categories of R-modules and finitely generated R-modules have enough projectives.*

Proof. Every R-module M is a quotient of a free R-module, and free modules are projective. More concretely, if M is an R-module, let $\{m_i\}_{i\in I}$ be a generating set for M, and let F be the free R-module with basis set $\{m_i\}$,

$$F = \bigoplus_{i\in I} Rm_i$$

and we have a surjective map $F \to M$ by sending $m_i \in F$ to $m_i \in M$. This same argument shows that if M is finitely generated, then it is a quotient of a finitely generated free module. □

Unfortunately the analogous statement for injectives is not nearly as easy to prove, so it takes up our next few sections. First, we state without proof an occasionally useful criterion for injectivity.

Proposition 1.4.8 (Baer's criterion)**.** *Let R be a ring and Q an R-module. Then Q is injective (in the category of R-modules) if and only if for every left ideal $I \subset R$ any R-module homomorphism $\phi : I \to Q$ can be extended to an R-module homomorphism $\widetilde{\phi} : R \to Q$.*

Proof. Proposition 36 of Dummit and Foote [3]. □

1.4.1 Divisible abelian groups

Definition 1.4.9. Let A be an abelian group. A is **divisible** if for every $n \in \mathbb{Z}, n \neq 0$, the map

$$A \to A \qquad a \mapsto na$$

is surjective.

Example 1.4.10. No finite abelian group is divisible. Examples of divisible groups include the additive group $(\mathbb{Q}, +)$, $\mathbb{Q}/\mathbb{Z}$, and the multiplicative group $(\mathbb{C}^\times, \times)$.

Lemma 1.4.11. *An abelian group is injective (in the category of abelian groups) if and only if it is divisible.*

Proof. (Injective $\implies$ divisible) Let Q be an injective abelian group. Let $q \in Q$, and consider the map $\mathbb{Z} \to Q, 1 \mapsto q$. Since Q is injective, the following diagram can be completed to a homomorphism $\phi : \frac{1}{n}\mathbb{Z} \to Q$.

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \hookrightarrow & \frac{1}{n}\mathbb{Z} \\ & & {\scriptstyle 1\mapsto a}\downarrow & \swarrow_{\phi} & \\ & & Q & & \end{array}$$

For any $n \in \mathbb{Z}$ and any $q \in Q$, we get $n\phi\left(\frac{1}{n}\right) = \phi(1) = q$, so the map $n : Q \to Q$ is surjective, hence Q is divisible.

(Divisible $\implies$ injective) Let Q be a divisible abelian group, and suppose we have the diagram below. We need to construct h making the diagram commute.

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xrightarrow{f} & C \\ & & {\scriptstyle g}\downarrow & \swarrow_{h} & \\ & & Q & & \end{array}$$

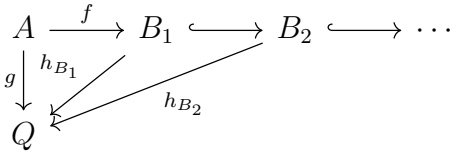
Consider the set $\mathcal{S}$ of pairs (B, h_B) where $A \subset B \subset C$ and $h_B : B \to Q$ is a lift making the following diagram commute.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \hookrightarrow & C \\ {\scriptstyle g}\downarrow & \swarrow_{h_B} & & & \\ Q & & & & \end{array}$$

We give $\mathcal{S}$ a partial order by $(B, h_B) \leq (B', h_{B'})$ when $B \subset B'$ and $h_{B'}|_B = h_B$.

$$\begin{array}{ccccccc} A & \xrightarrow{f} & B & \hookrightarrow & B' & \hookrightarrow & C \\ {\scriptstyle g}\downarrow & {\scriptstyle h_B}\swarrow & & \swarrow_{h_{B'}} & & & \\ Q & & & & & & \end{array}$$

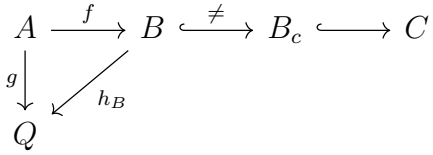
We want to apply Zorn's lemma to $\mathcal{S}$, so we need to show that any ascending chain has an upper bound. Let (B_i, h_{B_i}) be an ascending chain.



Then an upper bound is given by$(\widetilde{B}, h_{\widetilde{B}})$ where $\widetilde{B}$ is the subgroup generated by $\bigcup_i B_i$ and the map $h_{\widetilde{B}}$ is defined by $h_{\widetilde{B}}(b) = h_B(b)$ for $b \in B$. Thus Zorn's lemma applies to $\mathcal{S}$, so there is a maximal element $(B_{\max}, h_{B_{\max}})$.

If we can show that $B_{\max} = C$, and then we are done. To do this, it is sufficient to show that for any pair (B, h_B) such that $B \neq C$, there is $(B', h_{B'}) \in \mathcal{S}$ with $B \subsetneq B'$, since if we do this, then if $B_{\max} \neq C$, there is a larger subgroup strictly containing $B_{\max}$ with an extension, contradicting maximality of $B_{\max}$, and resulting in the conclusion that $B_{\max} = C$.

Now we show that if $(B, h_B) \in \mathcal{S}$ with $B \neq C$, there exists $(B', h_{B'}) \in \mathcal{S}$ with $B \subsetneq B'$ and $h_{B'}|_B = h_B$. Let $(B, h_B) \in \mathcal{S}$ with $B \neq C$ and choose $c \in C \setminus B$, and let $B_c = B + c = B + \mathbb{Z}c \subset B$ be the subgroup generated by B and c.



We consider two cases:

1. There does not exist $n \in \mathbb{Z}_{\geq 1}$ such that $nc \in B$.
2. There exists $n \in \mathbb{Z}_{\geq 1}$ such that $nc \in B$.

In case (1), $B_c = B + \mathbb{Z}c = B \oplus \mathbb{Z}c$, and h_B can be extended to $h_{B_c} : B_c \to Q$ by $h_{B_c}|_B = h_B$ and $h_{B_c}(c) = 0$. (Or set $h_{B_c}(c)$ to be anything, it doesn't have to be zero.) Thus B_c is a strictly larger extension than B.

In case (2), let $n \in \mathbb{Z}_{\geq 1}$ be the smallest integer so that $nc \in B$. Finally, we use the fact that Q is divisible to choose $q \in Q$ such that $nq = h_B(nc)$. Consider the map $\pi : B \oplus \mathbb{Z} \to B_c, (b, m) \mapsto b + mc$, which fits into the exact sequence

$$0 \to \ker \pi \to B \oplus \mathbb{Z}c \xrightarrow{\pi} B_c \to 0$$

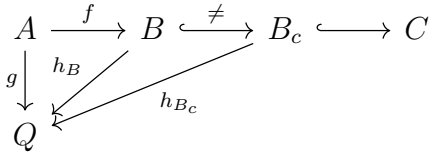
and (via the first isomorphism theorem) induces an isomorphism $(B \oplus \mathbb{Z}c)/\ker \pi \cong B_c$. Now consider the map

$$\widetilde{h} : B \oplus \mathbb{Z} \to Q \qquad \widetilde{h}(b, m) = h_B(b) + mq$$

If $(b, m) \in \ker \pi$ so that $b + mc = 0$, then $-mc \in B$, so $|m| \geq n$ and n divides m (by minimality of n), so $m = nt$ for some $t \in \mathbb{Z}$, and then

$$\widetilde{h}(b, m) = h_B(b) + mq = h_B(-mc) + mq = h_B(-tnc) + tnq = t(-h_B(nc) + nq) = 0$$

This shows that $\ker \pi \subset \ker \widetilde{h}$. Thus $\widetilde{h}$ factors through $(B \oplus \mathbb{Z}c)/\ker \pi \cong B_c$ to give a map $h_{B_c} : B_c \to Q$ satisfying $h_{B_c}(b + mc) = h_B(b) + mq$ and in particular $h_{B_c}(b + 0c) = h_B(b)$, so h_{B_c} extends h_B.



□

Remark 1.4.12. The proof given above that an injective abelian group is divisible also holds in the category of finitely generated abelian groups, since the groups used, $\mathbb{Z}$ and $\frac{1}{n}\mathbb{Z}$, are both finitely generated. That is to say, an injective object in the category of finitely generated abelian groups must be divisible.

Remark 1.4.13. The simplest examples of divisible abelian groups are $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$, so these are injective $\mathbb{Z}$-modules. Note that there are no finite abelian groups which are divisible.

Proposition 1.4.14 (Properties of divisible abelian groups)**.** .

1. *The tensor product of a divisible abelian group with any abelian group is divisible.*
2. *The torsion subgroup of a divisible abelian group is divisible.*
3. *A divisible group splits as a direct sum of its torsion subgroup and a torsion free group.*
4. *The tensor product of a divisible abelian group with a torsion group is zero.*
5. *The tensor product of two torsion free abelian groups is torsion free.*
6. *Then tensor product of divisible abelian groups is uniquely divisible.*

Proof. (1) Let A, B be abelian groups with A divisible. Then for a generator $a \otimes b$ of $A \otimes B$ and $n \in \mathbb{Z}$, there exists $a' \in A$ such that $na' = a$, so $n(a' \otimes b) = na' \otimes b = a \otimes b$. Since simple tensors generate $A \otimes B$, this shows that $A \otimes B$ is divisible.

(2) Let A be divisible and let $A_{\text{tor}} \subset A$ be the torsion subgroup. For $n \in \mathbb{Z}$, consider $n : A_{\text{tor}} \to A_{\text{tor}}$. Let $a \in A_{\text{tor}}$. Since A is divisible, there exists $a' \in A$ such that $n'a = a$. Since a is torsion, a' is also torsion, so $a' \in A_{\text{tor}}$. Thus A_{tor} is divisible.

(3) Let A be divisible and A_{tor} the torsion subgroup. Since A_{tor} is divisible, it is injective in the category of abelian groups, so

$$0 \to A_{\text{tor}} \to A \to A/A_{\text{tor}} \to 0$$

is split exact. Clearly A/A_{tor} is torsion free.

(4) Let A be divisible and B be torsion. Then for a generator $a \otimes b \in A \otimes B$, there exists $n \in \mathbb{Z}$ such that $nb = 0$, and then there exists $a' \in A$ such that $na' = a$. Then $a \otimes b = na' \otimes b = a' \otimes nb = a' \otimes 0 = 0$. So all the generators are zero, so $A \otimes B = 0$.

(5) Let A, B be torsion free, so they are flat. So $- \otimes A$ is exact, and $- \otimes B$ is exact. Then the composition $- \otimes B \circ \otimes A$ of functors is exact, but this is "the same " (naturally isomorphic as functors) as ${}_{\otimes}(A \otimes B)$, so $A \otimes B$ is flat, so it is torsion free.

(6) Let A, B be uniquely divisible. By (1), $A \otimes B$ is divisible, so to show it is uniquely divisible, it suffices to show that it is torsion free. By (2), they split as $A \cong A_{\text{tor}} \oplus A_{\text{free}}$ and $B \cong B_{\text{tor}} \oplus B_{\text{free}}$. Then

$$\begin{aligned} A \otimes B &\cong (A_{\text{tor}} \oplus A_{\text{free}}) \otimes (B_{\text{tor}} \oplus B_{\text{free}}) \\ &\cong (A_{\text{tor}} \otimes B_{\text{tor}}) \oplus (A_{\text{tor}} \otimes B_{\text{free}}) \oplus (A_{\text{free}} \otimes B_{\text{tor}}) \oplus (A_{\text{tor}} \otimes B_{\text{free}}) \end{aligned}$$

By (4), the first three terms vanish, and by (5), the last term is torsion free. □

1.4.2 Enough injectives for R-mod

Definition 1.4.15. Let R be a ring and M an R-module. We define $M^\vee = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. We view $M^\vee$ as an R-module via the action

$$(r \cdot \phi)(m) = \phi(r \cdot m)$$

where $r \in R, m \in M, \phi \in M^\vee$, and $r \cdot m$ is the action of R on M.

We view $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z}) = M \mapsto M^\vee$ as a contravariant functor from the category of R-modules to itself. Note that because $\mathbb{Q}/\mathbb{Z}$ is divisible, it is an injective abelian group, so the functor $\text{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is exact (as a functor from abelian groups to abelian groups), so it is an exact functor from R-mod to itself.

Definition 1.4.16. Let M be an R-module. The **evaluation map** is

$$\text{ev} : M \to (M^\vee)^\vee \qquad m \mapsto (\phi \mapsto \phi(m)) \qquad \text{ev}(m)(\phi) = \phi(m)$$

Definition 1.4.17. Let R be a ring and M an R-module. The free module on M is

$$F(M) = \bigoplus_{m \in M} R[m]$$

with the accompanying surjection

$$F(M) \to M \qquad \sum_i r_i[m_i] \mapsto \sum_i r_i m_i$$

We think of $M \mapsto (F(M) \to M)$ as a functor from R-mod to the arrow category of R-mod.

Definition 1.4.18. Let R be a ring and M an R-module. Set $J(M) = (F(M^\vee))^\vee$.

Theorem 1.4.19. *Let R be a ring and M an R-module.*

1. The evaluation map $\text{ev} : M \to (M^\vee)^\vee$ is injective.
2. There is a (canonical) embedding $M \hookrightarrow J(M)$.
3. $R^\vee$ is an injective R-module.
4. $J(M)$ is an injective R-module.

5. The category of R-modules has enough injectives.

Proof. (1) We show that if $x \in M$ and $x \neq 0$, then $\mathrm{ev}(x) \neq 0$. Equivalently, we need to show that there is $\phi \in M^\vee = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ such that $\mathrm{ev}(x)(\phi) = \phi(x) \neq 0$. Let $x \in M, x \neq 0$. Let $M' \subset M$ be the abelian subgroup generated by x (NOT the R-submodule generated by x, this is not the same thing). Then there is a nonzero map $\psi : M' \to \mathbb{Q}/\mathbb{Z}$ which does not vanish on x (for example, if $nx = 0$, send x to $\frac{1}{n}$). Then because $\mathbb{Q}/\mathbb{Z}$ is an injective abelian group, this extends to a map $\widetilde{\psi} : M \to \mathbb{Q}/\mathbb{Z}$ which does not vanish on x.

$$\begin{array}{ccccc} 0 & \longrightarrow & M' & \longrightarrow & M \\ & & \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle \widetilde{\psi}} & \\ & & \mathbb{Q}/\mathbb{Z} & & \end{array}$$

Then $\mathrm{ev}(x)(\widetilde{\psi}) = \widetilde{\psi}(x) \neq 0$. Hence ev is injective.

(2) Consider the canonical surjection $F(M^\vee) \to M^\vee$. Apply the contravariant, exact functor $(-)^\vee$ to obtain $(M^\vee)^\vee \to (F(M^\vee))^\vee = J(M)$. Since $(-)^\vee$ is exact, the surjection becomes an injection. Thus we have injections

$$M \xrightarrow{\mathrm{ev}} (M^\vee)^\vee \to J(M)$$

which is to say, M embeds into $J(M)$.

(3) Let N be an R-module. As some people would say,

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$$

However, I think that it's sloppy to write an equality here. What this really means is that there is a natural isomorphism of R-modules

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \to \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) \qquad \phi \mapsto \Big(n \mapsto \phi(n)(1)\Big)$$

with inverse given by

$$\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \qquad \psi \mapsto \Big(n \mapsto \big(1 \mapsto \psi(n)\big)\Big)$$

(details left unchecked by me, the author). By "natural isomorphism," I mean that this is furthermore an isomorphism of functors

$$(-)^\vee = \mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) = \mathrm{Hom}_R(-, R^\vee)$$

(once again, details left unchecked). Therefore since $(-)^\vee$ is exact, $\mathrm{Hom}_R(-, R^\vee)$ is exact, so $R^\vee$ is injective.

(4) Note that we have an isomorphism of R-modules

$$J(M) = (F(M^\vee))^\vee = \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{\phi \in M^\vee} R[\phi], \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{\phi \in M^\vee} \mathrm{Hom}_{\mathbb{Z}}(R[\phi], \mathbb{Q}/\mathbb{Z}) \cong \prod_{\phi \in M^\vee} R^\vee$$

Since a product of injective objects is injective and $R^\vee$ is injective by (3), this product is injective.

(5) This is immediate from (2) and (4). □

Remark 1.4.20. The previous proof, combined with the fact that the torsion subgroup of a divisible abelian group is injective (1.4.14) shows that the category of torsion abelian groups has enough injectives, since the canonical embedding $M \hookrightarrow J(M)$ has image in the torsion subgroup, which is also injective.

1.4.3 Projectives and injectives in some subcategories of abelian groups

Proposition 1.4.21. *The category of finitely generated abelian groups has enough projectives, but not enough injectives. (In fact, there are no nonzero injective objects at all in this category).*

Proof. Every finitely generated abelian group A is a finite direct sum of cyclic groups,

$$A \cong \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$$

Then A is a quotient of a a free module on the same number of generators by sending a generator for each infinite cyclic summand to a generator for the corresponding cyclic summand of A. That is, we have the surjection

$$\mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z} \xrightarrow{\mathrm{Id}^r \oplus \pi} \mathbb{Z}^r \oplus \bigoplus_i \mathbb{Z}/n_i\mathbb{Z}$$

where π sends the generator of the ith summand $\mathbb{Z}$ to the generator of $\mathbb{Z}/n_i\mathbb{Z}$. Hence there are enough projectives.

Now suppose A is an injective object in the category of finitely generated abelian groups. By remark 1.4.12, A is divisible. However, there are no divisible finitely generated abelian groups, except the trivial group. □

Proposition 1.4.22. *The category of torsion abelian groups has enough injectives, but not enough projectives.*

Proof. First, we show that there are enough injectives. Let M be a torsion abelian group. Then we have an embedding $M \to J(M)$, and by Theorem 1.4.19, $J(M)$ is injective. Note that the torsion subgroup of a divisible group is divisible, and that M lands in the torsion subgroup of $J(M)$, so M embeds into an injective object.

Now we show that there are not enough projectives [1]. To show there are not enough projectives, we show that there is no projective which surjects onto $\mathbb{Z}/2\mathbb{Z}$. Suppose there is a projective object P with a map $\phi : P \to \mathbb{Z}/2\mathbb{Z}$ and an element $x \in P$ so that $\phi(x) = 1$. For $k \geq 1$, we have the quotient map $\pi : \mathbb{Z}/2^k\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}, 1 \mapsto 1$. Since P is projective, there is a lift $\widetilde{\phi} : P \to \mathbb{Z}/2^k\mathbb{Z}$ with $\widetilde{\phi}(x) = 1$.

$$\begin{array}{ccccc} & & & & P \\ & & & \overset{\widetilde{\phi}}{\swarrow} & \downarrow{\scriptstyle \phi} \\ \mathbb{Z}/2^k\mathbb{Z} & \xrightarrow[\pi]{} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

[1] In fact, there are no nontrivial projective objects in this category, but the proof given here https://math.stackexchange.com/questions/1038786/existence-of-projectives-in-the-category-of-torsion-abelian-groups requires some knoweldge about Prufer groups, so we omit it. This proof is also given at that source, in the original question.

Note that any element of $\mathbb{Z}/2^k\mathbb{Z}$ which maps to 1 under π is a generator, since it is coprime to 2^k. In particular, $\widetilde{\phi}(x)$ is a generator of $\mathbb{Z}/2^k\mathbb{Z}$, so $x \in P$ has order at least 2^k. Since k was arbitrary, this shows that x has arbitrarily large order so x is not torsion, which is impossible since P is a torsion group. Thus P does not exist. □

1.5 Computations of Ext groups

As previously discussed, we do not give a full development of the definition of Ext. However, we recall the usual strategy for computing Ext groups via projective and injective resolutions. Let R be a ring and let A, B be R-modules. Given a projective resolution of A

$$\cdots \to P_1 \to P_0 \to A \to 0$$

we apply the contravariant functor $\mathrm{Hom}_R(-, B)$ and drop the A term to obtain a chain complex

$$0 \to \mathrm{Hom}_R(P_0, B) \to \mathrm{Hom}_R(P_1, B) \to \cdots$$

The ith homology of this chain complex is $\mathrm{Ext}^i_R(A, B)$. Alternatively, one may being with an injective resolution of B,

$$0 \to B \to I_0 \to I_1 \to \cdots$$

and apply the covariant functor $\mathrm{Hom}_R(A, -)$ and drop the B term to obtain a chain complex

$$0 \to \mathrm{Hom}_R(A, I_0) \to \mathrm{Hom}_R(A, I_1) \to \cdots$$

The ith homology of this chain complex is also $\mathrm{Ext}^i_R(A, B)$.

The main issue that needs addressing here is why on earth this computation does not depend on the choice of projective objects P_i or the choice of injective objects I_i. It is not at all clear that this is true from the outset. We even threw away the one term that we know doesn't depend on any choices, so maybe this is total nonsense. It takes some work, and I'm lazy, so I haven't done it here, but there are a few key technical results in homological algebra which tell us that this does not depend on the choice of resolution.

Now we give a variety of examples. The following computations of Ext groups are all examples, exercises, or theorems from Dummit and Foote [3].

Proposition 1.5.1. *Let A be an abelian group. Then*

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong \begin{cases} {}_mA & i = 0 \\ A/mA & i = 1 \\ 0 & i \geq 2 \end{cases}$$

Proof. We have a projective resolution of $\mathbb{Z}/m\mathbb{Z}$

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

Then we apply the contravariant functor $\mathrm{Hom}_{\mathbb{Z}}(-, A)$ and drop the $\mathbb{Z}/m\mathbb{Z}$ term to obtain a chain complex depicted below. Using the canoncial isomorphism $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ via $\phi \mapsto \phi(1)$, we get an isomorphism of chain complexes.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) & \xrightarrow{m} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & A & \xrightarrow{m} & A & \longrightarrow & 0 \end{array}$$

Thus $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong {}_mA$ and $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong A/mA$, and the higher ext groups vanish. □

Proposition 1.5.2. *Let m, d be integers with $d|m$, and let A be an abelian group of exponent m (aka A is a $\mathbb{Z}/m\mathbb{Z}$-module). Then*

$$\mathrm{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, A) = \begin{cases} {}_dA & i = 0 \\ {}_{m/d}A/dA & i = 1, 3, \dots \\ {}_dA/(m/d)A & i = 2, 4, \dots \end{cases}$$

Proof. We begin with a projective (free) resolution of $\mathbb{Z}/d\mathbb{Z}$ (in the category of $\mathbb{Z}/m\mathbb{Z}$-modules).

$$\cdots \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/d\mathbb{Z} \longrightarrow 0$$

The map π is the quotient map $1 \mapsto 1$, whose kernel is generated by m/d, which justifies exactness at the first $\mathbb{Z}/m\mathbb{Z}$ term. Exactness at the other terms is clear.

Then we apply the contravariant functor $\mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(-, A)$ and drop the $\mathbb{Z}/d\mathbb{Z}$ term to obtain the upper chain complex depicted below. Using the isomorphism $\mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) \cong A$, we get an isomorphism of chain complexes.

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) & \xrightarrow{d} & \mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) & \xrightarrow{m/d} & \mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, A) & \xrightarrow{d} & \cdots \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & A & \xrightarrow{d} & A & \xrightarrow{m/d} & A & \xrightarrow{d} & \cdots \end{array}$$

The ith homology of this periodic chain complex is $\mathrm{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(\mathbb{Z}/d\mathbb{Z}, A)$, so we read off exactly the homology as claimed. □

Lemma 1.5.3. *$\mathbb{Z}/m\mathbb{Z}$ is an injective $\mathbb{Z}/m\mathbb{Z}$-module.*

Proof. By Baer's criterion 1.4.8, it suffices to show that for any ideal $I \subset \mathbb{Z}/m\mathbb{Z}$ and any $\mathbb{Z}/m\mathbb{Z}$-linear map $I \to \mathbb{Z}/m\mathbb{Z}$, there is an extension $\widetilde{\phi} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. An ideal of $\mathbb{Z}/m\mathbb{Z}$ is a subgroup of the form $n\mathbb{Z}/m\mathbb{Z}$. Any such subgroup can be written as $d\mathbb{Z}/m\mathbb{Z}$ where $d = \gcd(n, m)$, in particular, $d|m$.

Suppose we have $\phi : d\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. By linearity, ϕ is determined by $\phi(d)$. Since d has order m/d, it must be mapped to something of order m/d, so it is mapped to something in the subgroup $d\mathbb{Z}/m\mathbb{Z}$ (since finite cyclic groups have a unique subgroup of each divisor order), so $\phi(d) = kd$. Then we extend ϕ to $\mathbb{Z}/m\mathbb{Z}$ by setting $\widetilde{\phi}(1) = k$. □

Proposition 1.5.4. *Let m, d be integers with $d|m$, and let A be an abelian group of exponent m (aka A is a $\mathbb{Z}/m\mathbb{Z}$-module). Let $\widehat{A} = \mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A, \mathbb{Z}/m\mathbb{Z})$ be the dual group of A. Then*

$$\mathrm{Ext}^i_{\mathbb{Z}/m\mathbb{Z}}(A, \mathbb{Z}/d\mathbb{Z}) = \begin{cases} {}_d\widehat{A} & i = 0 \\ {}_{m/d}\widehat{A}/d\widehat{A} & i = 1, 3, \dots \\ {}_d\widehat{A}/(m/d)\widehat{A} & i = 2, 4, \dots \end{cases}$$

Proof. By the previous lemma 1.5.3, $\mathbb{Z}/m\mathbb{Z}$ is an injective $\mathbb{Z}/m\mathbb{Z}$-module. Thus the following is an injective resolution of $\mathbb{Z}/d\mathbb{Z}$ (in the category of $\mathbb{Z}/m\mathbb{Z}$-modules).

$$0 \to \mathbb{Z}/d\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{d} \mathbb{Z}/m\mathbb{Z} \xrightarrow{m/d} \cdots$$

Then we apply the covariant functor $\mathrm{Hom}_{\mathbb{Z}/m\mathbb{Z}}(A, -)$ and drop the first term to obtain the chain complex below. We omit the subscript $\mathbb{Z}/m\mathbb{Z}$ for Hom.

$$0 \longrightarrow \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{d} \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{m/d} \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{d} \cdots$$

From this, we read off the necessary homology. □

Remark 1.5.5. A finite abelian group is (non-canonically) isomorphic to its dual, but an infinite abelian group need not be.

Proposition 1.5.6. *Let Q be an injective R-module. Then $\mathrm{Ext}^n_R(A, Q) = 0$ for all R-modules A and all $n \geq 1$.*

Proof. We have the somewhat trivial injective resolution of Q

$$0 \to Q \to Q \to 0$$

Then we apply the contravariant functor $\mathrm{Hom}_R(A, -)$ and drop the first term to obtain the even more trivial chain complex

$$0 \to \mathrm{Hom}_R(A, Q) \to 0$$

whose ith homology is $\mathrm{Ext}^i_R(A, Q)$. Thus $\mathrm{Ext}^0_R(A, Q) = \mathrm{Hom}_R(A, Q)$ (as always), and higher Ext groups vanish. □

Example 1.5.7. For $R = \mathbb{Z}$, we know that injective is equivalent to divisible. So as examples of the above we obtain

$$\mathrm{Ext}^n_{\mathbb{Z}}(A, \mathbb{Q}) = 0 \qquad \mathrm{Ext}^n_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) = 0$$

for all $n \geq 1$ and all abelian groups A.

Proposition 1.5.8. *Let P be a projective R-module. Then $\mathrm{Ext}^n_R(P, A) = 0$ for all R-modules A and all $n \geq 1$.*

Proof. We have the somewhat trivial projective resolution of P

$$0 \to P \to P \to 0$$

Then we apply the covariant functor $\mathrm{Hom}_R(-, A)$ and drop the first term to obtain the even more trivial chain complex

$$0 \to \mathrm{Hom}_R(P, A) \to 0$$

whose ith homology is $\mathrm{Ext}^i_R(P, A)$. Thus $\mathrm{Ext}^0_R(P, A) = \mathrm{Hom}_R(P, A)$ as always, and higher Ext groups vanish. □

Example 1.5.9. For $R = \mathbb{Z}$ (or any PID), we know that projective is equivalent to free. So from the above we obtain

$$\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}^k, A) = 0$$

for all $n, k \geq 1$ and all abelian groups A.

Proposition 1.5.10. *Let A, B be abelian groups. Then $\mathrm{Ext}^n_{\mathbb{Z}}(A, B) = 0$ for all $n \geq 2$.*

Proof. Recall that for abelian groups, injective is equivalent to divisible, and recall that a quotient of a divisible group is divisible. We know that $\mathbb{Z}$-mod has enough injectives, so choose an embedding $B \hookrightarrow Q$ with Q injective/divisible. Then the quotient Q/B is also divisible, to it is injective. Thus we have an injective resolution

$$0 \to B \to I \to I/B \to 0$$

Then we apply the covariant functor $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ and drop the B term to obtain a chain complex whose ith homology is $\mathrm{Ext}^i_{\mathbb{Z}}(A, B)$.

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, I) \to \mathrm{Hom}_{\mathbb{Z}}(A, I/B) \to 0$$

We can't say very much about Ext^0 and Ext^1, but we can read off from this that $\mathrm{Ext}^n_{\mathbb{Z}}(A, B) = 0$ for $n \geq 2$. □

Proposition 1.5.11. *Let A be a torsion abelian group. Then*

$$\mathrm{Ext}^i_{\mathbb{Z}}(A, \mathbb{Z}) = \begin{cases} 0 & i = 0, i \geq 2 \\ \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) & i = 1 \end{cases}$$

Proof. We have an injective resolution of $\mathbb{Z}$

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Then we apply the covariant functor $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ and drop the $\mathbb{Z}$ term to obtain a chain complex whose ith homology is $\mathrm{Ext}^i_{\mathbb{Z}}(A, \mathbb{Z})$.

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) \to \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) \to 0$$

Because A is torsion and $\mathbb{Q}$ is torsion free, $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}) = 0$. Thus the 0th homology is zero, the first homology is $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$, and the higher homology groups vanish. □

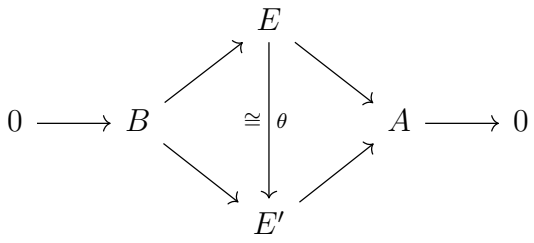
1.5.1 Extensions and Ext

Definition 1.5.12. Let A, B be R-modules. An **extension** of B by A is a short exact sequence of R-modules

$$0 \to B \to E \to A \to 0$$

Sometimes we are careless and refer to the object E as the extension, but this is not proper terminology.

Definition 1.5.13. Two extensions $0 \to B \to E \to A \to 0$ and $0 \to B \to E' \to A \to 0$ are **equivalent** if there is an isomorphism $\theta : E \to E'$ making the following diagram commute.



This is an equivalence relation.

A warning: It is NOT sufficient to have an isomorphism $E \cong E'$ if the diagram does not commute. That is, there may be extensions such that E, E' are isomorphic, and yet they are not equivalent extensions.

This is the real reason that it is improper to speak of the object E as the extension, since even the isomorphism class of E does not determine the equivalence class of the extension $0 \to B \to E \to A \to 0$. For a concrete example of this, see Example 1.5.15 where there are several inequivalent extensions with the same object in the middle.

Theorem 1.5.14. *There is an isomorphism between* $\mathrm{Ext}^1_R(A, B)$ *and the group of equivalence classes of extensions* $0 \to B \to E \to A \to 0$.

Proof. Omitted. □

Note that I haven't even told you what the group structure on extensions is. There is not even an obvious choice of definition for adding two extensions together. The "right" definition is something called the Baer sum, which involves the categorical pullback. Suffice it to say, the additive identity for this group is always the "trivial" or "split extension"

$$0 \to B \to B \oplus A \to A \to 0$$

where the left map is inclusion into the left factor and the right map is projection onto the right factor.

Example 1.5.15. We know that $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ by Proposition 1.5.1. By the previous theorem, this means that there are exactly p inequivalent extensions

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E \to \mathbb{Z}/p\mathbb{Z} \to 0$$

We now give concrete descriptions of these p extensions. As for any two groups, there is the trivial split extension

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

where the left map is inclusion into the left factor and the right map is projection onto the right factor (the choice of which factor does not change the equivalence class of this extension). For nontrivial extensions, we have the following $p-1$ extensions.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{p} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\bmod p} & \mathbb{Z}/p\mathbb{Z} & \to & 0 \\
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{2p} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\bmod p} & \mathbb{Z}/p\mathbb{Z} & \to & 0 \\
 & & \vdots & & \vdots & & \vdots & & \\
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{(p-1)p} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\bmod p} & \mathbb{Z}/p\mathbb{Z} & \to & 0
\end{array}$$

It is clear that none of these is equivalent to the trivial extension, since $\mathbb{Z}/p^2\mathbb{Z} \ncong \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$, so to know that we have found a representative for every equivalence class, it suffices to show that these $p-1$ extensions are all inequivalent. Suppose we have an equivalence as below with $m, n \in \{1, \ldots, p-1\}$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{mp} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\bmod p} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \cong\,\theta} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \xrightarrow{np} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\bmod p} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0
\end{array}$$

Commutativity of the right square gives $\theta(1) \equiv 1 \bmod p$, so $\theta(1) = 1 + kp$ for some k. Then commutativity of the left square gives

$$np \equiv \theta(mp) \equiv mp\theta(1) \equiv mp(1+kp) \equiv mp + mkp^2 \equiv mp \qquad \bmod p^2$$

Since $m, n < p$, this implies $m = n$.

Remark 1.5.16. Dummit and Foote do the same example where they describe the p distinct extension of $\mathbb{Z}/p\mathbb{Z}$ by itself, except that they write the nontrivial extensions as

$$0 \to \mathbb{Z}/p\mathbb{Z} \xrightarrow{p} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{n \bmod p} \mathbb{Z}/p\mathbb{Z} \to 0$$

where the left map is the inclusion $1 \mapsto p$ and the right map is $x \mapsto nx \bmod p$. As above, this gives $p-1$ inequivalent extensions for $n \in \{1, \ldots, p-1\}$.

Chapter 2

Infinite Galois theory

We assume the reader is already familiar with the Galois correspondence for finite field extensions. If not, there are many sources for this, such as Dummit and Foote [3] and Lang [6].

However, knowledge of finite extensions is insufficient for the ways that we want to describe Brauer groups later. For that, we will need to consider the separable closure of a field. (In the case of characteristic zero, separable closure is the same as algebraic closure.) Occasionally the separable closure is only a finite extension of the base field, such as $\mathbb{C}/\mathbb{R}$. But most of the time, it is an infinite extension. For example, the separable (also algebraic) closure of $\mathbb{Q}$, the separable closure of a finite field, etc.

It is either reasonable or crazy to hope that the Galois correspondence between intermediate subfields and subgroups of the Galois group would extend to the case of an infinite extension. It turns out to be a reasonable hope, for the simple reason that it is true. However, it is not just a verbatim translation of the usual correspondence. Somehow, topology gets involved - the Galois group of an infinite extension is a profinite group, so it is a topological group. Furthermore, this topology captures how much the Galois correspondence differs from the finite case. Specifically, the closed subgroups play a special role.

In this section we mostly follow chapter 7 of Milne [8].

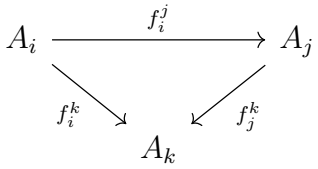
2.1 Direct and inverse limits

Before we can get to the Galois theory, we need to set up some background on direct and inverse limits, since they play a crucial role in discussing the Galois group of an infinite field extension. We will need inverse limits more at this stage, but direct limits are important much later for describing profinite cohomology of infinite Galois groups, so we include the material here.

Definition 2.1.1. A **directed set** is a set I with a partial ordering $\leq$, with the additional property that for every $i, j \in I$, there exists $k \in K$ such that $i \leq k$ and $j \leq k$.

Definition 2.1.2. Let $\mathcal{C}$ be a category and I be a directed set. A **directed system** in $\mathcal{C}$ is a collection of objects $\{A_i | i \in I\}$ and a collection of morphisms $f_i^j : A_i \to A_j$ for $i \leq j$, such

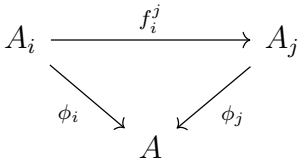
that $f_i^i = \mathrm{Id}_{A_i}$ and for $i \leq j \leq k$ the following diagram commutes.



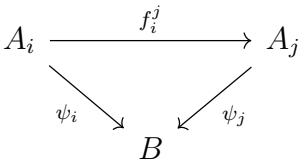
A perhaps useful mnemonic is that we always try to write our morphisms f_i^j so that the "smaller" index (in the sense of the partial order $\leq$) goes on the bottom.

There are usually two approaches when discussing categorical constructions like the direct limit. The first way, which is probably more popular, is to construct or describe the direct limit as an object, and then show that it has a universal property. The second way, which we take here, is to define it using the universal property, and only then show that such an object always exists. I prefer the second method, since it downplays the concrete distinctions between particular categories, and highlights the arrow-theoretic structural properties involved.

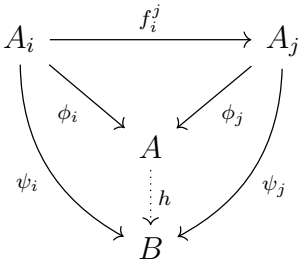
Definition 2.1.3. Let (A_i, f_i^j) be a directed system. A **direct limit** of the system is an object A with morphisms $\phi_i : A_i \to A$ making the following diagram commute,



and also with the following universal property: if B is any object with morphisms $\psi_i : A_i \to B$ making the analogous triangle commute,



then there exists a unique morphism $h : A \to B$ making the following diagram commute.



If A exists, we write $A = \varinjlim A_i$.

Remark 2.1.4. Due to the universal property, if the direct limit exists, it is unique up to isomorphism.

Proposition 2.1.5. *Direct limits exist in the categories of groups, abelian groups, and topological groups. Concretely, in all three, the direct limit of (A_i, f_i^j) is given by*

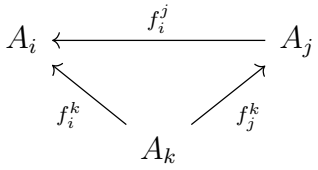
$$\varinjlim A_i = \left(\bigsqcup_{i \in I} A_i \right) / \sim$$

The equivalence relation is described by: for $x_i \in A_i, x_j \in A_j$, $x_i \sim x_j$ if and only if there exists $k \in I$ with $i, j \leq k$ such that $f_i^k(x_i) = f_j^k(x_j)$. (x_i, x_j "eventually become the same".)

Proof. Omitted. □

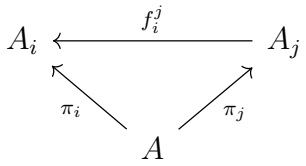
Having discussed direct limits, we now discuss inverse limits. The discussion is essentially the same, with all of the arrows reversed, except for the concrete description of inverse limit in the category of groups.

Definition 2.1.6. Let $\mathcal{C}$ be a category and I a directed set. An **inverse system** or **inversely directed system** is a collection of objects $\{A_i | i \in I\}$ and a collection of morphisms $f_i^j : A_j \to A_i$ for $i \leq j$ such that $f_i^i = \mathrm{Id}_{A_i}$ and that for $i \leq j \leq k$ the following diagram commutes.

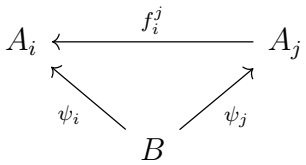


(Note that this is identical to the diagram in the definition of a directed system, with arrows reversed.)

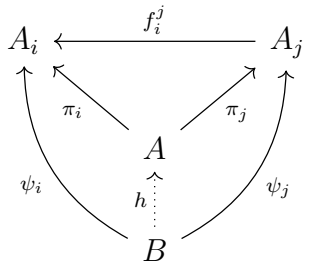
Definition 2.1.7. Let (A_i, f_i^j) be an inversely directed system. An **inverse limit** of the system is a group A with morphisms $\pi_i : A \to A_j$ making the following diagram commute,



and such that A is "universal in this diagram," meaning that if B is another object with morphisms $\psi_i : B \to A_i$ making the analogous triangle commute,



then there is a unique morphism $h : B \to A$ making the following diagram commute.



If the inverse limit A exists, we write $A = \varprojlim A_i$.

Remark 2.1.8. As with direct limits, the universal property ensures that if the inverse limit exists, it is unique up to isomorphism.

Proposition 2.1.9. *Inverse limits exist in the categories of groups, abelian groups, and topological groups. Concretely, in each case the direct limit of (A_i, f_i^j) is given by*

$$\varprojlim A_i = \left\{ (a_i) \in \prod_{i \in I} A_i \;\middle|\; a_i = f_i^j(a_j) \, \forall i \leq j \right\}$$

Proof. Omitted. □

Now that we have existence of direct and inverse limits in the categories we care about, we discuss inducing maps. From a categorical perspective, given a bunch of maps $A_i \to B_i$ between directed (or inverse) systems, there ought to be a canonical way of obtaining a map $\varinjlim A_i \to \varinjlim A_i$ (or $\varprojlim A_i \to \varprojlim B_i$ as the case may be). It turns out that just having maps $A_i \to B_i$ is not sufficient, but this captures the general idea. Now let's give the specifics.

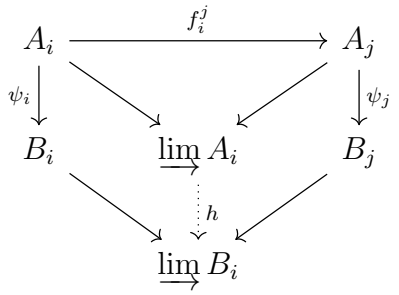
Definition 2.1.10. Let $\mathcal{C}$ be a category and I a directed set. Let (A_i, f_i^j) and (B_i, g_i^j) be directed systems (both using the same directed set I). A **morphism of directed systems** from (A_i, f_i^j) to (B_i, g_i^j) is a collection of morphisms $\psi_i : A_i \to B_i$ making the following squares commute for every $i \leq j$

$$\begin{array}{ccc} A_i & \xrightarrow{\psi_i} & B_i \\ \downarrow{\scriptstyle f_i^j} & & \downarrow{\scriptstyle g_i^j} \\ A_j & \xrightarrow{\psi_j} & B_j \end{array}$$

Definition 2.1.11. A morphism of inverse systems is defined in perfect analogy with the previous definition for directed systems, using an analogous commutative square.

Definition 2.1.12. Let $\psi_i : A_i \to B_i$ be a morphism of directed systems, and assume the direct limits $\varinjlim A_i$ and $\varinjlim B_i$ exist. Then such a morphism induces a morphism $\varinjlim A_i \to \varinjlim B_i$ as follows. Consider the following diagram, where the unlabelled morphisms $A_i \to$

$\varinjlim A_i, B_i \to B \varinjlim B_i$ are the morphisms associated with the direct limit.



By the universal property of direct limits, the dotted arrow h exists and is unique. We call h the direct limit of the maps ψ_i, and write $h = \varinjlim \psi_i$.

Remark 2.1.13. A morphism of inverse systems similarly induces a morphism on the inverse limits.

Remark 2.1.14. In terms of the concrete description of direct limits for groups, the direct limit of morphisms $\psi_i : A_i \to B_i$ is described by

$$\left(\bigsqcup_i A_i\right) / \sim \xrightarrow{\varinjlim \psi_i} \left(\bigsqcup_i B_i\right) / \sim$$

$$\overline{x_i} \longmapsto \overline{\psi_i(x_i)}$$

That is, the class of $x_i \in A_i$ gets mapped to the class of $\psi_i(x_i) \in B_i$.

Exercise 2.1.15. Using the concrete description of inverse limits, describe how the inverse limit of maps acts on the class of an element in the inverse limit.

Proposition 2.1.16. *Let $\mathcal{C}$ be the category of abelian groups, and let $\psi_i : A_i \to B_i$ be a morphism of directed systems. If $x \in \varinjlim A_i$ has a representative $x_i \in A_i$ such that $\psi_i(x_i) = 0$, the $(\varinjlim \psi_i)(x) = 0$. That is,*

$$\overline{\ker \psi_i} \subset \ker \varinjlim \psi_i$$

Proof. Exercise. □

2.2 Profinite groups

"Profinite" is just a fancy name for the inverse limit of a system of finite groups. Our main example of a profinite group will be the Galois group of an infinite field extension L/K. First, we discuss profinite groups in some generality, but the application is useful to keep in mind.

Definition 2.2.1. A **profinite** group is an inverse limit of finite groups. Concretely, if (G_i, ϕ_j^i) is an inverse system of groups indexed by I, the inverse limit is the group

$$\varprojlim G_i = \left\{ (g_i) \in \prod_{i \in I} G_i : \phi_j^i(g_i) = g_j \right\}$$

Giving each finite group G_i the discrete topology and the product topology on $\prod G_i$, the inverse limit is given the subspace topology.

The name "profinite" comes from the fact that profinite groups "behave like" finite groups in some ways, and are "controlled by" their finite quotients and subgroups in meaningful ways. This statement is very imprecise and frustrating at first, but some intuition hopefully develops over time. The closest we will get to making this precise is in Proposition 2.2.5, which says that a profinite group is determined by its finite quotients.

We will also need some general facts about topological groups.

Proposition 2.2.2. *Let G be a topological group.*

1. *An open subgroup of G is also closed. (Every open subgroup is clopen.)*
2. *A closed subgroup of finite index is open.*
3. *If G is compact, every open subgroup has finite index.*

Proof. (1) and (2) are immediate using the facts that cosets of a subgroup partition the group each coset is homeomorphic to the original subgroup. For (3), the cosets partition the group, and they are also open, so there can only be finitely many of them. □

Remark 2.2.3. We summarize the previous result somewhat more pictorially. Let G be a profinite group. Combining the previous two results, a subgroup is open if and only if it is closed and of finite idex.

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\}$$

Additionally, a closed subset of a compact set is compact, and since G is Hausdorff, a compact set is closed. Thus

$$\{\text{closed subgroups}\} = \{\text{compact subgroups}\}$$

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\} = \{\text{compact subgroups of finite index}\}$$

The original definition of profinite group is mostly algebraic and category-theoretic, so it is somewhat surprising that profinite groups can also be characterized entirely topologically, as in the next proposition.

Theorem 2.2.4. *A topological group G is profinite if and only if it is compact, Hausdorff, and totally disconnected.*

Proof. Sharifi 2.1.22 [15]. □

In the next proposition, the last isomorphism is the important one, the only one really worth remembering. Philosophically speaking, it says that a profinite group is determined by all of its finite quotients (the groups G/N are exactly all of the finite quotients, as per Remark open iff closed and finite index). Actually, it says you don't need all of the finite quotients, just enough of of them to determine the topology (in the sense of forming a basis of neighborhoods of the identity).

Proposition 2.2.5. *Let G be a profinite group, and let $\mathcal{U}$ be the collection of all open normal subgroups of G. Let $H \subset G$ be a closed subgroup, and $K \subset G$ a closed normal subgroup. Then we have isomorphisms*

$$G \cong \varprojlim_{N \in \mathcal{U}} G/N \qquad H \cong \varprojlim_{N \in \mathcal{U}} H/(H \cap N) \qquad G/K \cong \varprojlim_{N \in \mathcal{U}} G/(NK)$$

More generally, if $\mathcal{V} \subset \mathcal{U}$ is a set of open normal subgroups that form a basis of open neighborhoods of the identity of G, then

$$G \cong \varprojlim_{N \in \mathcal{V}} G/N$$

Proof. Partial proof in Sharifi [15], but mostly not a proof there either, sorry. □

All right, enough of general profinite group theory, on to the application to infinite Galois extensions.

2.3 Main correspondence for infinite extensions

Let L/K be a Galois extension, and $\mathcal{E}$ be the set of intermediate subfields $K \subset E \subset L$ such that E/K is finite Galois. Then

$$L = \bigcup_{E \in \mathcal{E}} E$$

Additionally, $\mathcal{E}$ is partially ordered by inclusion, and is a directed set, since the compositum EE'/K is a finite Galois extension containing E and E'. If $E \subset E'$, then we have a restriction map $\mathrm{Gal}(E'/K) \to \mathrm{Gal}(E/K)$ by restricting automorphisms of E' to E. This makes the Galois groups $\mathrm{Gal}(E/K)$ into an inversely directed system.

Proposition 2.3.1. *Let L/K be a Galois extension. Then*

$$\mathrm{Gal}(L/K) \to \varprojlim \mathrm{Gal}(E/K) \qquad \sigma \mapsto (\sigma|_E)$$

where E ranges over intermediate subfields $K \subset E \subset L$ such that E/K is finite Galois.

Proof. Exercise for the reader to check that this actually maps into the direct limit, because I feel lazy right now. This is clearly a group homomorphism. It is also clear that the kernel is trivial, since if σ restricts to the identity on each E, it is the identity on L, since $L = \bigcup E$.

All that remains is surjectivity. Consider $(\sigma_E) \in \varprojlim \mathrm{Gal}(E/K)$. Define $\sigma : L \to L$ by $\sigma(x) = \sigma_E(x)$ for $x \in E$. By the compatibility condition of (σ_E) being in the inverse limit, if x lies in two fields E, E' then $\sigma_E(x) = \sigma_{E'}(x) = \sigma_{EE'}(x)$ so this is well defined. Since $L = \bigcup E$, this defines σ on all of L. Clearly σ restricts to σ_E for each E, so (σ_E) is in the image. □

The previous theorem shows that the Galois group of an infinite Galois extension is determined by the Galois groups of finite subextensions. This is very important and will be used very often, because it is often much easier to prove something about a finite group or a finite extension.

Definition 2.3.2. Since the inverse limit has a natural topology as a profinite group, the isomorphism above makes $\mathrm{Gal}(L/K)$ a topological group. In the case where L/K is finite, this is just the discrete topology, but when L/K is infinite, this gives it a nontrivial topology. Whenever L/K is Galois, we assume that $\mathrm{Gal}(L/K)$ has this topology, called the **Krull topology**.

Theorem 2.3.3 (Fundamental theorem of (infinite) Galois theory)**.** *Let L/K be a Galois extension and let $G = \mathrm{Gal}(L/K)$. There is a bijection*

$$\begin{aligned} \{\text{closed subgroups } H \subset G\} &\longleftrightarrow \{\text{intermediate subfields } K \subset E \subset L\} \\ H &\mapsto L^H \\ \mathrm{Gal}(L/E) &\hookleftarrow E \end{aligned}$$

In particular, $L^{\mathrm{Gal}(L/E)} = E$ and $\mathrm{Gal}(L/L^H) = H$. Additionally,

1. *The correspondence is inclusion reversing, i.e. $H_1 \subset H_2 \iff L^{H_1} \supset L^{H_2}$.*
2. *A closed subgroup $H \subset G$ is normal if and only if L^H/K is Galois. In this case,*
$$\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$$
3. *A closed subgroup $H \subset G$ is open if and only if L^H/K is a finite extension. In this case,*
$$[G : H] = [L^H : K]$$

Proof. Various sources. Theorem 7.12 of Milne [8], Theorem 4.1.12 of Gille & Szamuely [4] □

Remark 2.3.4. The usual Galois correspondence for finite extensions is a special case of the above. In the case, every subgroup is closed and open, because G has the discrete topology. So all of the hypotheses involving closed-ness or open-ness of subgroups become vacuous.

2.4 Absolute Galois group

As alluded to in the introduction to this chapter, the main source of infinite Galois field extensions will be the separable closure of a field (and the accompanying absolute Galois group). This sort of approach will later be very useful for computing Brauer groups. Let's see what applying our Galois correspondence for infinite extensions gets us in this scenario.

Definition 2.4.1. Let K be a field. A **separable closure** of K is a field K^{sep} which contains all roots of separable polynomials over K.

Remark 2.4.2. In characteristic zero or for finite fields, separable closure is equal to algebraic closure. The separable closure exists and is unique up to isomorphism. Note that K^{sep}/K is Galois.

Definition 2.4.3. The **absolute Galois group** of K is $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

The first absolute Galois group we should try to compute is for a finite field, since in that situation we know an awful lot about all the possible field extensions. This is the first time we see the usefulness of how the structure of infinite Galois extension is determined by all of its finite subextensions.

Proposition 2.4.4. *Let $K = \mathbb{F}_q$ be a finite field with q elements. Then $G_K \cong \widehat{\mathbb{Z}}$.*

Proof. For each $n \geq 1$, there is a unique finite extension of $\mathbb{F}_q$ of degree n, which is $\mathbb{F}_{q^n}$. Furthermore, the Galois group is

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

The inclusion relation on $\mathbb{F}_{q^n}$ is by divisibility of n, so the inverse system of Galois groups are the groups $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$ ordered by divisibility with quotient maps $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ when $m|n$. This inverse limit of this, as we already know, is $\widehat{\mathbb{Z}}$. □

Definition 2.4.5. Let K be a field, and fix a separable closure K^{sep}. The **maximal abelian extension** of K, denoted K^{ab}, is the maximal subextension of K^{sep} with abelian Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. (This exists because a compositum of abelian extensions is abelian.)

We will not focus too much on the maximal abelian extension in these notes, since it doesn't come up too often in the study of Brauer groups. However, it is a very important object in local class field theory, which has connections to this type of material.

Proposition 2.4.6. *Let K be a field, and let K^{ab} be the maximal abelian extension of K. Then*

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}}$$

Proof. Consider the tower on the left, with corresponding Galois groups on the right.

$$\begin{array}{ccc} K^{\mathrm{sep}} & & \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{sep}}) \\ \uparrow & & \downarrow \\ K^{\mathrm{ab}} & & \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{ab}}) \\ \uparrow & & \downarrow \\ K & & \mathrm{Gal}(K^{\mathrm{sep}}/K) \end{array}$$

By Galois theory,

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \frac{\mathrm{Gal}(K^{\mathrm{sep}}/K)}{\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{ab}})}$$

By definition of K^{ab}, this is the maximal abelian quotient of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, which is, by definition, $\mathrm{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}}$. □

Chapter 3

Group cohomology

Introduction

As the starting point for group cohomology, we will take a group G, an abelian group A, where G acts on A, and associate to it an infinite sequence of cohomology groups $H^0(G,A), H^1(G,A), H^2(G,A), \ldots$

Each $H^i(G,A)$ is an abelian group, and for any fixed $i \in \mathbb{Z}_{\geq 1}$, the association $A \mapsto H^i(G,A)$ is a functor from the category of G-modules to the category of abelian groups. All this means is that if we have a morphism of G-modules $A \to B$, then there is an induced morphism $H^i(G,A) \to H^i(G,B)$. We haven't told you what exactly a G-module or morphism of G-modules is yet, but this gives a flavor.

For those who have seen enough homological algebra to know what the Ext functor is, all $H^i(G,A)$ is is $\mathrm{Ext}_{\mathbb{Z}[G]}(\mathbb{Z},A)$. This is the sophisticated approach, but we will also give more concrete and simpler approaches to defining $H^i(G,A)$.

However, the description via Ext does not capture the interesting aspects of group cohomology. It tells you to expect a long exact sequence and various computations involving projectives and injectives, but much of the power of group cohomology comes from varying not the A argument of $H^i(G,A)$, but instead varying the G entry. As the simplest example, if G acts on A and $H \subset G$ is a subgroup, then H also acts on A, so there are groups $H^i(G,A)$ and $H^i(H,A)$. How are they related? It turns out that they are very related, in the sense that there are functions (called restriction and corestriction) between them which we can sometimes describe very explicitly.

One question we should answer to justify the study of these functors is what more concrete situations do they arise? What are examples of groups acting on abelian groups where the cohomology groups $H^i(G,A)$ capture useful information, or answer questions that we might have had before studying group cohomology altogether?

The primary example that I know of is the following: consider a Galois field extension L/K. The Galois group $G = \mathrm{Gal}(L/K)$ acts on L, but how to view L? It is a field, so there are two immediately obvious abelian groups to consider: first, the additive group $(L,+)$, and second, the multiplicative group $(L^\times,\times)$. Because elements of $\mathrm{Gal}(L/K)$ are field automorphisms of L, there is an action of $\mathrm{Gal}(L/K)$ on both of these groups by taking an automorphism and having it act on a given element of L. Thus there are cohomology

groups $H^i(\mathrm{Gal}(L/K), L)$ and $H^i(\mathrm{Gal}(L/K), L^\times)$.

Ok, we have described a situation in which such a group action arises "in nature," but what does this actually accomplish? Eventually, we will see that the language of these groups gives a convenient way to state and prove a generalized version of Hilbert's Theorem 90, which was originally stated without reference to group cohomology.

As a more important application, one can eventually show that $H^2(\mathrm{Gal}(L/K), L^\times)$ is isomorphic to the "relative Brauer group" of L/K. This is likely utterly unhelpful to a reader trying to learn about group cohomology for the first time, since they probably don't know about Brauer groups. All you need to know at this point is that the Brauer group can be completely described without reference to group cohomology in terms of "central simple algebras" over the field K, and it turns out (the reader may think of this as magic) that somehow this group defined in terms of central simple algebras is the same as a group cohomology group. Using techniques of group cohomology, we can often know much more about the Brauer group than we could if we just tried to stick to the language of algebras.

Lastly, we should say something about the word "cohomology," since it is likely the reader has encountered the word before in a more geometric context, such as differential geometry or algebraic topology. There is a connection between geometric cohomology theories (like de Rham cohomology and singular cohomology), and the purely algebraic group cohomology. First, there is a rough correspondence

$$\begin{aligned} \{\text{topological spaces}\} &\longleftrightarrow \{\text{groups}\} \\ X &\longmapsto \pi_1(X) \\ K(G,1) &\longleftarrow\!\shortmid\ G \end{aligned}$$

As stated, this is very imprecise. We should probably require that X be connected and/or have a basepoint, and the topological spaces side should also be homotopy classes of spaces, rather than spaces. Then perhaps this correspondence makes sense.

The somewhat mysterious part of this is the $K(G,1)$, which is also known as an Eilenberg-MacLane space. This correspondence gives the connection between group cohomology and singular homology as follows: for any abelian group A,

$$H^i(K(G,1), A) \cong H^i(G, A)$$

The left side is singular homology with coefficients in A, and the right side is group cohomology with A viewed as trivial G-module. This is hopefully the last time we will think about homology in topological terms in these notes.

3.1 Group rings

As we mentioned previously, one approach to defining group cohomology groups is with the Ext functor, for which one needs a ring. The relevant ring here is the group ring $\mathbb{Z}[G]$. This group ring will be essential for some other approaches to defining $H^i(G, A)$ as well, so we may as well get familiar with it.

Definition 3.1.1. Let G be a group. The **group ring** of G, denoted $\mathbb{Z}[G]$ or sometimes just $\mathbb{Z}G$, is the set of finite formal linear combinations of elements of g with integer coefficients. These linear combinations are given a ring structure defined in perfect analogy with polynomial addition and multiplication. More explicitly,

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z}, g \in G, \text{ finitely many nonzero terms} \right\}$$

with addition given by

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and multiplication given by

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{\sigma \in G} \left(\sum_{gh = \sigma} a_g b_h \right) \sigma$$

Note that $\mathbb{Z}[G]$ is a module over itself, as is any ring.

Example 3.1.2. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Write G using the presentation

$$G = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1, \sigma\tau = \tau\sigma \rangle$$

The group ring $\mathbb{Z}[G]$ is the set

$$\mathbb{Z}[G] = \{ a + b\sigma + c\tau + d\sigma\tau \mid a, b, c, d \in \mathbb{Z} \}$$

Addition in $\mathbb{Z}[G]$ is works how you would expect. Multiplication also works most as one would expect, except that σ^2 and τ^2 are one. For example,

$$(1 + \sigma)(1 - \sigma) = 1 - \sigma + \sigma - \sigma^2 = 0$$

So $1 + \sigma$ is a zero divisor in $\mathbb{Z}[G]$. This example serves as a warning to avoid assuming much about $\mathbb{Z}[G]$. It is a unital and associative ring, but it is only commutative if G is, and it need not be an integral domain. Even though every element of G is invertible, linear combinations of them need not be units in $\mathbb{Z}[G]$.

Definition 3.1.3. Let G be a group. A **G-module** is a module A over the ring $\mathbb{Z}[G]$. Equivalently, a G-module is an abelian group A with a G-action such that the G-action distributes over addition in A. That is, for $g \in G, a, b \in A$,

$$g(a + b) = ga + gb$$

along with the other usual requirements for a group action, for all $g, h \in G$ and $a \in A$, with e the identity in G,

$$g(ha) = (gh)a \qquad ea = a$$

Alternately, one may think of encoding the G-action on A as a group homomorphism $G \to \mathrm{Aut}(A)$. A **morphism of G-modules** is a morphism of $\mathbb{Z}[G]$-modules.

Definition 3.1.4. A G-module A is **trivial** if the G-action on A is trivial, which is to say, every element of G acts on A by the identity map. That is, if we encode the G-action by a morphism $G \to \mathrm{Aut}(A)$, this is the trivial map.

Note that a trivial module need not be the trivial group, despite the confusing terminology. Any abelian group A may be viewed as a trivial module over any group G.

Definition 3.1.5. Let G be a group and let A be a G-module. The set of G-invariants is the set

$$A^G = \{a \in A \mid ga = a \ \forall g \in G\}$$

If there is a morphism of G-modules $f : A \to B$, then the restriction of f to A^G maps into B^G, so there is an "induced" map $f : A^G \to B^G$. Thus the assignment $A \mapsto A^G$ is a (covariant) functor from the category of G-modules to the category of abelian groups. (We could think of A^G as a G-module, but the G-action is trivial, so this is not so useful.)

Definition 3.1.6. Let G be a finite group. The **norm element** of $\mathbb{Z}[G]$ is

$$N_G = \sum_{g \in G} g$$

Example 3.1.7. Let $G = \mathbb{Z}/n\mathbb{Z}$ be a finite cyclic group with a generator σ. The norm element of $\mathbb{Z}[G]$ is

$$N_G = 1 + \sigma + \sigma^2 + \cdots + \sigma^{n-1}$$

Definition 3.1.8. Let G be a group. The **augmentation map** is the ring homomorphism $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ given by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g$$

It is clearly surjective. The **augmentation ideal** I_G is the kernel of ϵ. Note that I_G is the ideal of $\mathbb{Z}[G]$ generated by elements of the form $g - 1$.

Lemma 3.1.9. *Let G be a group.*

1. *If G is finite, let N_G be the norm element. Then*

$$\mathbb{Z}[G]^G = \mathbb{Z}N_G = \{mN_G \mid m \in \mathbb{Z}\}$$

2. *If G is infinite, $\mathbb{Z}[G]^G = 0$.*

3. *If G is finite, view N_G as a map $\mathbb{Z}[G] \to \mathbb{Z}[G]$. The kernel of this is I_G.*

Proof. (1) The inclusion $\mathbb{Z}N_G \hookrightarrow \mathbb{Z}[G]^G$ is clear. For the reverse inclusion, suppose $x \in \mathbb{Z}[G]^G$. Write x as

$$x = \sum_{g \in G} a_g g$$

For $\sigma \in G$, we have

$$0 = \sigma x - x = \sum_{g \in G} a_g \sigma g - \sum_{g \in G} a_g g = \sum_{g \in G} a_{\sigma^{-1} g} \sigma g - \sum_{g \in G} a_g g = \sum_{g \in G} (a_{\sigma^{-1} g} - a_g) g$$

Thus $a_{\sigma^{-1}g} - a_g = 0$ for every $\sigma \in G$. Since G acts transitively on itself by left multiplication, all the coefficients a_g must be equal. That is, $x \in \mathbb{Z}N_G$.
(2) By the same argument as in (1), an element of $\mathbb{Z}[G]^G$ has all equal coefficients. Since G is infinite, all the coefficients must then be zero, because only finitely many nonzero coefficients are allowed.
(3) To show $I_G \subset \ker N_G$ it suffices to show that $g - 1 \in \ker N_G$ for all $g \in G$. This is a simple computation, which we leave to the reader. For the reverse inclusion, let $x \in \ker N_G$.

$$x = \sum_{g \in G} a_g g$$

Then

$$0 = N_G x = \sum_{h \in G} h \sum_{g \in G} a_g g = \sum_{\sigma \in G} \left(\sum_{hg = \sigma} a_g \right) \sigma$$

Thus

$$\sum_{hg = \sigma} a_g = 0$$

for all $\sigma \in G$. For fixed σ, this sum is equal to $\sum_{g \in G} a_g$, so $\sum_{g \in G} a_g = 0$, which is to say, $x \in \ker \epsilon = I_G$. □

Definition 3.1.10. Let G be a group and A be a G-module. The set of G-coinvariants is

$$A_G = A / I_G A$$

Note that this is not nearly as important as A^G, even though it plays something of a dual role. Similarly as with A^G, a morphism of G-modules $f : A \to B$ induces a morphism $A_G \to B_G$, making the assignment $A \mapsto A_G$ into a functor.

3.1.1 The standard resolution of $\mathbb{Z}$

Definition 3.1.11. Let G be a group and $\mathbb{Z}$ a trivial G-module. Define $d_i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ by

$$d_i(g_0, \ldots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \ldots, \widehat{g}_j, \ldots, g_i)$$

The **standard resolution** of $\mathbb{Z}$ is

$$\cdots \longrightarrow \mathbb{Z}[G^3] \xrightarrow{d_2} \mathbb{Z}[G^2] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

Note that this is exact (exercise to check), and $\mathbb{Z}[G^i]$ is a free $\mathbb{Z}[G]$-module, so this is a projective resolution of $\mathbb{Z}$ in the category of G-modules.

Remark 3.1.12. Warning: $\mathbb{Z}[G^i]$ is not the same as $\mathbb{Z}[G]^i$. $\mathbb{Z}[G]^i$ is a free $\mathbb{Z}[G]$-module of rank i. $\mathbb{Z}[G^i]$ is also a free $\mathbb{Z}[G]$-module, but it only has finite rank if G is finite, and even when it has finite rank, the rank is not necessarily i.

3.2 Definitions of group cohomology

We now define our main object of study, the group cohomology groups $H^i(G, A)$. Or preferably, the real object of interest is the functor $H^i(G, -)$ which takes A to $H^i(G, A)$. We give several equivalent definitions, becuase it is always good to have different ways to think about the same thing. We won't go into all the details of why these are equivalent.

3.2.1 In terms of a projective resolution of $\mathbb{Z}$

Definition 3.2.1. Let G be a group, let A be a G-module, and let

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

be a projective resolution of $\mathbb{Z}$ as a trivial G-module. We apply the contravariant functor $\mathrm{Hom}_{\mathbb{Z}}[G](-, A)$ to this and drop the $\mathbb{Z}$ term to obtain a chain complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, A) \to \cdots$$

Then we define the **ith cohomology group of G with coefficients in A**, denoted $\boldsymbol{H^i(G, A)}$, to be the ith homology of this chain complex.

Due to various standard results in homological algebra, this is independent of the choice of projective resolution, and by Proposition 1.4.6 such resolutions exist in the category of $\mathbb{Z}[G]$-modules. Even better, there is always a free resolution, called the standard resolution, see Definition 3.1.11.

This definition is computationally approachable in some basic cases which are very important, most notably the case where G is cyclic, see section 3.3.1.

3.2.2 As derived functor of G-invariants

Now we give an alternate definition of $H^i(G, A)$ in terms of right derived functors and injective resolutions.

Definition 3.2.2. Note that the functor $A \mapsto A^G$ is left exact (do not waste your time verifying this directly, we will show it in a minute). We denote this functor by $(-)^G$. Then we may form its right derived functors, which we denote by $H^i(G, -)$. Note that it is immediate from this definition that $H^0(G, A) \cong A^G$.

The previous definition is rather hard for someone not familiar with the whole machinery of derived functors, but this is why we provide a few definitions. The functor $(-)^G$ is not so well known, but it turns out to be just another well known functor in disguise, due to the next lemma.

Lemma 3.2.3. *There is a natural isomorphism of (covariant) functors* $(-)^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$.

Proof. For a G-module M, we define a map

$$\Phi_M : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \to M^G \qquad \phi \mapsto \phi(1)$$

First note that the image lands in M^G because for $g \in G, \phi \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$,

$$g \cdot \big(\phi(1)\big) = \phi(g \cdot 1) = \phi(1)$$

since $\mathbb{Z}$ is a trivial G-module. Also note that Φ_M is a morphism of abelian groups, because

$$\Phi_M(\phi + \psi) = (\phi + \psi)(1) = \phi(1) + \psi(1) = \Phi_M(\phi) + \Phi_M(\psi)$$

To show that Φ_M is an isomorphism, we construct an inverse map

$$\Psi_M : M^G \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \qquad \Big(\Psi_M(m)\Big)(1) = m$$

We verify that the composition both ways gives the identity.

$$\Phi_M \Psi_M(m) = \Phi_M(\Psi_M(m)) = \Big(\Psi_M(m)(1)\Big) = m$$
$$\Big(\Psi_M \Phi_M(\phi)\Big)(1) = \Big(\Psi_M(\phi(1))\Big)(1) = \phi(1)$$

Thus Φ_M is an isomorphism. Finally, to check that Φ_M provides an isomorphism of functors, we verify that the following square commutes for any morphism $f : M \to N$ of G-modules.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) & \xrightarrow{f_*} & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, N) \\ \downarrow{\scriptstyle \Phi_M} & & \downarrow{\scriptstyle \Phi_N} \\ M^G & \xrightarrow{\quad f \quad} & N^G \end{array}$$

where $f_*\phi = f\phi$. This is easy to check.

$$\Phi_N f_*(\phi) = \Phi_N(f\phi) = (f\phi)(1) = f(\phi(1)) = f(\Phi_M(1)) = f\Phi_M(\phi)$$

□

Since $\mathrm{Hom}(X, -)$ is left exact for any X, this shows that $(-)^G$ is a left exact functor. The derived functors of Hom are also known by the name Ext^i, so we can write

$$H^i(G, A) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

As noted in the introduction, this characterization has several advantages, notably it implies the existence of a long exact sequence of cohomology groups associated to a short exact sequence of G-modules.

Another advantage is that it tells us that we can compute group homology groups using injective resolutions as well. By Proposition 1.4.6, there is an injective resolution of a G-module A,

$$0 \to A \to I_0 \to I_1 \to \cdots$$

Then applying the (covariant) functor $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ and dropping the A term we obtain a chain complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I_0) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, I_1) \to \cdots$$

and then the ith homology of this complex is $H^i(G, A)$.

3.2.3 Cohomology via cochains

Finally, we give the most hands-on definition of group cohomology using cochains. This is frequently the first definition presented, but we put it last to emphasize the categorical approach of the other definitions. The cochain description is frequently very useful in proofs and especially useful for describing induced maps on cohomology, but it is quite unwieldy to work with in more complicated situations.

Definition 3.2.4. Let A be a G module. For $i \geq 0$, let

$$\boldsymbol{C^i(G,A)} = \left\{ f : G^i \to A \right\}$$

(These are functions with no additional conditions, in particular they are NOT required to be group homomorphisms.) Note that $C^i(G,A)$ is an abelian group via pointwise addition. It is called the group of i-**cochains**. Define $\boldsymbol{d^i_A} : C^i(G,A) \to C^{i+1}(G,A)$ by

$$\begin{aligned} d^i(f)(g_0, g_1, \ldots, g_i) = {} & g_0 f(g_1, \ldots, g_i) \\ & + \sum_{j=1}^{i} (-1)^j f(g_0, \ldots, g_{j-2}, g_{j-1}g_j, g_{j+1}, \ldots, g_i) \\ & + (-1)^{i+1} f(g_0, \ldots, g_{i-1}) \end{aligned}$$

A standard calculation show that $d^{i+1}d^i = 0$, so the groups $C^i(G,A)$ form a chain complex. Define $Z^i(G,A) = \ker d^i$ and $B^i(G,A) = \operatorname{im} d^{i-1}$, and $\boldsymbol{H^i(G,A)} = Z^i(G,A)/B^i(G,A)$. $Z^i(G,A)$ is the group of i-**cocycles**, and $B^i(G,A)$ is the group of i-**boundaries**.

Definition 3.2.5. A G-module homomorphism $\alpha : A \to B$ induces a homomorphism $\alpha^i : C^i(G,A) \to C^i(G,B), f \mapsto \alpha f$. Note that this makes $C^i(G,-)$ a (covariant) functor from G-modules to abelian groups. One can verify that $C^i(G,-)$ is an exact functor.

Note that α^i commutes with the differentials d^i, so α induces a morphism of chain complexes $\alpha^\bullet : C^\bullet(G,A) \to C^\bullet(G,B)$.

$$\begin{array}{ccc} C^i(G,A) & \xrightarrow{d^i_A} & C^{i+1}(G,A) \\ \downarrow{\scriptstyle \alpha^i} & & \downarrow{\scriptstyle \alpha^{i+1}} \\ C^i(G,B) & \xrightarrow{d^i_B} & C^{i+1}(G,B) \end{array}$$

Thus α induces maps on the homology of the respective chain complexes $C^\bullet(G,A), C^\bullet(G,B)$. This is the **induced map on group cohomology** $H^i(G,A) \to H^i(G,B)$. We can describe $H^i(G,A) \to H^i(G,B)$ explicitly as follows: given $\phi \in H^i(G,A)$, choose a representative $\widetilde{\phi} \in \ker d^i_A \subset C^i(G,A)$, which is a map $G^i \to A$. The composition $\alpha\widetilde{\phi} : G^i \to B$ is in $\ker d^i_B$, and the image of ϕ in $H^i(G,B)$ is the class of $\alpha\widetilde{\phi}$.

Remark 3.2.6. There is a natural isomorphism of functors $\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], -) \cong C^i(G,-)$, and these isomorphisms commute with the differentials on the chain complexes $\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{\bullet+1}], A)$ and $C^\bullet(G,A)$, so they induce natural isomorphisms on homology. This provides the final needed equivalence between the definitions of $H^i(G,A)$ in terms of cochains with the definition in terms of projective resolutions, but we omit the details.

3.2.4 Explicit description of cocycles and coboundaries in degrees 0,1,2

Let G be a group and let A be a G-module. We describe $H^0(G,A), H^1(G,A), H^2(G,A)$ as explicitly as possible in terms of cochains, cocycles, and coboundaries. We already know that $H^0(G,A) \cong A^G$, but we want to see why this happens in terms of cochains.

First, we describe the boundary maps d^0, d^1, d^2 of the chain complex of cochains. Let f be a cochain. Depending on the context, f lies in $C^0(G,A), C^1(G,A)$, or $C^2(G,A)$. Let $g_0, g_1, g_2 \in G$.

$$\begin{aligned}(d^0 f)(g_0) &= g_0 f - f \\ (d^1 f)(g_0, g_1) &= g_0 f(g_1) - f(g_0 g_1) + f(g_0) \\ (d^2 f)(g_0, g_1, g_2) &= g_0 f(g_1, g_2) - f(g_0 g_1, g_2) + f(g_0, g_1 g_2) - f(g_0, g_1)\end{aligned}$$

In degree zero, a cochain is a set map $f : G^0 \to A$. Since G^0 is a point, we identify f with a point in A. In degree zero, there is no image to quotient out by, so

$$H^0(G,A) = \ker d^0 = \{f \in A \mid g_0 f = f,\ \forall g_0 \in G\} = A^G$$

which is good, because we already knew this is what it should be. Perhaps this is an abuse of the $=$ sign and we should really write $\cong$, but whatever. In degree one,

$$\begin{aligned}\operatorname{im} d^0 &= \{f : G \to A \mid \exists a \in A,\ f(g_0) = g_0 a - a,\ \forall g_0 \in G\} \\ \ker d^1 &= \{f : G \to A \mid f(g_0 g_1) = g_0 f(g_1) + f(g_0),\ \forall g_0, g_1 \in G\}\end{aligned}$$

Thus we may describe $H^1(G,A)$ as equivalence classes of functions $G \to A$ which satisfy the cocycle condition $f(g_0 g_1) = g_0 f(g_1) + f(g_0)$ with equivalence classes given by considering functions $g \mapsto (g-1)a$ to be zero.

$$H^1(G,A) = \frac{\ker d^1}{\operatorname{im} d^0} = \frac{\{f : G \to A \mid f(g_0 g_1) = g_0 f(g_1) + f(g_0),\ \forall g_0, g_1 \in G\}}{\{f : G \to A \mid \exists a \in A,\ f(g_0) = g_0 a - a,\ \forall g_0 \in G\}}$$

In particular, we notice that if A is a trivial G-module, then the image of d^0 is trivial, since $g_0 a - a = 0$ for all $g_0 \in G, a \in A$, and the kernel of d^1 is the set of group homomorphisms $G \to A$, since $g_0 f(g_1) = f(g_1)$. Since A is abelian, any group homomorphism $G \to A$ factors through the abelianization, so we have proved the following proposition.

Proposition 3.2.7. *Let G be a group and A be a trivial G-module. Then*

$$H^1(G,A) \cong \operatorname{Hom}_{\mathrm{Grp}}(G,A) = \operatorname{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, A)$$

Note that if A is not a trivial G-module, this is far from true.

Degree two is the last place we can reasonably write down the cocycle and coboundary conditions explicitly and hope to have it be useful (even this is of dubious value).

$$\begin{aligned}\operatorname{im} d^1 &= \left\{f : G^2 \to A \mid \exists \widetilde{f} : G \to A,\ f(g_0, g_1) = g_0 \widetilde{f}(g_1) - \widetilde{f}(g_0 g_1) + \widetilde{f}(g_0),\ \forall g_0, g_1 \in G\right\} \\ \ker d^2 &= \left\{f : G^2 \to A \mid g_0 f(g_1, g_2) - f(g_0 g_1, g_2) + f(g_0, g_1 g_2) - f(g_0, g_1) = 0,\ \forall g_0, g_1, g_2 \in G\right\}\end{aligned}$$

$$H^2(G,A) = \frac{\{f : G^2 \to A \mid g_0 f(g_1, g_2) - f(g_0 g_1, g_2) + f(g_0, g_1 g_2) - f(g_0, g_1) = 0,\ \forall g_0, g_1, g_2 \in G\}}{\left\{f : G^2 \to A \mid \exists \widetilde{f} : G \to A,\ f(g_0, g_1) = g_0 \widetilde{f}(g_1) - \widetilde{f}(g_0 g_1) + \widetilde{f}(g_0),\ \forall g_0, g_1 \in G\right\}}$$

3.3 Cohomology for cyclic groups

With our definitions in hand, we set out to do some calculations. We should at least be able to calculate some cohomology groups in simple cases, like when G is uncomplicated (such as G being cyclic) or when the G-action on A is trivial.

The case of G being cyclic can be done about as explicitly as possible. Somewhat surprisingly, even when G acts trivially on A, $H^2(G, A)$ and higher cohomology groups do not have a very simple description.

3.3.1 Cohomology of a finite cyclic group

Proposition 3.3.1. *Let $G = \mathbb{Z}/n\mathbb{Z}\langle\sigma\rangle$ be a finite cyclic group of order n with generator σ, and let A be a G-module. Let*

$$N_G = \sum_{g\in G} g = \sum_{i=0}^{n-1} \sigma^i = 1 + \sigma + \cdots + \sigma^{n-1}$$

be the norm element of $\mathbb{Z}[G]$, which we also view as a map $N_G : A \to A$. Then

$$H^i(G, A) = \begin{cases} A^G & i = 0 \\ \ker N_G/(\sigma - 1)A & i = 1, 3, \ldots, \\ A^G/N_G A & i = 2, 4, \ldots \end{cases}$$

Proof. We denote N_G by N. We have the following periodic projective (actually free) resolution of the trivial G-module $\mathbb{Z}$, where ϵ is the augmentation map, characterized by $\sigma \mapsto 1$ and $\mathbb{Z}$-linearity.

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

It is immediate to check that this is a chain complex, and not terribly hard to check that it is in fact exact. Then we apply $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A)$ and drop the $\mathbb{Z}$ term to obtain a complex whose homology is $H^i(G, A)$.

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{(\sigma-1)_*} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{N_*} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \xrightarrow{(\sigma-1)_*} \cdots$$

Since $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$ via $\phi \mapsto \phi(1)$, we have an isomorphism of chain complexes

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xrightarrow{(\sigma-1)_*} & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xrightarrow{N_*} & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xrightarrow{(\sigma-1)_*} & \cdots \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \longrightarrow & A & \xrightarrow{\sigma-1} & A & \xrightarrow{N} & A & \xrightarrow{\sigma-1} & \cdots \end{array}$$

The maps on the bottom row of A's are determined by commutativity of this diagram, and thinking about the exact description of the isomorphism $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$ says that

they must be as written. Thus

$$H^i(G,A) = \begin{cases} \ker(\sigma - 1) & i = 0 \\ \ker N/(\sigma - 1)A & i = 1, 3, \dots \\ \ker(\sigma - 1)/NA & i = 2, 4, \dots \end{cases}$$

Since the G-action is determined by the action of σ, we see that $\ker(\sigma - 1) = A^G$, hence the result. □

Corollary 3.3.2. *Let $G = \mathbb{Z}/n\mathbb{Z}\langle\sigma\rangle$ be a finite cyclic group and A a trivial G-module. Then*

$$H^i(G,A) = \begin{cases} A & i = 0 \\ {}_nA & i = 1, 3, \dots, \\ A/nA & i = 2, 4, \dots \end{cases}$$

where ${}_nA$ is the n-torsion subgroup of A.

Proof. Since A is a trivial module, $A^G = A$, and the norm element just acts by multiplication by $|G| = n$ on A, and $(\sigma - 1)A = 0$, so the result is immediate from the previous calculation. □

As a somewhat interesting application of the previous calculations, we have a cohomology calculation for a matrix group.

Proposition 3.3.3. *Let p be a prime, and consider $M = \mathbb{F}_p^2$ (viewed as column vectors) with the standard action from $\mathrm{GL}_2(\mathbb{F}_p)$ (by left matrix multiplication). For any subgroup $G \subset \mathrm{GL}_2(\mathbb{F}_p)$, $H^1(G,M)$ has order 1 or order p. If $p = 2$, then the order is 1.*

Proof. Let $G_p \subset G$ be a Sylow p-subgroup. Note that since the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2 - p)(p^2 - 1) = p(p-1)^2(p+1)$, any Sylow p-subgroup has order p or 1.

Because $pM = 0$, $H^1(G,M)$ is a p-torsion group. Since $\mathrm{Res} : H^1(G,M) \to H^1(G_p,M)$ is injective on the p-primary component (Corollary 1.8.24 of Sharifi [15]), this says that $\mathrm{Res} : H^1(G,M) \to H^1(G_p,M)$ is injective.

If $G_p = 0$, then $H^1(G,M) = H^1(G_p,M) = 0$ and there is nothing to prove, so suppose G_p has order p. Since all p-Sylow subgroups are conjugate, G_p is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to the cyclic unipotent subgroup U generated by

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Then $G_p \cong U$ so $H^1(G_p,M) \cong H^1(U,M)$. So to show that $H^1(G,M)$ has order 1 or p, it suffices to show that $H^1(U,M)$ has order 1 or p (since the restriction map embeds $H^1(G,M)$ into $H^1(G_p,M) \cong H^1(U,M)$). Since U is fintie cyclic (of order p), by the computation of cohomology for finite cyclic groups,

$$H^1(U,M) \cong \ker N/(u-1)M$$

where $N = 1 + u + \cdots + u^{p-1} \in \mathrm{Mat}_2(\mathbb{F}_p)$ is the norm map. For p odd,

$$N = \sum_{k=0}^{p-1} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p & \frac{p(p-1)}{2} \\ 0 & p \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

For $p = 2$,

$$N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

So for p odd, $\ker N = \mathbb{F}_p^2$, and for p even, $\ker N = \mathbb{F}_p = \mathbb{F}_p e_1$, generated (as a U-module) by $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The other part we need for $H^1(U, M) \cong \ker N/(u-1)M$ is $(u-1)M$, which is $\mathbb{F}_p e_1$. Thus we obtain

$$H^1(U, M) = \begin{cases} 0 & p = 2 \\ \mathbb{F}_p & p > 2 \end{cases}$$

□

Remark 3.3.4. The previous proof says a little bit more than the proposition asserts. It says that if p is odd and $G \subset \mathrm{GL}_2(\mathbb{F}_p)$ is a Sylow p-subgroup (so it has order p), then $H^1(G, M) \cong \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

It also says that if p does not divide the order of $G \subset \mathrm{GL}_2(\mathbb{F}_p)$, then $H^1(G, M) = 0$, since $G_p = 0$ and $H^1(G_p, M) = 0$. On the other hand, if p does divide the order of G, all the proof tells us is that $H^1(G, M)$ embeds into $H^1(G_p, M) = \mathbb{Z}/p\mathbb{Z}$, so $H^1(G, M)$ may be zero or $\mathbb{Z}/p\mathbb{Z}$, we don't know for sure. Perhaps other methods exist to sharpen this, but this proof does not accomplish this.

3.3.2 Cohomology of infinite cyclic group

After our success with finite cyclic groups, the infinite cyclic group seems a likely target for the next attack.

Lemma 3.3.5. *Let G be a group and let $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ be the augmentation map,*

$$\epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \qquad a_g \in \mathbb{Z}$$

The kernel of ϵ is equal to the ideal $I_G \subset \mathbb{Z}[G]$ generated by elements $g - 1$ for $g \in G$.

Proof. It is clear that for $g \in G$, $\epsilon(g-1) = 0$ so $I_G \subset \ker \epsilon$. Conversely, if $x = \sum a_g g \in \ker \epsilon$, then

$$0 = \epsilon\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g \implies \sum_{g \in G} a_g g = \sum_{g \in G} a_g g - \sum_{g \in G} a_g = \sum_{g \in G} a_g (g - 1)$$

so $x \in I_G$. □

Remark 3.3.6. The previous lemma works in a more general setting which we will only rarely need. Replacing $\mathbb{Z}$ with an arbitrary commutative unital ring R, we can form a group ring $R[G]$, and an augmentation map

$$\epsilon : R[G] \to R \qquad \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$$

Then by the same argument as above, the kernel of ϵ is exactly the ideal of $R[G]$ generated by elements $g - 1$.

Proposition 3.3.7. *Let G be an infinite cyclic group with generator σ. Then*

$$0 \to \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

is a free resolution of $\mathbb{Z}$ as trivial $\mathbb{Z}[G]$-module. Thus

$$H^i(G, A) = \begin{cases} A^G & i = 0 \\ A/(\sigma - 1)A & i = 1 \\ 0 & i \geq 2 \end{cases}$$

Proof. It is clear that ϵ is surjective. To verify injectivity, suppose $x = \sum_{g\in G} a_g g = \sum_{i\in\mathbb{Z}} a_i \sigma^i \in \ker(\sigma - 1)$. Since $\sigma x - x = 0$, all the coefficients of x must be the same. Since x can have only finitely many nonzero coefficients, they must all be zero. Regarding exactness at the middle term, in the language of the previous lemma, $\ker \epsilon = I_G$. Since G is cyclic, I_G is generated by $\sigma - 1$, which is to say, I_G is the image of $\sigma - 1$, so the sequence is exact.

From this resolution, we apply $\mathrm{Hom}_{\mathbb{Z}[G]}(-, A)$ and drop the $\mathbb{Z}$ term to obtain a complex whose homology is $H^i(G, A)$. We also have canonical isomorphisms $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) \cong A$, which gives an isomorphic complex whose homology is easier to read off.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \xrightarrow{(\sigma-1)^*} & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], A) & \longrightarrow & 0 \\ & & \downarrow\cong & & \downarrow\cong & & \\ 0 & \longrightarrow & A & \xrightarrow{\sigma-1} & A & \longrightarrow & 0 \end{array}$$

From the bottom complex, we read off

$$H^i(G, A) = \begin{cases} \ker(\sigma - 1) = A^G & i = 0 \\ A/(\sigma - 1)A & i = 1 \\ 0 & i \geq 2 \end{cases}$$

□

3.4 Long exact sequence of cohomology

We have alluded to the long exact sequence for too long without stating it, so here it is.

Theorem 3.4.1. *Let G be a group and let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Then there is a long exact sequence*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to \cdots$$

where the maps $H^i(G, A) \to H^i(G, B) \to H^i(G, C)$ are the usual induced maps on cohomology.

Proof. Fix a projective resolution $P_\bullet \to \mathbb{Z} \to 0$. Then we have a short exact sequence of chain complexes

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, A) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, B) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, B) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, B) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, C) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, C) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, C) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The columns are exact since P_i is a projective $\mathbb{Z}[G]$-module. Note that the homology of the chain complex rows is exactly $H^i(G, A), H^i(G, B), H^i(G, C)$ by definition of group cohomology. Thus applying Proposition 1.3.1, we obtain the desired long exact sequence. □

Remark 3.4.2. There is an analogous long exact sequence for group homology (this will make sense only after we define group homology, but it is convenient to talk about this here). Given a short exact sequence of G-modules $0 \to A \to B \to C \to 0$, there is a long exact sequence

$$\cdots \to H_1(G, C) \to H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0$$

3.5 $H^2(G, A)$ and group extensions

We have seen that in degree zero, $H^0(G, A)$ is just A^G. We also saw that when G acts trivially on A, $H^1(G, A)$ is just $\mathrm{Hom}(G, A)$ (Proposition 3.2.7). The next goal is to describe a somewhat analogous description of $H^2(G, A)$, using something more tangible than cocycles.

Definition 3.5.1. Let G be a group and A be a G-module. Consider a short exact sequence of groups

$$1 \to A \to E \to G \to 1$$

By assumption, A has some action of G. Since $A \subset E$ is the kernel of a group homomorphism, A is a normal subgroup so there is the conjugation action

$$E \times A \to A \qquad e \cdot a = eae^{-1}$$

which factors through E/A to induce an action

$$\big(G \cong E/A\big) \times A \to A \qquad \overline{e} \cdot a = eae^{-1}$$

We call the exact sequence $1 \to A \to E \to G \to 1$ an **extension of G by A** if these two G-actions coincide.

Example 3.5.2. The previous definition is unfortunately cumbersome, but in the case where A is a trivial G-module we may simplify it greatly. In this case the G-action on A is just

$$G \times A \to A \qquad g \cdot a = a$$

so the requirement for the actions to agree just means that

$$E \times A \to A \qquad e \cdot a = eae^{-1} = a$$

which is equivalent to saying that the image of A under $A \to E$ is contained in the center of E.

Definition 3.5.3. Let G be a group and A be a G-module. Two extensions E, E' of G by A (in the sense of Definition 3.5.1) are **isomorphic** if there is an isomorphism of short exact sequences as depicted below.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

The set of isomorphism classes of such extensions is denoted $\mathrm{Ext}(G, A)$. An extension is **split** if there is a group homomorphism $G \to E$ so that the composition $G \to E \to G$ is the identity on G (this is equivalent to E being the semidirect product of G and A, utilizing the G-action on A for the semidirect product).

The set $\mathrm{Ext}(G, A)$ has a "natural" structure of an abelian group given by Baer sum, which we neglect to describe in detail at this time. However, we do note that the identity element of this group is the isomorphism class of the split extension.

Theorem 3.5.4. *Let G be a group and A a G-module. There is an isomorphism of groups $H^2(G, A) \cong \mathrm{Ext}(G, A)$.*

Proof. A description of the correspondence as sets (ignoring group structures) is given in Example 3.2.6 of Gille & Szamuely [4], who also refer the reader to Section 6.6 of Weibel [16] for more details. A detailed proof and description of Baer sum in the case where A is a trivial G-module is given in Theorem 4.1.16 of Rosenberg [13]. □

Corollary 3.5.5. *Let G be a group and A a trivial G-module. Then every central extension of G by A is split if and only if $H^2(G, A) = 0$.*

Proof. Immediate consequence of Theorem 3.5.4. □

3.5.1 Application - a special case of the Schur-Zassenhaus theorem

The general Schur-Zassenhaus theorem is the following.

Theorem 3.5.6. *Let G be a finite group with $H \subset G$ a normal subgroup with $\gcd(|H|, |G/H|) = 1$. Then G is isomorphic to a semidirect product of H and G/H.*

In this section we will use the correspondence between H^2 and group extensions to prove this in the special case where H is abelian (Proposition 3.5.9).

Lemma 3.5.7 (Coprime order makes cohomology trivial)**.** *Let G be a finite group of order n and A be a G-module which is a finite abelian group of order m, such that $\gcd(n, m) = 1$. Then for $i \geq 1$,*

$$H^i(G, A) = 0$$

Proof. Since elements of $H^i(G, A)$ are represented by cocycles which are functions $G^i \to A$, it is clear that $H^i(G, A)$ is a finite group. From the $\mathrm{Cor} \circ \mathrm{Res}$ composition (Proposition 3.9.17), we know that $H^i(G, A)$ is annihilated by the order of G. It is also clear that a function $G^i \to A$ is annihilated by the order of A. Thus $H^i(G, A)$ is annihilated by $\gcd(n, m) = 1$, which is to say, it is the trivial group. □

Remark 3.5.8. Let G be a group with abelian normal subgroup H. The conjugation action of G on H induces an action of G/H on H, described explicitly by

$$G/H \times H \to H \qquad gH \cdot h = ghg^{-1}$$

where g is any coset representative of gH. Since H is normal, $ghg^{-1} \in H$. We verify that this is well defined. Let $g, g' \in gH$, so $g^{-1}g' \in H$. Then

$$(g^{-1}g')h(g^{-1}g')^{-1} = h \implies ghg^{-1} = g'h(g')^{-1}$$

The equality on the left uses the fact that $g^{-1}g' \in H$ and that H is abelian.

Proposition 3.5.9 (Special case of Schur-Zassenhaus)**.** *Let G be a finite group with $H \subset G$ an **abelian** normal subgroup with $\gcd(|H|, |G/H|) = 1$. Then G is isomorphic to a semidirect product of H and G/H.*

Proof. Using Remark 3.5.8, H is a G/H-module. Since H is abelian, by the correspondence between H^2 and group extensions, elements of $H^2(G/H, H)$ correspond to isomorphism classes of extensions

$$1 \to H \to E \to G/H \to 1$$

and furthermore such an extension is split by a group homomorphism $G/H \to E$ if and only if the corresponding class in $H^2(G/H, H)$ is trivial, which by the splitting lemma for groups is equivalent to saying that E is a semidirect product of H and G/H. One obvious choice of such an extension is

$$1 \to H \to G \to G/H \to 1$$

where $H \hookrightarrow G$ is the inclusion and $G \to G/H$ is the quotient map. (A little thought verifies that this satisfies the compatibility between the two possible G-actions as required in Definition 3.5.1.) Since $\gcd(|H|, |G/H|) = 1$, by Proposition 3.5.7, $H^2(G/H, H) = 0$, so the extension G must correspond to the trivial element, which is to say, it is split and G is isomorphic to a semidirect product of H and G/H. □

3.6 Group homology

While we are primarily focused on group cohomology, it will be useful to know about group homology as well. If the reader has heard of Ext functors, they have probably seen Tor as well. The relationship between group cohomology and group homology is very analoguous to the relationship between Ext and Tor.

While we could give a longer description of various equivalent definitions of group homology, the discussion would be much the same in flavor as that for group cohomology. Since we won't work with homology as much, we shorten the discussion.

3.6.1 Definition of group homology

Definition 3.6.1. Let G be a group and A a $\mathbb{Z}$-module. We define

$$H_i(G, A) = \operatorname{Tor}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

$H^i(G, A)$ is called the i**th homology group of** G **with coefficients in** A. That is, $H_i(G, -)$ is the ith right derived functor of the left exact covariant functor $- \otimes_{\mathbb{Z}[G]} A$.

Remark 3.6.2. Having defined $H_i(G, A)$ in terms of Tor, we have the usual method of computation. Take a projective resolution of $\mathbb{Z}$ by G-modules (possibly the standard resolution 3.1.11),

$$\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

Apply the (covariant) functor $- \otimes_{\mathbb{Z}[G]} A$ and drop the $\mathbb{Z}$ term to obtain a chain complex

$$\cdots \to P_2 \otimes_{\mathbb{Z}[G]} A \to P_1 \otimes_{\mathbb{Z}[G]} A \to P_0 \otimes_{\mathbb{Z}[G]} A \to 0$$

Then the ith homology of this complex is $H_i(G, A) = \operatorname{Tor}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Alternatively, since tensor and Tor are symmetric up to natural isomorphism, we can start with a projective resolution of A by G-modules,

$$\cdots \to P_1 \to P_0 \to A \to 0$$

and apply the (covariant) functor $\mathbb{Z} \otimes_{\mathbb{Z}[G]} -$ and drop the A term to obtain a chain complex whose homology is also $H_i(G, A)$.

$$\cdots \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_2 \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_1 \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} P_0 \to 0$$

Definition 3.6.3. Let A be a G-module. We define $A_G = A/I_G A$, that is, the maximal quotient of A fixed by G. A_G is called the group of G**-coinvariants**. Note that $\mathbb{Z}[G]_G \cong \mathbb{Z}[G]/I_G \cong \mathbb{Z}$.

Remark 3.6.4. In analogy with Lemma 3.2.3, there is a natural isomorphism of functors $(-)_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} (-)$, which means that we could have alternatively defined $H_i(G, -)$ as the right derived functors of $(-)_G$. One consequence of this is that $H_0(G, A) \cong A_G$.

Definition 3.6.5. The group $H_2(G, \mathbb{Z})$ is the **Schur multiplier** of the group G.

Schur multiplier groups will not be important for the rest of these notes on group cohomology. We just note this here because of the connection with algebraic K-theory, which is the following: For a ring R, the Schur multiplier of the matrix group $\mathrm{E}(R)$ can be identified with $\mathrm{K}_2(R)$, see Corollary 5.5.21.

3.6.2 Group homology for cyclic group

We essentially repeat the calculation for group cohomology when G is cyclic, except for homology.

Proposition 3.6.6. *Let G be a finite cyclic group with generator σ and let A be a G-module. Then*

$$H_i(G,A) = \begin{cases} A/(\sigma-1)A & i=0 \\ A^G/N_G A & i=1,3,\cdots \\ \ker N_G/(\sigma-1)A & i=2,4,\cdots \end{cases}$$

Proof. We start with the same projective resolution of $\mathbb{Z}$ as in the calculation of cohomology for finite cyclic G (Proposition **??**).

$$\cdots \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N_G} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

then apply (covariant) $- \otimes_{\mathbb{Z}[G]} A$ and drop the $\mathbb{Z}$ term. Similar to before, we have very convenient isomorphisms.

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{\sigma-1\otimes \mathrm{Id}_A} & \mathbb{Z}[G]\otimes_{\mathbb{Z}[G]} A & \xrightarrow{N_G\otimes \mathrm{Id}_A} & \mathbb{Z}[G]\otimes_{\mathbb{Z}[G]} A & \xrightarrow{\sigma-1\otimes \mathrm{Id}_A} & \mathbb{Z}[G]\otimes_{\mathbb{Z}[G]} A & \longrightarrow & 0 \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\ \cdots & \xrightarrow{\sigma-1} & A & \xrightarrow{N_G} & A & \xrightarrow{\sigma-1} & A & \longrightarrow & 0 \end{array}$$

From this, we read off the homology and it is exactly what we claimed. Note that $\ker(\sigma-1) = A^G$. □

3.6.3 $H_1(G,\mathbb{Z}) \cong G^{\mathrm{ab}}$

There isn't much suspense here - the section title gives it all away. We will give a description of $H_1(G,\mathbb{Z})$ in the case where G is any group, and $\mathbb{Z}$ is a trivial G-module. I like to think of this as a dual/companion result to the isomorphism

$$H^1(G,A) \cong \mathrm{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, A)$$

from Proposition 3.2.7.

Proposition 3.6.7. *Let G be a group and view $\mathbb{Z}$ as a trivial G-module. Then*

$$H_1(G,\mathbb{Z}) \cong I_G/I_G^2 \cong G^{\mathrm{ab}}$$

Proof. Consider the short exact sequence of G-modules

$$0 \longrightarrow I_G \hookrightarrow \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

Since $\mathbb{Z}[G]$ is a free (hence flat) $\mathbb{Z}[G]$-module, $H_1(G,\mathbb{Z}[G]) = 0$, so the low degree part of the associated long exact sequence on homology is

$$0 \longrightarrow H_1(G,\mathbb{Z}) \xrightarrow{\delta} H_0(G,I_G) \longrightarrow H_0(G,\mathbb{Z}[G]) \xrightarrow{\epsilon_*} H_0(G,\mathbb{Z}) \longrightarrow 0$$

In a more useful form, these terms are

$$H_0(G, I_G) = (I_G)_G = I_G/I_G^2$$
$$H_0(G, \mathbb{Z}[G]) = \mathbb{Z}[G]_G = \mathbb{Z}[G]/I_G \cong \mathbb{Z}$$
$$H_0(G, \mathbb{Z}) = \mathbb{Z}_G = \mathbb{Z}/I_G\mathbb{Z} = \mathbb{Z}$$

Since ϵ vanishes on I_G, the induced map $\epsilon_* : \mathbb{Z}[G]/I_G \to \mathbb{Z}$ is an isomorphism. Then by exactness, the connecting homomorphism δ gives an isomorphism

$$H_1(G, \mathbb{Z}) \cong I_G/I_G^2$$

Now we show $I_G/I_G^2 \cong G^{\text{ab}}$. Consider the map

$$\phi : G \to I_G/I_G^2 \qquad g \mapsto \overline{g-1}$$

This is a group homomorphism because

$$\begin{aligned}\phi(gh) &= \overline{gh-1} = \overline{gh-1} - \overline{(g-1)(h-1)} \\ &= \overline{gh-1-gh+g+h-1} = \overline{g-1} + \overline{h-1} \\ &= \phi(g) + \phi(h)\end{aligned}$$

Furthermore, since I_G/I_G^2 is an abelian group, ϕ vanishes on the commutator subgroup $[G, G]$ and induces a homomorphism

$$\overline{\phi} : G^{\text{ab}} \to I_G/I_G^2 \qquad \overline{g} \mapsto \overline{g-1}$$

To show this is an isomorphism, we construct an inverse map. Since I_G is the free $\mathbb{Z}$-module generated by elements $g-1$ for $g \in G$, the assignment

$$\psi : I_G \to G^{\text{ab}} \qquad g-1 \mapsto \overline{g}$$

extends to a group homomorphism by $\mathbb{Z}$-linearity. Now note that for $g, h \in G$, we have

$$(g-1)(h-1) = gh - g - h + 1 = (gh-1) - (g-1) - (h-1)$$

Applying ψ to both sides of the equation we obtain

$$\psi\Big((g-1)(h-1)\Big) = ghg^{-1}h^{-1}$$

Thus ψ vanishes on I_G^2, and induces a map

$$\overline{\psi} : I_G/I_G^2 \to G^{\text{ab}} \qquad \overline{g-1} \mapsto \overline{g}$$

It is clear that $\overline{\phi}, \overline{\psi}$ are inverses, so $G^{\text{ab}} \cong I_G/I_G^2$. □

This gives a nice criterion for a group to be perfect in terms of homology. This turns out to be useful in the context of algebraic K-theory.

Definition 3.6.8. A group G is **perfect** if $G = [G, G]$.

Corollary 3.6.9. *A group G is perfect if and only if $H_1(G, \mathbb{Z}) = 0$.*

Proof. By Theorem 3.6.7, $H_1(G, \mathbb{Z}) \cong G^{\text{ab}} = G/[G, G]$, so

$$G = [G, G] \iff G^{\text{ab}} = 0 \iff H_1(G, \mathbb{Z}) = 0$$

□

3.6.4 Universal coefficient theorem and Kunneth formula

The next theorem says that the module $\mathbb{Z}$, viewed as trivial G-module, does a lot to "control" other cohomology groups $H^i(G, A)$. So $\mathbb{Z}$ is a sort of "universal coefficient" module.

Theorem 3.6.10 (Universal coefficient theorem)**.** *Let G be a group and A be a trivial G-module. Then for $k \in \mathbb{Z}_{\geq 1}$, there is a split short exact sequence*

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(H_{k-1}(G, \mathbb{Z}), A) \to H^k(G, A) \to \mathrm{Hom}_{\mathbb{Z}}(H_k(G, \mathbb{Z}), A) \to 0$$

Proof. Rosenberg [13] 4.1.13. □

Theoretically speaking, the universal coefficient theorem says that group cohomology $H^i(G, A)$ is entirely determined by group homology (in the case where G acts trivially on A). Since the sequence is split, the middle term is isomorphic to the direct sum of the outer terms, which depend only on group homology.

Even more, the module A is mostly irrelevant, since it suffices to compute group homology groups with the module $\mathbb{Z}$. The module $\mathbb{Z}$ is the group of "universal coefficients," whence the name of the theorem. So one could maybe think that we could forget about group homology, and just work with groups acting trivially on $\mathbb{Z}$, and see what happens.

While this has some interesting theoretical value, in practice it is still much nicer to actually work in group cohomology. First of all, not all modules are trivial, in fact, the primary example we gave in the introduction of a Galois group acting on the top field of a field extension is not a trivial module, and this is a central motivating example. Secondly, group homology and Ext and Hom groups are not necessarily that much easier to calculate that cohomology groups.

Nevertheless, the universal coefficient theorem is often useful, especially the fact that the exact sequence is split. The next corollary provides an example of this.

Corollary 3.6.11. *Let G be a group. Then $H^2(G, A) = 0$ for all trivial G-modules A if and only if G^{ab} is free abelian and $H_2(G, \mathbb{Z}) = 0$.*

Proof. Consider the split short exact sequence of the universal coefficient theorem 3.6.10 in the case $k = 2$.

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}(H_1(G, \mathbb{Z}), A) \to H^2(G, A) \to \mathrm{Hom}_{\mathbb{Z}}(H_2(G, \mathbb{Z}), A) \to 0$$

Since this is split, $H^2(G, A)$ is isomorphic to the direct sum of the outer terms, so $H^2(G, A)$ vanishes if and only if both outer terms vanish. By Theorem 3.6.7, $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$. Thus

$$\mathrm{Ext}^1_{\mathbb{Z}}(H_1(G, \mathbb{Z}), A) = \mathrm{Ext}^1_{\mathbb{Z}}(G^{\mathrm{ab}}, A)$$

which vanishes for all A if and only if G^{ab} is a projective $\mathbb{Z}$-module, which is to say, if and only if G^{ab} is free abelian[1]. Similarly,

$$\mathrm{Hom}_{\mathbb{Z}}(H_2(G, \mathbb{Z}), A)$$

vanishes for all A if and only if $H_2(G, \mathbb{Z}) = 0$. □

[1]Since projective $\iff$ free for modules over a PID, such as $\mathbb{Z}$.

Both the universal coefficient theorem and the Kunneth formula, which is next, originally arose in the context of algebraic topology, to the best of my knowledge. They turn out to be true in the more purely algebraic group cohomology context as well.

Theorem 3.6.12 (Kunneth formula)**.** *Let G_1, G_2 be groups and M an abelian group, viewed as a trivial module over $G_1, G_2, G_1 \times G_2$. Then*

$$H_n(G_1 \times G_2, M) \cong \left(\bigoplus_{i+j=n} H_i(G_1, M) \otimes H_j(G_2, M) \right) \oplus \left(\bigoplus_{i+j=n-1} \operatorname{Tor}_{\mathbb{Z}}^1 \Big(H_i(G_1, M), H_j(G_2, M) \Big) \right)$$

Proof. Unfortunately, I do not know a good source for this. □

The next computation gives an example usage of the universal coefficient theorem and Kunneth formula.

Proposition 3.6.13 (Rosenberg [13] Exercise 4.1.26)**.** *Let $G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and view $\mathbb{Z}$ as a trivial G-module.*

1. $H_1(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
2. $H_2(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$
3. $H^2(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Proof. For (1), we apply the Kunneth formula, and our computation of cohomology for finite cyclic groups, and various standard facts about Ext and Tor.

$$\begin{aligned}
H_1\Big((\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}\Big) &\cong \Big(H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \otimes H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \Big(H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \otimes H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \operatorname{Tor}_{\mathbb{Z}}^1 \Big(H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\cong \Big(\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \Big) \oplus \Big(\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \Big) \oplus \operatorname{Tor}_{\mathbb{Z}}^1(\mathbb{Z}, \mathbb{Z}) \\
&\cong (\mathbb{Z}/2\mathbb{Z})^2
\end{aligned}$$

For (2) we again use the Kunneth formula.

$$\begin{aligned}
H_2\Big((\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}\Big) &\cong \Big(H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \otimes H_2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \Big(H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \otimes H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \Big(H_2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \otimes H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \operatorname{Tor}_{\mathbb{Z}}^1 \Big(H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}), H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\quad \oplus \operatorname{Tor}_{\mathbb{Z}}^1 \Big(H_1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}), H_0(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \Big) \\
&\cong (\mathbb{Z} \otimes 0) \oplus (\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}) \oplus (0 \otimes \mathbb{Z}) \\
&\quad \oplus \operatorname{Tor}_{\mathbb{Z}}^1(\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \oplus \operatorname{Tor}_{\mathbb{Z}}^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \\
&\cong \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \\
&\cong \mathbb{Z}/2\mathbb{Z}
\end{aligned}$$

For (3), the universal coefficient theorem gives a split exact sequence

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}}((\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/2\mathbb{Z}) \to H^2(V, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \to 0$$

Clearly $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$. By a well-known computation, the Ext term is

$$\mathrm{Ext}^1_{\mathbb{Z}}((\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \oplus \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}2/\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^2$$

Thus we have a split exact sequence

$$0 \to (\mathbb{Z}/2\mathbb{Z})^2 \to H^2(V, \mathbb{Z}/2\mathbb{Z}) \to \mathbb{Z}/2\mathbb{Z}) \to 0$$

hence $H^2(V, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})^3$. □

3.7 Tate cohomology of finite groups

In the case where G is finite, we can combine all of the information of group cohomology and group homology into one infinite sequence of cohomology groups, which are called Tate cohomology groups, and denote $\widehat{H}^i(G, A)$. Let me repeat for emphasis: the Tate cohomology groups will only be defined when G is finite. It is meaningless to talk about Tate cohomology when G is infinite.

For $i \geq 1$, they are the same as group cohomology groups. For $i \leq 1$, they are the same as group homology groups. In degrees $-1, 0$, we make some special definitions, which seem somewhat unmotivated at first. It is not immediately clear that these are the "right" definitions. But eventually some of the theorems begin to show how the definitions in degree -1 and 0 couldn't be anything else to make the theory hang together.

Perhaps the simplest motivation for the definition is that of a cyclic group. Recall that if G is finite cyclic, then the groups $H^i(G, A)$ are 2-periodic, starting with $i = 1$ and $i = 2$.

$$H^1(G, A) \cong H^3(G, A) \cong \cdots \qquad H^2(G, A) \cong H^4(G, A) \cong \cdots$$

One way to think of Tate cohomology groups in degrees zero and one is that they are defined so that this pattern continues in degrees zero and one. So (in the case of G being finite cyclic) we want

$$\widehat{H}^{-1}(G, A) \cong H^1(G, A) \cong H^3(G, A) \cong \cdots \qquad \widehat{H}^0(G, A) \cong H^2(G, A) \cong H^4(G, A) \cong \cdots$$

3.7.1 Definition of Tate cohomology

Definition 3.7.1. Let G be a finite group, and let

$$N_G = \sum_{g \in G} g \in \mathbb{Z}[G]$$

be the norm element. Let A be a G-module, and view N_G as a map $A \to A$. The image lands in A^G, since for $\sigma \in G$, $\sigma N_G = N_G$. Also, N_G vanishes on I_G since $(\sigma - 1)(N_G) = 0$. Thus N_G induces a map

$$N_G : A_G \to A^G$$

We define

$$\widehat{H}_0(G,A) = \ker N_G \qquad \widehat{H}^0(G,A) = \operatorname{coker} N_G$$

making an exact sequence

$$0 \longrightarrow \widehat{H}_0(G,A) \longrightarrow A_G \xrightarrow{N_G} A^G \longrightarrow \widehat{H}^0(G,A) \longrightarrow 0$$

Remark 3.7.2. If A is a trivial module, then $A^G = A_G = A$ and $N_G : A \to A$ is just multiplication by $n = |G|$. Hence in this case

$$\widehat{H}^0(G,A) = A/nA \qquad \widehat{H}_0(G,A) = {}_nA$$

where ${}_nA$ denotes the n-torsion subgroup of A.

Definition 3.7.3. Let G be a finite group and let A be a G-module. For $i \in \mathbb{Z}$, the ith **Tate cohomology group** of G with coefficients in A is

$$\widehat{H}^i(G,A) = \begin{cases} H_{-i-1}(G,A) & i \leq -2 \\ \widehat{H}_0(G,A) & i = -1 \\ \widehat{H}^0(G,A) & i = 0 \\ H^i(G,A) & i \geq 1 \end{cases}$$

Here is the same information in a possibly more accessible format.

$$\begin{array}{cccccc} -3 & -2 & -1 & 0 & 1 & 2 \\ \widehat{H}^{-3} & \widehat{H}^{-2} & \widehat{H}^{-1} & \widehat{H}^0 & \widehat{H}^1 & \widehat{H}^2 \\ H_2 & H_1 & \widehat{H}_0 & \widehat{H}^0 & H^1 & H^2 \end{array}$$

That is, the Tate cohomology groups combine the information of homology and cohomology groups $H^i(G,A), H_i(G,A)$ into one series, with the H^0, H_0 terms replaced. They are replaced so that we get a two-tailed long exact sequence, see Theorem 1.6.6 of Sharifi [15].

Remark 3.7.4. Since we can already compute $H_i(G,A)$ and $H^i(G,A)$ using projective resolutions, we can already compute $\widehat{H}^i$ by these same resolutions, except in the cases of $i = -1, 0$. And we can describe $\widehat{H}^{-1} = \widehat{H}_0$ and $\widehat{H}^0$ in terms of the norm map.

But even better, we can actually "stitch together" projective resolutions used to compute H^i, H_i respectively, and join them in the middle with two extra terms that have $\widehat{H}_0$ and $\widehat{H}^0$ as homology. This lets us compute Tate cohomology via a doubly-infinite projective exact sequence and resulting chain complex, see Theorem 3.7.6 for details.

Definition 3.7.5. Let G be a finite group, and A a G-module. We define the following shorthand for orders of Tate cohomology groups.

$$h_k(G,A) = |\widehat{H}^k(G,A)|$$

Often the group G is understood, and this is abbreviated to $h_k(A)$. If both $h_0(A)$ and $h_1(A)$ are finite, the **Herbrand quotient** of A is

$$h(A) = \frac{h_0(A)}{h_1(A)}$$

This is usually only talked about when G is cyclic (since in this case we will soon show that $\widehat{H}^i = \widehat{H}^{i+2}$), though the definition makes sense in general.

There are a lot of results about Herbrand quotients, such as when one can say they are finite, and so on. We won't use this sort of thing much, so we leave it to the reader to find another source for that kind of thing.

3.7.2 Doubly infinite resolution for Tate cohomology

As we already motivated, Tate cohomology is the "right" way to stich together group homology and cohomology for a finite group into a doubly infinite sequence of invariants. It captures all of the homology and cohomology groups except $H_0(G, A)$ and $H^0(G, A)$, instead replacing them with $\widehat{H}^0(G, A)$ and $\widehat{H}^{-1}(G, A)$.

Perhaps the main justification that this is the "right" way to replace the zero degree groups is the following result, which says that we can also stitch together projective resolutions in the right way to give $\widehat{H}^i(G, A)$ groups as the homology of a doubly infinite chain complex.

Theorem 3.7.6. *Let G be a finite group. Let $P_\bullet \to \mathbb{Z} \to 0$ be a projective resolution of $\mathbb{Z}$ as a trivial G-module, with P_i of finite $\mathbb{Z}$-rank. Let $P_i^* = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$, and define a G-action on P_i by $(g \cdot \phi)(x) = \phi(g^{-1}x)$. Consider the exact sequence*

$$\cdots \to P_1 \to P_0 \to P_0^* \to P_1^* \to \cdots$$

Let A be a G-module. Then the Tate cohomology group $\widehat{H}^i(G, A)$ is the ith homology of the chain complex

$$\cdots \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1^*, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0^*, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \to \cdots$$

Proof. Sharifi [15] Theorem 1.6.10. □

Remark 3.7.7. In the preceeding theorem, the map $P_0 \to P_0^*$ is the composition of $P_0 \to \mathbb{Z}$ and $\mathbb{Z} \to P_0^*$ coming from the projective resolution $P_\bullet \to \mathbb{Z}$. In the resulting chain complex, P_0 is the 0th degree term, that is, $\widehat{H}^0(G, A)$ is the homology at the $\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A)$ term, and $\widehat{H}^1(G, A)$ is the homology at the $\mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A)$ term, and so on.

3.7.3 Computation of Tate cohomology of finite cyclic group

We can repeat the essential ideas of the calculation in Section 3.3.1 to compute Tate cohomology of any G-module A in the case where G is a finite cyclic group.

One way to see this is by Theorem 3.7.6, though we give an even simpler argument. The end result is that the groups $\widehat{H}^i(G, A)$ are again periodic of order 2, except even better, because the pattern continues in degrees zero and one.

Proposition 3.7.8 (Tate cohomology of a finite cyclic group)**.** *Let G be a finite cyclic group with generator σ and let A be a G-module. Then*

$$\widehat{H}^i(G, A) = \begin{cases} \ker N_G/(\sigma - 1)A & i = \ldots, -3, -1, 1, 3, \ldots \\ A^G/N_G A & i = \ldots -2, 0, 2, 4, \ldots \end{cases}$$

Proof. We already know this for $i \geq 1$ by Proposition 3.3.1. We also already know this for $i \leq -1$ by Proposition 3.6.6. For $i = -1, 0$, these are the right Tate cohomology groups essentially by definition of Tate cohomology in degrees $-1, 0$. □

3.7.4 Tate's theorem

The next goal is to prove Theorem 3.7.10. It's hard at first to see why this theorem is interesting - the hypotheses ask an awful lot to be true, and it's not very clear why they would ever be true in a concrete example. But they are, as Remark 3.7.11 describes.

Perhaps it would be best to read the statement of Tate's theorem first, then the remark, and only then try to read the proof. Not because the proof really involves understanding the remark, but because the remark explains why the theorem is useful to begin with. But of course, the reader is a strong indepedent person and they can read this in whatever order they choose.

Before Tate's theorem, though, we need a lemma, for which we give a only a halfhearted proof.

Theorem 3.7.9. *Let G be a finite group and let A be a G-module. Suppose that for all subgroups $H \subset G$,*

$$\widehat{H}^1(H, A) = \widehat{H}^2(H, A) = 0$$

Then $\widehat{H}^i(G, A) = 0$ for all $i \in \mathbb{Z}$.

Proof. Theorem 3.10 of Milne [9]. As a rough outline, this is clear if G is cyclic by the calculation of section 3.7.3. Using this, one proves the result for solvable groups by an inductive process. Then using that, the result is proved for a general group by considering Sylow subgroups of G. □

Theorem 3.7.10 (Tate's theorem)**.** *Let G be a finite group and A a G-module. Suppose that for all subgroups $H \subset G$ that*

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

Then a choice of generator γ of $H^2(G, A)$ induces isomorphisms

$$\widehat{H}^i(G, \mathbb{Z}) \to \widehat{H}^{i+2}(G, A)$$

for all $i \in \mathbb{Z}$.

Proof. We begin with an outline of the proof (from Milne [9]).

1. Construct the G-module A_ϕ.
2. Describe relevant short exact sequence involving A_ϕ.

$$0 \to A \xrightarrow{\iota} A_\phi \to I_G \to 0$$

3. Show that $\iota_* : H^2(H, A) \to H^2(H, A_\phi)$ is the zero map for any subgroup H.
4. For a subgroup $H \subset G$, extract information from long exact sequence on $\widehat{H}^i(H, -)$ associated to

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

5. For a subgroup $H \subset G$, using the long exact sequence on $\widehat{H}^i(H, -)$ associated to the A_ϕ short exact sequence, conclude that

$$H^1(H, A_\phi) = H^2(H, A_\phi) = 0$$

6. Use Theorem 3.7.9 to conclude that $H^i(G, A_\phi) = 0$ for all i. Use this to obtain the desired isomorphism.

(Step 1) Let $\phi : G^2 \to A$ be a cocycle representing our chosen generator γ. Let F be the free abelian group generated by symbols x_σ for $\sigma \in G, \sigma \neq 1$, and set

$$A_\phi = A \oplus F$$

We give A_ϕ a G-module structure by

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \phi(\sigma, \tau)$$

for $\sigma, \tau \in G$ and setting $x_1 = \phi(1, 1) \in A$. We need to check that $(\rho\sigma)x_\tau = \rho(\sigma x_\tau)$ for $\rho, \sigma, \tau \in G$ to verify this is a G-action.

$$\begin{aligned}
(\rho\sigma)x_\tau &= x_{\rho\sigma\tau} - x_{\rho\sigma} + \phi(\rho\sigma, \tau) \\
\rho(\sigma x_\tau) &= \rho(x_{\sigma\tau} - x_\sigma + \phi(\sigma, \tau)) \\
&= x_{\rho\sigma\tau} - x_\rho + \phi(\rho, \sigma\tau) - \Big(x_{\rho\sigma} - x_\rho + \phi(\rho, \sigma)\Big) + \rho\phi(\sigma, \tau) \\
&= x_{\rho\sigma\tau} - x_\rho + \phi(\rho, \sigma\tau) - x_{\rho\sigma} + x_\rho - \phi(\rho, \sigma) + \rho\phi(\sigma, \tau)
\end{aligned}$$

Thus these are equal if and only if

$$\phi(\rho\sigma, \tau) = \phi(\rho, \sigma\tau) - \phi(\rho, \sigma) + \rho\phi(\sigma, \tau)$$

which is precisely the cocycle condition.
(Step 2) Define

$$\begin{aligned}
\alpha : A_\phi &\to I_G \\
a &\mapsto 0 \\
x_\sigma &\mapsto \sigma - 1
\end{aligned}$$

where $a \in A, \sigma \in G, \sigma \neq 1$. This is a G-module homomorphism because

$$\sigma\alpha(x_\tau) = \sigma(\tau - 1) = \sigma\tau - \sigma = \alpha(x_{\sigma\tau} - \alpha(x_\sigma) + \alpha(\phi(\sigma, \tau))$$

Clearly $A = \ker \alpha$, so we have a short exact sequence of G-modules, where $\iota : A \hookrightarrow A_\phi$ is the inclusion into the first component.

$$0 \longrightarrow A \xrightarrow{\iota} A_\phi \xrightarrow{\alpha} I_G \longrightarrow 0$$

(Step 3) For any subgroup $H \subset G$, we know that $\operatorname{Cor}\operatorname{Res} : H^2(G, A) \to H^2(G, A)$ is multiplication by $[G : H] = \frac{|G|}{|H|}$ (Proposition 3.9.17). Hence $\operatorname{Cor}\operatorname{Res}\gamma$ has order $|H|$, so

$\operatorname{Res}\gamma \in H^2(H,A)$ has order at least $|H|$. Since $H^2(H,A)$ is cyclic of order $|H|$, this just says that $\operatorname{Res}\gamma$ is a generator of $H^2(H,A)$. Now consider the 1-cochain

$$f : G \to A_\phi \qquad \sigma \mapsto x_\sigma$$

which represents an element of $H^1(G, A_\phi)$. Then

$$(df)(\sigma,\tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma) = \sigma x_\tau - x_{\sigma\tau} + x_\sigma = \iota \circ \phi(\sigma,\tau)$$

Hence $\iota \circ \phi$ is a coboundary, which is to say,

$$\iota_*\gamma = \iota_*[\phi] = [\iota \circ \phi] = 0 \in H^2(G, A_\phi)$$

Since γ generates $H^2(G,A)$, this says that $\iota_* : H^2(G,A) \to H^2(G,A_\phi)$ is the zero map. Then since $\operatorname{Res}\gamma$ generates $H^2(H,A)$ and using commutativity of the following diagram, the map $\iota_* : H^2(H,A) \to H^2(H,A_\phi)$ is trivial for any subgroup $H \subset G$.

$$\begin{array}{ccc} H^2(G,A) & \xrightarrow{\iota_*=0} & H^2(G,A_\phi) \\ \big\downarrow{\scriptstyle \operatorname{Res}} & & \big\downarrow{\scriptstyle \operatorname{Res}} \\ H^2(H,A) & \xrightarrow{\iota_*} & H^2(H,A_\phi) \end{array}$$

(Step 4) Let $H \subset G$ be any subgroup. Since $\mathbb{Z}[G]$ is a free (hence projective) $\mathbb{Z}[H]$-module (Lemma 3.8.4), for all $i \in \mathbb{Z}$, we have

$$\widehat{H}^i(H, \mathbb{Z}[G]) = 0$$

Then from the long exact sequence on Tate cohomology associated to $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, the connecting homomorphisms give isomorphisms

$$\widehat{H}^i(H,\mathbb{Z}) \to \widehat{H}^{i+1}(H, I_G)$$

In particular,

$$\begin{array}{lll} H^1(H,I_G) \cong \widehat{H}^0(H,\mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z} & & \text{Proposition } \textbf{??} \\ H^2(H,I_G) \cong H^1(H,\mathbb{Z}) \cong \operatorname{Hom}(H,\mathbb{Z}) & & \text{Proposition 3.2.7} \\ \qquad = 0 & & \text{because } H \text{ is finite} \end{array}$$

(Step 5) Let $H \subset G$ be any subgroup. Now we consider the long exact sequence on cohomology associated to $0 \to A \to A_\phi \to I_G \to 0$. (We could use Tate cohomology or not, they are the same in this case.)

$$\begin{array}{ccccccccccc} H^1(H,A) & \to & H^1(H,A_\phi) & \to & H^1(H,I_G) & \to & H^2(H,A) & \xrightarrow{0} & H^2(H,A_\phi) & \to & H^2(H,I_G) \\ \cong & & & & \cong & & \cong & & & & \cong \\ 0 & & & & \mathbb{Z}/|H|\mathbb{Z} & & \mathbb{Z}/|H|\mathbb{Z} & & & & 0 \end{array}$$

The various isomorphisms come from our hypotheses and Step 4. The map $H^2(H,A) \to H^2(H,A_\phi)$ is zero by Step 3, so by exactness $H^1(H,I_G) \to H^2(H,A)$ is surjective. Since

they are finite groups of the same order, this implies it is an isomorphism. Then by exactness, $H^1(H, A_\phi) = 0$. Also by exactness, $H^2(H, A_\phi) = 0$.

(Step 6) By Step 5, the hypotheses of Theorem 3.7.9 are satisfied, so $\widehat{H}^i(G, A_\phi) = 0$ for all $i \in \mathbb{Z}$. Thus the connecting homomorphisms in the long exact sequence on $\widehat{H}^i(G, -)$ associated to $0 \to A \to A_\phi \to I_G \to 0$ are isomorphisms. Composing this with the connecting isomorphisms of Step 4, we obtain the desired isomorphisms.

$$\widehat{H}^i(G, \mathbb{Z}) \xrightarrow{\cong} \widehat{H}^{i+1}(G, I_G) \xrightarrow{\cong} \widehat{H}^{i+2}(G, A)$$

□

Remark 3.7.11. The hypotheses that $\widehat{H}^1(H, A) = 0$ and $\widehat{H}^2(H, A)$ is cyclic of order $|H|$ for all subgroups seems so strong that it would not arise very often in useful circumstances. However, it does occur in the following important situation which is central to local class field theory.

Let K be a complete nonarchimedean discretely valued local field (such as $\mathbb{Q}_p$), and let L/K be a finite extension. Let $G = \mathrm{Gal}(L/K)$ and $A = L^\times$, so A is a G-module. By Galois theory, all subgroups $H \subset G$ are of the form $\mathrm{Gal}(L/E)$ where $K \subset E \subset L$ is an intermediate subfield. By Hilbert 90,

$$\widehat{H}^1(H, A) = H^1(\mathrm{Gal}(L/E), L^\times) = 0$$

and by Corollary 4.6.37,

$$\widehat{H}^2(H, A) = H^2(\mathrm{Gal}(L/E), L^\times) \cong \mathbb{Z}/m\mathbb{Z}$$

where $m = [L : E] = |H|$. Thus, all the hypotheses of Tate's theorem are satisfied in this situation.

The following slightly different statement (and very different proof) of Tate's theorem is given in section 1.12 (in particular, Theorem 1.12.3) of Sharifi [15].

Theorem 3.7.12 (Tate's theorem)**.** *Let G be a finite group and let A be a G-module. For each prime p, fix a Sylow p-subgroup $G_p \subset G$. Let $\alpha \in H^2(G, A)$. Suppose that for every p, $H^1(G_p, A) = 0$ and $H^2(G_p, A)$ is cyclic of order $|G_p|$ generated by* $\mathrm{Res}\,\alpha$*. Then for $i \in \mathbb{Z}$ we have isomorphisms*

$$\widehat{H}^i(G, \mathbb{Z}) \to \widehat{H}^{i+2}(G, A) \qquad \beta \mapsto (\mathrm{Res}\,\alpha) \cup \beta$$

The hypotheses of this version are essentially the same, the main difference is that the isomorphisms constructed as a composition of connecting homomorphisms in the Milne proof are instead manifested as cup products with some element. This is often a very important aspect of application of the theorem. Unfortunately, we do not include the proof of this version here. See section 1.12 of Sharifi [15] for details.

3.8 Dimension shifting

Dimension shifting is a very powerful technique for group cohomology and homology. It allows one to define/construct maps on all homology groups just by defining them in one degree, often degree zero since that's where things are very concrete.

The price for this is that the higher degree versions of the maps are often very difficult to compute explicitly. But the benefit of the construction is that such maps are "compatible" with all of morphisms involved in the long exact sequences, in the sense that certain squares commute, even squares involving the connecting homomorphisms.

This is excellent because the connecting homomorphisms have much the same problem - they were constructed via snake lemma, so they aren't convenient to describe simply in terms of elements. The whole thing has a very categorical flavor.

3.8.1 Induced and coinduced modules

Before we can do any dimension shifting, we need to develop some tools, primarily induced and coinduced modules and some important short exact sequences involving them. This will build up to Shapiro's lemma 3.8.10, which tells us that homology and cohomology groups always vanish for induced and coinduced modules. From there, dimension shifting will be an immediate corollary.

Definition 3.8.1. Let $H \subset G$ be a subgroup, and let A be an H-module. The **induced module** associated to A is

$$\mathrm{Ind}_H^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$$

This is a G-module via the action

$$g(x \otimes a) = (gx) \otimes a$$

where $g \in G, x \in \mathbb{Z}[G], a \in A$. If A is any abelian group, then it is a module over the trivial subgroup, so there is an induced module

$$\mathrm{Ind}^G(A) = \mathrm{Ind}_{\{1\}}^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$$

Any G-module which is isomorphic to $\mathrm{Ind}^G(A)$ for some A is called an **induced** module.

Definition 3.8.2. Let $H \subset G$ be a subgroup, and let A be an H-module. The **coinduced module** associated to A is

$$\mathrm{CoInd}_H^G(A) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$$

This is also sometimes denoted $M_H^G(A)$. This is a G-module via the action

$$(g \cdot \phi)(x) = \phi(xg)$$

where $g \in G, x \in \mathbb{Z}[G], \phi \in \mathrm{CoInd}_H^G(A)$. As in the case of induced modules, the case where H is the trivial subgroup is of particular importance, and it is written

$$\mathrm{CoInd}^G(A) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$$

and any G-module isomorphic to $\mathrm{CoInd}^G(A)$ for some A is called a **coinduced module**. $\mathrm{CoInd}^G(A)$ is also sometimes written $M^G(A)$.

Lemma 3.8.3. *A direct sum of induced (coinduced) modules is induced (coinduced).*

Proof. For induced modules, this follows from the fact that tensor products distribute over arbitrary direct sums. For coinduced modules, this follows that arbitrary direct sums in the 2nd variable of Hom pull out as arbitrary direct sums. (Note that for Hom, an infinite direct sum in the first variable pulls out as a direct product, but this does not affect us at the moment.) □

The next lemma we could have proved a long time ago right after defining group rings, but we didn't need it so we put it off until now.

Lemma 3.8.4. *Let $H \subset G$ be a subgroup. Then $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module of rank $[G : H]$.*

Proof. To clarify, the action of $\mathbb{Z}[H]$ on $\mathbb{Z}[G]$ is just left multiplication in $\mathbb{Z}[G]$. Let $\{\sigma_i : i \in I\}$ be a set of right coset representatives for H. Let $x \in \mathbb{Z}[G]$ be arbitrary, written uniquely as

$$x = \sum_{g \in G} m_g g \in \mathbb{Z}[G] \qquad m_g \in \mathbb{Z}$$

Since the cosets $H\sigma_i$ partition G, we can rewrite this as

$$\sum_{g \in G} m_g g = \sum_{i \in I} \sum_{g \in H\sigma_i} m_g g$$

For $g \in H\sigma_i$, we can write it as $g = h_g \sigma_i$ for a unique $h_g \in H$. Then we write the above uniquely as

$$\sum_{i \in I} \sum_{g \in H\sigma_i} m_g g = \sum_{i \in I} \sum_{g \in G} m_g h_g \sigma_i = \sum_{i \in I} \left(\sum_{g \in H\sigma_i} m_g h_g \right) \sigma_i$$

Thus the σ_i form a $\mathbb{Z}[H]$-spanning set for $\mathbb{Z}[G]$, of size $[G : H]$. They are also linearly independent, as

$$\sum_{i \in I} \left(\sum_{g \in H\sigma_i} m_g h_g \right) \sigma_i = 0 \implies m_g = 0, \ \forall g \implies \sum_{g \in H\sigma_i} m_g h_g = 0, \ \forall i$$

□

Lemma 3.8.5. *The functor $\mathrm{CoInd}_H^G(-)$ is exact.*

Proof. By definition, $\mathrm{CoInd}_H^G(-) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], -)$. By Lemma 3.8.4, $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module, hence projective, so $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], -)$ is exact. □

3.8.2 Induced/coinduced isomorphism for finite index subgroups

In general the induced and coinduced modules for a given G-module A are not the same, $\mathrm{Ind}_H^G(A) \ncong \mathrm{CoInd}_H^G(A)$. However, if H is finite index, they are.

This section is not critically important for dimension shifting, so the reader could reasonably skip this section and go directly to section 3.8.3.

Proposition 3.8.6. *Let $H \subset G$ be a subgroup of finite index, and let A be an H-module. There is a canonical isomorphism of G-modules*

$$\chi : \mathrm{CoInd}_H^G(A) \to \mathrm{Ind}_H^G(A) \qquad \phi \mapsto \sum_{gH \in G/H} g^{-1} \otimes \phi(g)$$

where g is any coset representative for gH. More precisely, let $n = [G : H]$, and let $g_1H, \ldots, g_nH$ be a set of left coset representatives, then

$$\chi(\phi) = \sum_{i=1}^{n} g_i^{-1} \otimes \phi(g_i)$$

where the right hand side does not depend on the choice of coset representatives. (In fact, each term $g_i^{-1} \otimes \phi(g_i)$ does not depend on the choice of $g_i \in g_iH$.)

Proof. First, we show that each term $g^{-1} \otimes \phi(g)$ does not depend on the choice of coset representative $g \in gH$. If $g' = gh$ is a different coset represenative for gH, then using $\mathbb{Z}[H]$-linearity we get

$$((g')^{-1}) \otimes \phi(g') = (gh)^{-1} \otimes \phi(gh) = h^{-1}g^{-1} \otimes h\phi(g) = g \otimes \phi(g)$$

thus the terms in the sum defining $\chi(\phi)$ do not depend on the choice of coset representatives. We verify that χ is a G-module homomorphism. Let $g \in G, \phi \in \mathrm{CoInd}_H^G(A)$.

$$\begin{aligned}\chi(g\phi) &= \sum_{i=1}^{n} g_i^{-1} \otimes (g\phi)(g_i) = \sum_{i=1}^{n} g_i^{-1} \otimes \phi(g_ig) = \sum_{i=1}^{n} g \cdot \left(g^{-1}g_i^{-1} \otimes \phi(g_ig)\right) \\ &= g \sum_{i=1}^{n} (g_ig)^{-1} \otimes \phi(g_ig) = g\chi(\phi)\end{aligned}$$

The final equality comes from the fact that if $g_1, \ldots, g_n$ are coset representatives for H, then $gg_1, \ldots, gg_n$ are another set of coset representatives for H. Now we show that χ is an isomorphism. It is relatively easy to see that χ has trivial kernel, since if

$$\chi(\phi) = \sum_{gH \in G/H} g^{-1} \otimes \phi(g) = 0$$

then each term must be zero (since none of the g^{-1} are equal, the terms are linearly independent), hence $\phi(g) = 0$ for each g. Since this is independent of representative, $\phi(g) = 0$ for all $g \in gH$, and since G is covered by the cosets, ϕ is the zero map. Hence χ is injective.

To show that χ is surjective, we note that $\mathrm{Ind}_H^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$ is generated by elements of the form $x \otimes a$ where $x \in Z[G], a \in A$, so it is sufficient to show that such elements lie in the image of χ. If we fix a set of coset representatives $g_1, \ldots, g_n$ for H, then $g_1^{-1}, \ldots, g_n^{-1}$ are also coset representatives, and by Lemma 3.8.4 x can be written uniquely as

$$x = \sum_{i=1}^{n} y_i g_i^{-1}$$

where $y_i \in \mathbb{Z}[H]$. Then define

$$\phi : \mathbb{Z}[G] \to A \qquad \phi(g_i) = y_i a$$

This defines ϕ on one element of each coset of G, and extending by $\mathbb{Z}[H]$-linearity this extends to define ϕ on all of $\mathbb{Z}[G]$, hence $\phi \in \mathrm{CoInd}_H^G(A)$. Furthermore,

$$\chi(\phi) = \sum_{i=1}^{n} g_i^{-1} \otimes \phi(g_i) = \sum_{i=1}^{n} g_i^{-1} \otimes y_i a = \sum_{i=1}^{n} y_i g_i^{-1} \otimes a = \left(\sum_{i=1}^{n} y_i g_i^{-1} \right) \otimes a = x \otimes a$$

Thus χ is surjective. This completes the proof that χ is an isomorphism. □

Remark 3.8.7. In particular, the previous result holds in the case where G is a finite group and H is the trivial subgroup, so for finite G, we have

$$\mathrm{CoInd}^G(A) \cong \mathrm{Ind}^G(A)$$

In the case where G is finite, the isomorphism of the previous theorem is simpler, since there is no issue of coset representatives (the cosets of the trivial subgroup are just the elements of G).

$$\chi : \mathrm{CoInd}^G(A) \to \mathrm{Ind}^G(A) \qquad \phi \mapsto \sum_{g \in G} g^{-1} \otimes \phi(g)$$

3.8.3 Shapiro's lemma

The following isomorphism is really just a disguised version of a specific case of the tensor-hom adjunction, but we spell things out in gory detail. The main purpose of this lemma is to use it to prove Shapiro's lemma.

Lemma 3.8.8 (Tensor-hom adjunction)**.** *Let $H \subset G$ be a subgroup, let A be a G-module, and let B be an H-module. Then*

$$\psi_B^A : \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B)) \to \mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \qquad \Big(\psi_B^A(\alpha)\Big)(a) = \Big(\alpha(a)\Big)(1)$$

is an isomorphism of abelian groups. Furthermore, this gives a natural isomorphism of bifunctors

$$\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathrm{CoInd}_H^G(-)) \cong \mathrm{Hom}_{\mathbb{Z}[H]}(-, -)$$

Explicitly, being a natural isomorphism means that for any morphism $\eta : A \to A'$ of G-modules and any morphism $\chi : B \to B'$ of H-modules, the folllowing two squares commute.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}[G]}(A', \mathrm{CoInd}_H^G(B)) & \xrightarrow{f \mapsto f\eta} & \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B)) \\ \cong \downarrow \psi_B^{A'} & & \cong \downarrow \psi_B^A \\ \mathrm{Hom}_{\mathbb{Z}[H]}(A', B) & \xrightarrow{f \mapsto f\eta} & \mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \end{array}$$

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B)) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B')) \\ \cong \downarrow \psi_B^A & & \cong \downarrow \psi_{B'}^A \\ \mathrm{Hom}_{\mathbb{Z}[H]}(A, B) & \xrightarrow{f \mapsto \chi f} & \mathrm{Hom}_{\mathbb{Z}[H]}(A, B') \end{array}$$

To describe the upper arrow on the bottom square, we first note that the induced map $\mathrm{CoInd}_H^G(B) \to \mathrm{CoInd}_H^G(B')$ *is* $f \mapsto \chi f$*, and then the map on Homs is*

$$\alpha \mapsto \Big((f \mapsto \chi f) \circ \alpha \Big)$$

Proof. For simplicity, denote ψ_B^A by ψ. Throughout,

$$a \in A \qquad h \in H \qquad \alpha \in \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B)) \qquad \beta \in \mathrm{Hom}_{\mathbb{Z}[H]}(A, B)$$

First we verify that ψ lands in $\mathrm{Hom}_{\mathbb{Z}[H]}(A, B)$, so we check that for $\alpha \in \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B))$, the map $\psi(\alpha)$ is H-linear.

$$\Big(\psi(\alpha)\Big)(ha) = \Big(\alpha(ha)\Big)(1) = \Big(h\alpha(a)\Big)(1) = \Big(\alpha(a)\Big)(h) = h\Big(\big(\alpha(a)\big)(1)\Big) = h\Big(\big(\psi(\alpha)\big)(a)\Big)$$

Thus $\psi(\alpha)$ is H-linear, so ψ lands in the correct target. Now we define a map which we will show to be the inverse of ψ.

$$\phi : \mathrm{Hom}_{\mathbb{Z}[H]}(A, B) \to \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(B)) \qquad \Big(\big(\phi(\beta)\big)(a)\Big)(1) = \beta(a)$$

where $\beta \in \mathrm{Hom}_{\mathbb{Z}[H]}(A, B)$ and $a \in A$. We have defined $\phi(\beta)(a)$ only on $1 \in \mathbb{Z}[G]$, and then extend by G-linearity, so we do not have check that $\phi(\beta)(a)$ is $\mathbb{Z}[H]$-linear. We don't need to verify that ϕ is a group homomorphism, since the inverse to a group homomorphism (if it exists) is a group homomorphism. Now we check that ϕ, ψ are inverses.

$$\Big((\psi\phi)(\beta)\Big)(a) = \Big(\psi\big(\phi(\beta)\big)\Big)(a) = \Big(\big(\phi(\beta)\big)(a)\Big)(1) = \beta(a)$$

which is to say $(\psi\phi)(\beta) = \beta$, hence $\psi\phi = \mathrm{Id}$. For the composition in the other order, first we note that

$$\begin{aligned}(\phi\psi)(\alpha) = \alpha &\iff \Big((\phi\psi)(\alpha)\Big)(a) = \alpha(a)\ \forall a \in A \\ &\iff \Big(\big(\phi\psi)(\alpha)\big)(a)\Big)(1) = \Big(\alpha(a)\Big)(1)\ \forall a \in A\end{aligned}$$

so to show $\phi\psi = \mathrm{Id}$, it suffices to verify the last condition, which we do. For $a \in A$, we have

$$\Big((\phi\psi)(\alpha)\Big)(1) = \Big(\Big(\phi\big(\psi(\alpha)\big)\Big)(a)\Big)(1) = \Big(\psi(\alpha)\Big)(a) = \Big(\alpha(a)\Big)(1)$$

Thus $\phi\psi = \mathrm{Id}$, so ϕ, ψ are inverses. Now we show that the isomorphisms ψ_B^A provide a natural transformation by proving commutativity of the two squares above, starting with the upper square.

$$\Big(\psi_B^A(f\eta)\Big)(a) = \Big(f\eta(a)\Big)(1) = \Big(f\big(\eta(a)\big)\Big)(1) = \Big(\psi_B^{A'}(f)\Big)\big(\eta(a)\big) = \Big(\big(\psi_B^{A'}(f)\big) \circ \eta\Big)(a)$$

This proves commutativity of the top square. For the lower square, going around the bottom we obtain

$$\Big(\chi\psi_B^A(\alpha)\Big)(a) = \chi\Big(\big(\psi_B^A(\alpha)\big)(a)\Big) = \chi\Big(\big(\alpha(a)\big)(1)\Big)$$

and going around the top, we have

$$\Big(\psi^A_{B'}\Big((f \mapsto \chi f)\circ\alpha\Big)\Big)(a) = \Big(\Big((f\mapsto\chi f)\circ\alpha\Big)(a)\Big)(1) = \chi\Big(\big(\alpha(a)\big)(1)\Big)$$

Thus both squares commute as claimed. □

Just one more lemma before Shapiro's lemma. It's a bit strange that a lemma requires so many other lemmas to prove. Oh well.

Lemma 3.8.9 (CoInd preserves injectives)**.** *If I is an injective H-module, then* $\mathrm{CoInd}_H^G(I)$ *is an injective G-module.*

Proof. Let I be an injective H-module. We use the characterization that I is injective if and only if the functor $\mathrm{Hom}_{\mathbb{Z}[H]}(-, I)$ is exact, so to show $\mathrm{CoInd}_H^G(I)$ is injective, we show that the functor $\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathrm{CoInd}_H^G(I))$ is exact.

Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules, which we can also view as H-modules by restricting the action. To show that $\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathrm{CoInd}_H^G(I))$ is exact, we need to show that the image of $0 \to A \to B \to C \to 0$ under this functor is exact. By the first commutative square of Lemma 3.8.8, we have the following commutative diagram (of abelian groups).

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[H]}(C, I) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[H]}(B, I) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[H]}(A, I) & \longrightarrow & 0 \\
 & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\
0 & \to & \mathrm{Hom}_{\mathbb{Z}[G]}(C, \mathrm{CoInd}_H^G(I)) & \to & \mathrm{Hom}_{\mathbb{Z}[G]}(B, \mathrm{CoInd}_H^G(I)) & \to & \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{CoInd}_H^G(I)) & \to & 0
\end{array}$$

By injectivity of I, the top row is exact. Since the vertical maps are isomorphisms, we have an isomorphism of chain complexes, hence exactness of the top implies exactness of the bottom. Thus $\mathrm{CoInd}_H^G(I)$ is an injective G-module. □

Proposition 3.8.10 (Shapiro's lemma)**.** *Let $H \subset G$ be a subgroup. There are natural isomorphisms of functors*

$$H^i(H, -) \cong H^i(G, \mathrm{CoInd}_H^G(-))$$
$$H_i(H, -) \cong H_i(G, \mathrm{Ind}_H^G(-))$$

for all $i \geq 0$.

Proof. We only prove the isomorphism for cohomology on the level of groups, and omit the details of the natural isomorphism of functors. Let A be an H-module, and choose an injective resolution of A by H-modules.

$$0 \to A \to I_0 \to I_1 \to \cdots$$

Since $H^i(H, -)$ is the ith right derived functor of $(-)^H$, $H^i(H, A)$ is the ith cohomology of the following complex.

$$0 \to I_0^H \to I_1^H \to \cdots$$

On the other hand, if we apply the functor $\mathrm{CoInd}_H^G(-)$ to our injective resolution of A, by Lemmas 3.8.5 and 3.8.9 we get an injective resolution of $\mathrm{CoInd}_H^G(A)$.

$$0 \to \mathrm{CoInd}_H^G(A) \to \mathrm{CoInd}_H^G(I_0) \to \mathrm{CoInd}_H^G(I_1) \to \cdots$$

Then since $H^i(G,-)$ is the ith right derived functor of $(-)^G$, $H^i(G, \mathrm{CoInd}_H^G(A))$ is the ith cohomology of the complex

$$0 \to \mathrm{CoInd}_H^G(I_0)^G \to \mathrm{CoInd}_H^G(I_1)^G \to \cdots \tag{3.8.1}$$

Note that

$$\mathrm{CoInd}_H^G(I_k)^G = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], I_k)^G \cong \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I_k)$$

so we may replace the resolution 3.8.1 by the resolution

$$0 \to \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I_0) \to \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I_1) \to \cdots$$

Finally, applying the natural isomorphism of Lemma 3.2.3, we get an isomorphism of chain complexes

$$\begin{array}{ccccccc}
0 & \longrightarrow & I_0^H & \longrightarrow & I_1^H & \longrightarrow & \cdots \\
 & & \downarrow\cong & & \downarrow\cong & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I_0) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}, I_1) & \longrightarrow & \cdots
\end{array}$$

which induces isomorphisms on homology,

$$H^i(H, A) \cong H^i(G, \mathrm{CoInd}_H^G(A))$$

□

The most important corollary of Shapiro's lemma is that induced and coinduced modules have trivial homology groups for $i \geq 1$, as the next corollary spells out.

Corollary 3.8.11. *Let G be a group, and A a G-module. Then*

$$H^i(G, \mathrm{Ind}^G(A)) = 0 \qquad H_i(G, \mathrm{CoInd}^G(A)) = 0$$

for all $i \geq 1$.

Proof. Let $H \subset G$ be the trivial group subgroup. Note that $H^i(H, A) = 0$ for $i \geq 1$, just by thinking in terms of cocycles. By Shapiro's lemma,

$$H^i(G, \mathrm{CoInd}^G(A)) \cong H^i(H, A) = 0 \qquad H_i(G, \mathrm{Ind}^G(A)) \cong H_i(H, A) = 0$$

□

3.8.4 Dimension shifting isomorphisms

Finally we get to dimension shifting, which was the whole purpose for defining and studying induced and coinduced modules.

Definition 3.8.12. Let G be a group and A a G-module. There is an injection

$$\iota : A \to \mathrm{CoInd}^G(A) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \qquad \Big(\iota(a)\Big)(g) = a$$

for $a \in A, g \in G$, extended by $\mathbb{Z}$-linearity. Alternately, using the canonical isomorphism

$$\theta : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A \qquad \phi \leftrightarrow \phi(1)$$

we can describe ι as $\iota = j\theta^{-1}$ where

$$j : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \qquad \phi \mapsto \phi\epsilon$$

Here, ϵ is the augmentation map. We define A^* to be the cokernel of this map, making the following exact sequence.

$$0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$$

Note that this is split exact, see Remark 3.8.15.

Definition 3.8.13. Similarly to the above, there is a surjection

$$\pi : \mathrm{Ind}^G(A) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to A \qquad \pi(g \otimes a) = a$$

Alternately, using the canonical isomorphism

$$\eta : \mathbb{Z} \otimes_{\mathbb{Z}} A \cong A \qquad 1 \otimes a \leftrightarrow a$$

we have $\pi = \eta^{-1} \circ (\epsilon \otimes \mathrm{Id}_A)$ where

$$\epsilon \otimes \mathrm{Id}_A : \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to \mathbb{Z} \otimes_{\mathbb{Z}} A$$

Here, ϵ is the augmentation map. We define A_* to be the kernel of π, making the following exact sequence.

$$0 \to A_* \to \mathrm{Ind}^G(A) \to A \to 0$$

Note that this is split exact, see Remark split exact.

Proposition 3.8.14. *Let $I_G \subset G$ be the augmentation ideal. Using the notation above,*

$$A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \qquad A_* \cong I_G \otimes_{\mathbb{Z}} A$$

Proof. Using the map j from the previous definitions and the augmentation map ϵ, we know that A^* is isomorphic to the cokernel of j, which is described by the following short exact sequence.

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \xrightarrow[\phi \mapsto \phi\epsilon]{j} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \xrightarrow[\psi \mapsto \psi|_{I_G}]{} \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \longrightarrow 0$$

After checking exactness here, immediately we get $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$. Similarly, A_* is isomorphic to the kernel of $\epsilon \otimes \mathrm{Id}_A$, which is depicted below.

$$0 \longrightarrow I_G \otimes_{\mathbb{Z}} A \hookrightarrow \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \xrightarrow{\epsilon \otimes \mathrm{Id}_A} \mathbb{Z} \otimes_{\mathbb{Z}} A \longrightarrow 0$$

Hence $A_* \cong I_G \otimes_{\mathbb{Z}} A$. □

Remark 3.8.15. The sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ is exact, and additive functors preserve split exactness, so the sequences defining A_*, A^* are also split exact, because they are the image of this sequence under the respective functors $\mathrm{Hom}(-, A)$ and $- \otimes A$.

This is it, the big moment where we actually do dimension shifting.

Proposition 3.8.16 (Dimension shifting property)**.** *Let A be a G-module, and let A^*, A_* be as defined above. Then for all $i \geq 1$,*

$$H^{i+1}(G, A) \cong H^i(G, A^*) \qquad H_{i+1}(G, A) \cong H_i(G, A_*)$$

with isomorphisms provided by connecting homomorphisms of long exact sequences.

Proof. Consider the short exact sequence

$$0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$$

and the associated long exact sequence on cohomology,

$$0 \to A^G \to \mathrm{CoInd}^G(A)^G \to (A^*)^G \to H^1(G, A) \to H^1(G, \mathrm{CoInd}^G(A)) \to \cdots$$

By Shapiro's lemma 3.8.10, for $i \geq 1$ the terms $H^i(G, \mathrm{CoInd}^G(A))$ vanish.

$$0 \to H^i(G, A^*) \to H^{i+1}(G, A) \to 0$$

By exactness, the connecting homomorphism must be an isomorphism for $i \geq 1$. The result for homology follows in the same manner by considering the LES on homology associated to

$$0 \to A_* \to \mathrm{Ind}^G(A) \to A \to 0$$

□

In the next few sections, we will put these isomorphisms to work repeatedly.

3.9 Functorial properties of group cohomology

The title for this section is a bit grandiose. Really, it just means an assortment of things which induce maps and make diagrams commute in nice ways.

3.9.1 Compatible pairs

One very broad tool for inducing maps on cohomology is via compatible pairs.

Definition 3.9.1. Let G, G' be groups. Let A be a G-module, and A' be a G'-module. A **compatible pair** (for cohomology) is a pair (ρ, λ) of homomorphisms $\rho : G' \to G$ and $\lambda : A \to A'$ making the following diagram commute for every $g' \in G'$.

$$\begin{array}{ccc} A & \xrightarrow{\rho(g')} & A \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda} \\ A' & \xrightarrow{g'} & A' \end{array}$$

As an equation, we write this as $\lambda(\rho(g')a) = g'\lambda(a)$. We denote a compatible pair with the notation $(\rho, \lambda) : (G, A) \to (G', A')$. (This notation sort of implies that ρ maps from G to G', but it doesn't, so be careful.) This generalizes the notion of a morphism of G-modules, which is the case $G' = G$, $\rho = \mathrm{Id}_G$.

For the categorically inclined, there is a category whose objects are pairs (G, A) of a group G acting on an abelian group A, and whose morphisms are compatible pairs. I've never seen anyone really take this point of view, though, so it may not be that useful.

One advantage of thinking this way is that we can think of group cohomology (or homology) as taking an object in the category of pairs and outputting an abelian group $H^i(G, A)$ (or $H_i(G, A)$). We would like this to be a functor, so a morphism in our category (a compatible pair) should induce a morphism in the target category. This does in fact happen, as we now define.

Definition 3.9.2. Let $(\rho, \lambda) : (G, A) \to (G', A')$ be a compatible pair. The **induced map on cochains** is

$$C^i(G, A) \to C^i(G', A') \qquad f \mapsto \lambda \circ f \circ (\rho \times \cdots \times \rho)$$

Since this is a chain map (see Sharifi 1.8.2), it induces a map $H^i(G, A) \to H^i(G', A')$, which is called the **induced map on cohomology**. Alternately, the **induced map on the standard complex** is

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) \to \mathrm{Hom}_{\mathbb{Z}[G']}(\mathbb{Z}[(G')^{i+1}], A') \qquad \psi \mapsto \lambda \circ \psi \circ (\rho \times \cdots \times \rho)$$

which is also a chain map, and induces a map on cohomology $H^i(G, A) \to H^i(G', A')$. The induced maps on cohomology are the same from these two processes. As a third alternative, one could even define an induced map on general projective resolutions of $\mathbb{Z}$, but this seems unnecessary.

Returning to thinking categorically, we can say that $H^i(-, -)$ is a functor from the category of pairs (G, A) to the category of abelian groups. As I said before, no one except me seems to think about it this way, so perhaps it's not so useful.

Definition 3.9.3. For homology (in contrast with cohomology), the analogous notion of a compatible pair is a pair of homomorphisms $\rho : G \to G'$ and $\lambda : A \to A'$, with A a G-module, and A' a G'-module, making the analogous square commute.

$$\begin{array}{ccc} A & \xrightarrow{g} & A \\ \downarrow{\scriptstyle \lambda} & & \downarrow{\scriptstyle \lambda} \\ A' & \xrightarrow{\rho(g)} & A' \end{array}$$

These induce morphisms

$$\overline{\rho} \otimes \lambda : \mathbb{Z}[G^{i+1}] \otimes_{\mathbb{Z}[G]} A \to \mathbb{Z}[(G')^{i+1}] \otimes_{\mathbb{Z}[G']} A'$$

where $\overline{\rho}$ is the induced map $\mathbb{Z}[G^{i+1}] \to \mathbb{Z}[(G')^{i+1}]$ defined by ρ on G and extending by $\mathbb{Z}$-linearity. This gives the induced chain map on the sequence defining $H_i(G, A)$, so it induces maps on homology $H_i(G, A) \to H_i(G', A')$.

3.9.2 Important compatible pairs: restriction, inflation, corestriction

We aren't going to study compatible pairs in any sort of generality. Instead, we're just going to look at a few very useful compatible pairs and the maps they induce. Historically, people probably described these maps on cohomology in other terms before using the language of compatible pairs, but I'm not sure.

The main induced maps we will have are restriction, corestriction, and inflation. There is also a coinflation map which we won't describe, because it doesn't get as much done later. Restriction is named after function restriction, which it bears some resemblence too. It will be a map

$$\mathrm{Res} : H^i(G, A) \to H^i(H, A)$$

where $H \subset G$ is any subgroup. Res is inspired by the idea of restricting a cocycle, which is a function $f : G \to A$ to $f|_H : H \to A$. Of course, since elements of $H^i(G, A)$ are equivalence classes of cocycles, more subtlety is involved. Corestriction will be a map going the other way,

$$\mathrm{Cor} : H_i(H, A) \to H_i(G, A)$$

which is not so directly inspired, so things are more complicated. Inflation maps are losely related to quotient maps, so we will need $H \subset G$ to be a normal subgroup, and will obtain a map

$$\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G, A)$$

Coinflation goes the oppposite direction from inflation, but we don't describe it in detail in these notes.

Definition 3.9.4. Let $H \subset G$ be a subgroup, and let A be a G-module. Let $e : H \hookrightarrow G$ be the inclusion, so we have a compatible pair $(e, \mathrm{Id}_A) : (G, A) \to (H, A)$. The induced map $\mathrm{Res} : H^i(G, A) \to H^i(H, A)$ is called the **restriction map**.

Remark 3.9.5. We may describe restriction maps more simply than this, and connect this with the description of induced maps in Definition 3.2.5. We may represent an element of $H^i(G,A)$ by an i-cocycle $f : G^i \to A$ (recall that f being a cocycle just means $f \in Z^i(G,A) = \ker d_A^i$). On cocycles, we have the map

$$\text{Res} : Z^i(G,A) \to Z^i(H,A) \qquad f \mapsto f|_H$$

which respects the equivalence classes of $H^i(G,A)$, so we may think of $\text{Res} : H^i(G,A) \to H^i(H,A)$ as this "same" map, $f \mapsto f|_H$.

$$\text{Res} : H^i(G,A) \to H^i(H,A) \qquad [f] \mapsto [f|_H]$$

In degree zero, where $H^0(G,A) \cong A^G, H^0(H,A) = A^H$, the restriction map is just the inclusion $A^G \hookrightarrow A^H$.

Definition 3.9.6. Let $H \subset G$ be a subgroup. We have a homology compatible pair of the inclusion $e : H \hookrightarrow G$ with the $\text{Id}_A : A \to A$, which induces a map on homology

$$\text{Cor} : H_i(H,A) \to H_i(G,A)$$

This is called the **corestriction map**. In degree zero, corestriction is just the quotient map

$$A_H = A/I_H A \to \frac{A/I_H A}{I_G A/I_H A} \cong A/I_G A = A_G$$

Definition 3.9.7. Let $H \subset G$ be a normal subgroup, and let $q : G \to G/H$ be the quotient map. Let A be a G-module, and let $\iota : A^H \hookrightarrow A$ be the inclusion. Then $(q,\iota) : (G/H, A^H) \to (G,A)$ forms a compatible pair. The induced map on cohomology is called the **inflation map**, and denoted $\text{Inf} : H^i(G/H, A^H) \to H^i(G,A)$.

Remark 3.9.8. As in Remark 3.9.5, we can describe inflation more concretely on i-cocycles. On cocycles, inflation is given by

$$\text{Inf} : Z^i(G/H, A^H) \to Z^i(G,A) \qquad f \mapsto \Big(g \mapsto f(\overline{g})\Big)$$

Note that here $g \in G^i$, so by $\overline{g}$, we mean the class of g in $(G/H)^i$. In degree zero, where $H^0(G,A) \cong A^G, H^0(G/H, A^H) \cong (A^H)^{G/H} \cong A^G$, inflation is just the identity map.

Remark 3.9.9. The restriction maps $\text{Res} : H^i(G,A) \to H^i(H,A)$ provide a morphism of δ-functors $H^i(G,-) \to H^i(H,-)$ (but we omit the proof). All this means is that if we have a short exact sequence $0 \to A \to B \to C \to 0$ of G-modules, the following diagram commutes.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H^i(G,A) & \longrightarrow & H^i(G,B) & \longrightarrow & H^i(G,C) & \xrightarrow{\delta} & H^{i+1}(G,A) & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} & & \downarrow{\scriptstyle \text{Res}} & & \\
\cdots & \longrightarrow & H^i(H,A) & \longrightarrow & H^i(H,B) & \longrightarrow & H^i(H,C) & \xrightarrow{\delta} & H^{i+1}(H,A) & \longrightarrow & \cdots
\end{array}$$

The main content of this diagram is the squares involving connecting homomorphisms δ, since the other squares commute just because Res is a natural transformation. So one can think of a morphism of δ-functors as a family of natural transformations which are also compatible with connecting homomorphisms.

Cor and Inf are also morphisms of δ-functors, but again we provide no proof of this fact.

3.9.3 Extending Res and Cor

From the previous section, for a subgroup $H \subset G$, we have maps

$$\text{Res} : H^i(G, A) \to H^i(H, A) \qquad \text{Cor} : H_i(G, A) \to H_i(H, A)$$

So Res is defined on cohomology, and Cor is defined on homology. We want both Res and Cor to be defined for cohomology and homology, so in this section we work toward that goal, in the case where H has finite index (see Proposition 3.9.15). We will also obtain restriction and corestriction maps on Tate cohomology. The case of Tate cohomology is simplest, so we start there.

Definition 3.9.10. Let G be a finite group and $H \subset G$ a subgroup. Let A be a G-module. By dimension shifting, we have isomorphism

$$\widehat{H}^{i-1}(G, A) \cong \widehat{H}^i(G, A_*) \qquad \widehat{H}^{i-1}(H, A) \cong \widehat{H}^i(H, A_*)$$

For $i \geq 1$, we already have restriction maps

$$\text{Res} : \widehat{H}^i(G, A_*) \to \widehat{H}^i(H, A_*)$$

for $i \leq 0$, so we may define $\text{Res} : \widehat{H}^{i-1}(G, A) \to \widehat{H}^{i-1}(H, A)$ to be the unique map making the following square commute.

$$\begin{array}{ccc} \widehat{H}^{i-1}(G, A) & \xrightarrow{\cong} & \widehat{H}^i(G, A_*) \\ \vdots\,\text{Res} & & \downarrow\text{Res} \\ \widehat{H}^{i-1}(H, A) & \xrightarrow{\cong} & \widehat{H}^i(H, A_*) \end{array}$$

This inductively defines restriction maps on all Tate cohomology groups. Note that by the previous remark, these squares commute for $i \geq 1$ as well.

Definition 3.9.11. Following the same procedure as above, we already have corestriction maps on Tate cohomology for $i \leq -2$, so using the same isomorphisms as above, inductively define Cor for $i > -2$ to be the unique map making the following square commute.

$$\begin{array}{ccc} \widehat{H}^{i-1}(H, A) & \xrightarrow{\cong} & \widehat{H}^i(H, A_*) \\ \downarrow\text{Cor} & & \vdots\,\text{Cor} \\ \widehat{H}^{i-1}(G, A) & \xrightarrow{\cong} & \widehat{H}^i(G, A_*) \end{array}$$

Remark 3.9.12. The previous definitions serve to give restriction maps on homology and corestriction maps on cohomology in the case that G is finite, since that is when Tate cohomology makes sense. We would like to have them even when G is not finite, though, so we need a bit more work. Even still, it will only work if $[G : H]$ is finite.

The general strategy is to define Res on H_0, then use dimension shifting to inductively define it on all other homology groups. Similarly, we'll define Cor on H^0 and dimension shift.

Definition 3.9.13. Let G be a group and $H \subset G$ a subgroup of finite index and A a G-module. Regardless of whether H is normal, view G/H as a coset space, and define

$$\text{Res} : H_0(G, A) \to H_0(H, A) \qquad x \mapsto \sum_{gH \in G/H} g\widetilde{x}$$

where for $x \in A_G = H_0(G, A) = A/I_G A$, the element $\widetilde{x}$ is any lift of $x \in A_H$ under the quotient map $A_H \to A_G$. Similarly, define

$$\text{Cor} : H^0(H, A) \to H^0(G, A) \qquad y \mapsto \sum_{gH \in G/H} gy$$

where $y \in A^H$.

Lemma 3.9.14. *The maps* Res *and* Cor *defined above are well defined.*

Proof. We can handle the issue of coset representatives for both maps at once. We need to check that for $\widetilde{x} \in A_H$ or $y \in A^H$, the sums

$$\sum_{gH \in G/H} g\widetilde{x} \qquad \sum_{gH \in G/H} gy$$

are independent of the choice of coset representatives. Let $g_1, \ldots, g_n$ and $\sigma_1, \ldots, \sigma_n$ be two sets of coset representatives for H, where $n = [G : H]$, and $\sigma_i^{-1} g_i \in H$ (that is, g_i and σ_i represent the same coset). Then

$$\sum_{i=1}^{n} g_i \widetilde{x} = \sum_{i=1}^{n} (\sigma_i \sigma_i^{-1}) g_i \widetilde{x} = \sum_{i=1}^{n} \sigma_i (\sigma_i^{-1} g_i \widetilde{x}) = \sum_{i=1}^{n} \sigma_i \widetilde{x}$$

The last equality follows from the fact that $\widetilde{x} \in A_H$, so the action of H on $\widetilde{x}$ is trivial, and $\sigma_i^{-1} g_i \in H$. The same symbol-pushing works for an element of A^H as well. Thus Cor is well defined, and Res is well defined at least with respect to the issue of coset representatives.

Now we show that Res does not depend on the choice of lift of x. Let $\widetilde{x}, \widetilde{y} \in A_H$ both be lifts of $x \in A_G$. Then by definition of the quotient map below,

$$A_H = A/I_H A \to \frac{A/I_H A}{I_G A/I_H A} \cong A/I_G A = A_G$$

we must have $\widetilde{x} - \widetilde{y} \in I_G A/I_H A$. Then we can write $\widetilde{x} - \widetilde{y}$ as a finite sum

$$\widetilde{x} - \widetilde{y} = \sum \sigma, a(\sigma - 1)a$$

where $\sigma \in G \setminus H, a \in A$. Then

$$\begin{aligned} \sum_{gH \in G/H} g\widetilde{x} - \sum_{gH \in G/H} g\widetilde{y} &= \sum_{gH \in G/H} g(\widetilde{x} - \widetilde{y}) \\ &= \sum_{gH \in G/H} \sum_{\sigma, a} g(\sigma - 1)a \\ &= \sum_{gH \in G/H} \sum_{\sigma, a} g\sigma a - \sum_{gH \in G/H} \sum_{\sigma, a} ga \end{aligned}$$

For any $\sigma \in G$, as g ranges over cosets of H, the elements σg also range over cosets of H, so the two sums above are the same sum. Hence the difference is zero, so

$$\sum_{gH \in G/H} g\widetilde{x} = \sum_{gH \in G/H} g\widetilde{y}$$

proving that Res is well defined. □

Proposition 3.9.15. *Let G be a group and H a subgroup of finite index. There are maps*

$$\mathrm{Res} : H_i(G, A) \to H_i(H, A) \qquad \mathrm{Cor} : H^i(H, A) \to H^i(G, A)$$

for all $i \geq 0$ that coincide with the maps of Definition 3.9.13 for $i = 0$ and that provide morphisms of δ-functors

$$H^i(G, -) \implies H^i(H, -) \qquad H^i(H, -) \implies H^i(G, -)$$

Proof. Consider the long exact sequences on homology induced by the short exact sequence

$$0 \to A_* \to \mathrm{Ind}^G(A) \to A \to 0$$

They give the following commutative diagram.

$$\begin{array}{ccccccc}
H_1(G, \mathrm{Ind}^G(A)) = 0 & \longrightarrow & H_1(G, A) & \longrightarrow & H_0(G, A_*) & \longrightarrow & H_0(G, \mathrm{Ind}^G(A)) \\
 & & & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
H_1(H, \mathrm{Ind}^G(A)) = 0 & \longrightarrow & H_1(H, A) & \longrightarrow & H_0(H, A_*) & \longrightarrow & H_0(H, \mathrm{Ind}^G(A))
\end{array}$$

Then define $\mathrm{Res} : H_1(G, A) \to H_1(H, A)$ to be the induced map on kernels, making the following diagram commute.

$$\begin{array}{ccccccc}
0 & \longrightarrow & H_1(G, A) & \longrightarrow & H_0(G, A_*) & \longrightarrow & H_0(G, \mathrm{Ind}^G(A)) \\
 & & \vdots{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
0 & \longrightarrow & H_1(H, A) & \longrightarrow & H_0(H, A_*) & \longrightarrow & H_0(H, \mathrm{Ind}^G(A))
\end{array}$$

Having defined Res on H_1, we now proceed as in the case of Tate cohomology to use dimension shifting to define Res on H_i for $i \geq 2$. From dimension shifting, we have isomorphisms

$$H_{i+1}(G, A) \cong H_i(G, A_*) \qquad H_{i+1}(H, A) \cong H_i(H, A_*)$$

so we inductively define Res on H_{i+1} to be the unique map making the following square commute.

$$\begin{array}{ccc}
H_{i+1}(G, A) & \xrightarrow[\delta]{\cong} & H_i(G, A_*) \\
\vdots{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} \\
H_{i+1}(H, A) & \xrightarrow[\delta]{\cong} & H_i(H, A_*)
\end{array}$$

So by construction Res maps commute with the connecting homomorphisms from the LES. In total analogy with everything we just did, define Cor on H^1 by considering the long exact sequences associated to

$$0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$$

then define Cor inductively on H^{i+1} to be the unique map making the following square commute.

$$\begin{array}{ccc} H^{i+1}(G,A) & \xrightarrow[\delta]{\cong} & H^i(G,A^*) \\ \vdots\,\mathrm{Cor} & & \downarrow\mathrm{Cor} \\ H^{i+1}(H,A) & \xrightarrow[\delta]{\cong} & H^i(H,A^*) \end{array}$$

□

We have now defined Res and Cor for all H^i, H_i with $i \geq 1$.

Remark 3.9.16. We don't go into all the detail of δ-functors here, but roughly speaking, a δ-functor is a family of functors indexed by $\mathbb{Z}_{\geq 0}$ which turns short exact sequences into long exact sequences. So the prime example of a δ-functor is any family of derived functors, such as group cohomology $H^i(G,-)$ or group homology $H_i(G,-)$.

Roughly speaking, a morphism of δ-functors is a family of natural transformations which induce a chain map between the induced long exact sequences. So saying that Res and Cor are a morphism of δ-functors is asserting commutativity of some large diagram involving the long exact sequences of homology/cohomology.

3.9.4 Composition $\mathrm{Cor} \circ \mathrm{Res}$ and applications

Let H be a subgroup of finite index in a group G. What can we say about the follwoing composition?

$$H^i(G,A) \xrightarrow{\mathrm{Res}} H^i(H,A) \xrightarrow{\mathrm{Cor}} H^i(G,A)$$

It turns out that we can say exactly what this composition is, and as an endomorphism of $H^i(G,A)$, this will tell us a lot about $H^i(G,A)$, in particular when it is torsion, and about p-primary torsion subgroups for primes p.

Proposition 3.9.17. *Let G be a group and H a subgroup of finite index. Then the maps*

$$\begin{aligned} \mathrm{Cor}\,\mathrm{Res} &: H^i(G,A) \to H^i(G,A) \\ \mathrm{Cor}\,\mathrm{Res} &: H_i(G,A) \to H_i(G,A) \\ \mathrm{Cor}\,\mathrm{Res} &: \widehat{H}^i(G,A) \to \widehat{H}^i(G,A) \end{aligned}$$

are multiplication by $[G:H]$. (Note that the last map is only defined in the case where G is finite.)

Proof. We just prove this for regular cohomology, the proofs for homology and Tate cohomoloy are similar. First we prove the case $i = 0$. In degree zero, Res is the inclusion and Cor is given by the formula in Definition 3.9.13.

$$\mathrm{Cor}\,\mathrm{Res} : A^G \to A^G \qquad y \mapsto \sum_{gH \in G/H} gy$$

Since $y \in A^G$, the sum on the right is just $[G:H]$ copies of y, so the map is as claimed. Now we inductively prove it for higher degrees by dimension shifting. The induction is basically contained in the following commutative diagram.

$$\begin{array}{ccc} H^{i+1}(G,A) & \xrightarrow{\cong} & H^i(G,A^*) \\ \Big\downarrow{\scriptstyle \mathrm{Res}} & & \Big\downarrow{\scriptstyle \mathrm{Res}} \\ H^{i+1}(H,A) & \xrightarrow{\cong} & H^i(H,A^*) \\ \Big\downarrow{\scriptstyle \mathrm{Cor}} & & \Big\downarrow{\scriptstyle \mathrm{Cor}} \\ H^{i+1}(G,A) & \xrightarrow{\cong} & H^i(G,A^*) \end{array} \qquad \Big\}{\scriptstyle [G:H]}$$

The bottom square commutes by definition of Cor on cohomology. The top square commutes because Res as defined by compatible pairs is a morphism of δ-functors. □

We get a very useful consequence of this is when G is finite.

Corollary 3.9.18. *Let G be a finite group. Then for any G-module A and any $i \in \mathbb{Z}_{\geq 1}$, $H^i(G,A)$ is a torsion group of exponent $|G|$.*

Proof. Take H to be the trivial subgroup in Proposition 3.9.17, and note that $H^i(H,A) = 0$ for any A and $i > 0$. Thus multiplication by $|G|$ is the same as the zero map on $H^i(G,A)$.

$$H^i(G,A) \xrightarrow{\mathrm{Res}} H^i(H,A) = 0 \xrightarrow{\mathrm{Cor}} H^i(G,A)$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{|G|}$$

□

Note that it is not at all clear how one might prove that $H^i(G,A)$ has exponent $|G|$ just by thinking about cocycles, so we really did get something out of all our compatible pairs technology that we couldn't have gotten without it. The next corollary is another great example of this.

Corollary 3.9.19. *Let G be a finite group. For each prime p, fix a Sylow p-subgroup $G_p \subset G$. Then*

1. *The kernel of*
$$\mathrm{Res} : \widehat{H}^i(G,A) \to \widehat{H}^i(G_p,A)$$
has no elements of order p^n for any $n \geq 1$. Another way to say this is that Res *is injective on the p-primary component of $\widehat{H}^i(G,A)$. (Milne 1.33 [9])*

2. *If for some $i \in \mathbb{Z}$, all the maps*
$$\mathrm{Res} : \widehat{H}^i(G,A) \to \widehat{H}^i(G_p,A)$$
are trivial for each prime p, then $\widehat{H}^i(G,A) = 0$.

Proof. (1) Suppose $\alpha \in \widehat{H}^i(G,A)$ has order p^n, so $p^n\alpha = 0$ for some $n \geq 1$. By Proposition 3.9.17,

$$\operatorname{Cor}\operatorname{Res}(\alpha) = [G : G_p]\alpha$$

Since G_p is a Sylow p-subgroup, $[G : G_p]$ is coprime to p, and since α has order p^n, $[G : G_p]\alpha \neq 0$. Thus α is not in the kernel of $\operatorname{Cor}\operatorname{Res}$, so α is not in the kernel of Res.

(2) By (1), if $\operatorname{Res} : \widehat{H}^i(G,A) \to \widehat{H}^i(G_p,A)$ is the zero map, then $\widehat{H}^i(G,A)$ has no elements of p-power order. Thus if the restriction maps are zero for all p, then $\widehat{H}^i(G,A)$ has no elements of p-power order for any prime p, which is only possible if $\widehat{H}^i(G,A) = 0$. □

3.9.5 Inflation restriction sequence

We addressed the composition of Cor and Res, at least in the case where the subgroup involved has finite index. There is also a natural composition of Inf and Res, which turns out to be very useful as well. The best way to describe this is actually using the language of spectral sequences, but we don't have space for all of that here.

Proposition 3.9.20 (Inflation restriction sequence)**.** *Let $N \subset G$ be a normal subgroup, and let A be a G-module. The follow sequence is exact.*

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\text{Inf}} H^1(G,A) \xrightarrow{\text{Res}} H^1(N,A) \xrightarrow{\tau} H^2(G/N, A^N) \xrightarrow{\text{Inf}} H^2(G,A)$$

The map τ is something I don't understand, but it seems to be quite complicated to describe.

An incomplete proof of the above is given in Theorem 4.1.20 of Rosenberg [13]. A confusing proof is given in Proposition 3.3.16 of Gille & Szamuely [4]. A proof utilizing spectral sequences is given in Proposition 6.8.2 and Remark 6.8.3 of Weibel [16].

In lieu of a full proof of exactness for the inflation-restriction sequence, we can at least give a proof here of exactness for the first three terms, just involving Inf and Res. See below for a proof of exactness for just the first three terms, following Theorem 1.8.10 of Sharifi [15]. First, we recall the descriptions of Inf and Res in terms of cocycles.

Remark 3.9.21. Let G be a group with a normal subgroup N and let A be a G-module. For a cocycle $\phi : G/N \to A^N$ and for $g \in G$, we have a cocycle in $Z^1(G,A)$ described by

$$\widetilde{\text{Inf}}(\phi) : G \to A \qquad \widetilde{\text{Inf}}(\phi)(g) = \phi(\overline{g})$$

where $\overline{g} = gN$ is the image of g in G/N. That is to say, there is a map

$$\widetilde{\text{Inf}} : Z^1(G,A) \to Z^1(G/N, A^N) \qquad \phi \mapsto (g \mapsto \phi(\overline{g}))$$

In these terms, $\text{Inf}[\phi] = [\widetilde{\text{Inf}}(\phi)]$. The previous equality is represented by the following commutative square, where the vertical arrows are quotient maps.

$$\begin{array}{ccc} Z^1(G/N, A^N) & \xrightarrow{\widetilde{\text{Inf}}} & Z^1(G,A) \\ \downarrow & & \downarrow \\ H^1(G/N, A^N) & \xrightarrow{\text{Inf}} & H^1(G,A) \end{array}$$

Remark 3.9.22. Now we recall the description of Res in terms of cocycles. Let G be a group with a subgroup N and let A be a G-module. The literal function restriction map

$$Z^1(G,A) \to Z^1(N,A) \qquad \psi \mapsto \psi|_H$$

induces Res, which is to say $\mathrm{Res}[\psi] = [\psi|_N]$. We represent this with the following commutative square, where vertical arrows are quotient maps.

$$\begin{array}{ccc} Z^1(G,A) & \xrightarrow{\psi \mapsto \psi|_N} & Z^1(N,A) \\ \downarrow & & \downarrow \\ H^1(G,A) & \xrightarrow{\mathrm{Res}} & H^1(N,A) \end{array}$$

Proposition 3.9.23 (Partial inflation restriction sequence)**.** *Let G be a group and $N \subset G$ a normal subgroup, and let A be a G-module. Then the following sequence is exact.*

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(N,A)$$

Proof. First, we show Inf is injective (which gives exactness at the first term). Let $[\phi] \in H^1(G/N, A^N)$ with representative cocycle ϕ such that $[\phi] \in \ker \mathrm{Inf}$, so $\mathrm{Inf}[\phi] = [\widetilde{\mathrm{Inf}}(\phi)] = 0 \in H^1(G,A)$. That is, $\widetilde{\mathrm{Inf}}(\phi)$ is a coboundary, which in degree one means that there exists $a \in A$ so that for all $g \in G$,

$$\widetilde{\mathrm{Inf}}(\phi)(g) = \phi(\overline{g}) = (g-1)a$$

In particular, for $n \in N$,

$$0 = \phi(\overline{n}) = (n-1)a$$

so $a \in A^N$. Then reusing the previous equality, we have $a \in A^N$ such that

$$\phi(\overline{g}) = (g-1)a = (\overline{g}-1)a$$

which is exactly the condition for ϕ to be a coboundary. Thus $[\phi] = 0$, and Inf is injective.

Now we need exactness at $H^1(G,A)$. We can easily get $\mathrm{im}\,\mathrm{Inf} \subset \ker \mathrm{Res}$ by showing that $\mathrm{Res} \circ \mathrm{Inf} = 0$. Let $[\phi] \in H^1(G/N, A^N)$ with representative cocycle ϕ. Then

$$\mathrm{Res} \circ \mathrm{Inf}[\phi] = \mathrm{Res}[\widetilde{\mathrm{Inf}}(\phi)] = [\widetilde{\mathrm{Inf}}(\phi)|_N]$$

But just as a cocycle, $\widetilde{\mathrm{Inf}}(\phi)|_N$ is zero, because for $n \in N$,

$$\widetilde{\mathrm{Inf}}(\phi)|_N(n) = \phi(\overline{n}) = \phi(1) = 0$$

[2] Thus $\mathrm{Res} \circ \mathrm{Inf} = 0$. Now we need to show $\ker \mathrm{Res} \subset \mathrm{im}\,\mathrm{Inf}$. Let $[\alpha] \in \ker \mathrm{Res} \subset H^1(G,A)$, with representative cocycle $\alpha \in Z^1(G,A)$. Since $\mathrm{Res}[\alpha] = [\alpha|_N] = 0$, $\alpha|_N$ is a coboundary, so there exists $a \in A$ such that for all $n \in N$, $\alpha(n) = (n-1)a$. Define

$$\beta : G \to A \qquad \beta(g) = \alpha(g) - (g-1)a$$

[2] Note that a cocycle vanishes on the identity. This follows from the cocycle relation: $\phi(x) = \phi(1x) = 1\phi(x) + \phi(1) \implies \phi(1) = 0$.

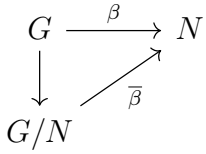
This is defined so that for $n \in N$,

$$\beta(n) = \alpha(n) - (n-1)a = 0$$

Note that $\beta \in Z^1(G, A)$, since it differs from the cocylce α by a coboundary $(g-1)a$, which also means $[\beta] = [\alpha] \in H^1(G, A)$. Also, for $g \in G, n \in N$,

$$\beta(gn) = g\beta(n) + \beta(g) = \beta(g)$$

so β factors through G/N, meaning that there is a map $\overline{\beta}$ making the following diagram commute, which is to say, $\overline{\beta}(\overline{g}) = \beta(g)$.



Also, for $g \in G, n \in N$,

$$\begin{aligned} n\beta(g) &= n\beta(g) + \beta(n) = \beta(ng) \\ &= \beta(gg^{-1}ng) = g\beta(g^{-1}ng) + \beta(g) = \beta(g) \end{aligned}$$

the last equality uses normality of N to say that $g^{-1}ng \in N$. Thus the image of β lands in A^N, so $\overline{\beta} \in H^1(G/N, A^N)$. Finally, it is immediate that $\widetilde{\text{Inf}}(\overline{\beta}) = \beta$, so

$$\text{Inf}[\,\overline{\beta}\,] = [\widetilde{\text{Inf}}(\overline{\beta})] = [\beta] = [\alpha]$$

proving $\ker \text{Res} \subset \text{im}\, \text{Inf}$. □

There is also a generalization of the inflation restriction sequence for higher cohomology groups, but with additional hypotheses involving vanishing of smaller cohomology groups. We don't prove this one even for the first few terms.

Proposition 3.9.24 (Generalized inflation restriction sequence)**.** *Let $N \subset G$ be a normal subgroup, and let A be a G-module. Let $i \geq 1$, and suppose that $H^j(N, A) = 0$ for $1 \leq j \leq i-1$. The follow sequence is exact.*

$$0 \longrightarrow H^i(G/N, A^N) \xrightarrow{\text{Inf}} H^i(G, A) \xrightarrow{\text{Res}} H^i(N, A) \xrightarrow{\tau_{i,A}} H^{i+1}(G/N, A^N) \xrightarrow{\text{Inf}} H^{i+1}(G, A)$$

Proof. See Sharifi 1.8.11 [15] or Gille and Szamuely 3.3.19 [4]. Sharifi only includes the first three nonzero terms, the others come from CSAGC. The map $\tau_{i,A}$ does not seem to have a simple description. This is really coming from the Hochschild-Serre spectral sequence. □

The following exercise from Rosenberg [13] gives an application of the inflation-restriction sequence.

Proposition 3.9.25 (Exercise 4.1.30 of Rosenberg [13]). *Let G be an abelian group and choose a free resolution of G*

$$0 \to F_1 \xrightarrow{i} F_0 \xrightarrow{\pi} G \to 0$$

with F_1, F_0 free abelian. View $\mathbb{Z}$ as a trivial module for F_0 and G. Then the induced map $\pi_* : H_2(F_0, \mathbb{Z}) \to H_2(G, \mathbb{Z})$ is surjective.

Proof. (Note that all hom groups in this proof are over $\mathbb{Z}$.) Let A be an abelian group, viewed as trivial module over G, F_0, F_1. The inflation-restriction sequence 3.9.20 is

$$0 \longrightarrow \mathrm{Hom}(G, A) \xrightarrow{\mathrm{Inf}} \mathrm{Hom}(F_0, A) \xrightarrow{\mathrm{Res}} \mathrm{Hom}(F_1, A) \xrightarrow{\tau} H^2(G, A) \xrightarrow{\mathrm{Inf}} H^2(F_0, A)$$

We also have a long exact sequence associated to $0 \to F_1 \to F_0 \to G \to 0$ from the functors $\mathrm{Ext}_{\mathbb{Z}}(-, A)$. Note that $\mathrm{Ext}^1_{\mathbb{Z}}(F_0, A) = 0$ because F_0 is a projective $\mathbb{Z}$-module.

$$0 \longrightarrow \mathrm{Hom}(G, A) \xrightarrow{\pi_*} \mathrm{Hom}(F_0, A) \xrightarrow{i_*} \mathrm{Hom}(F_1, A) \xrightarrow{\delta} \mathrm{Ext}^1_{\mathbb{Z}}(G, A) \longrightarrow 0$$

Note that the following diagram commutes. This follows from thinking about what Inf and Res do in terms of cocycles. Our next step is to define α making this commute.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(G, A) & \xrightarrow{\pi_*} & \mathrm{Hom}(F_0, A) & \xrightarrow{i_*} & \mathrm{Hom}(F_1, A) & \xrightarrow{\delta} & \mathrm{Ext}^1_{\mathbb{Z}}(G, A) \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow{\scriptstyle \mathrm{Id}} & & \vdots{\scriptstyle \alpha} \\
0 & \longrightarrow & \mathrm{Hom}(G, A) & \xrightarrow{\mathrm{Inf}} & \mathrm{Hom}(F_0, A) & \xrightarrow{\mathrm{Res}} & \mathrm{Hom}(F_1, A) & \xrightarrow{\tau} & H^2(G, A) \xrightarrow{\mathrm{Inf}} H^2(F_0, A)
\end{array}$$

We define $\alpha : \mathrm{Ext}^1_{\mathbb{Z}}(G, A) \to H^2(G, A)$ as follows. Take $x \in \mathrm{Ext}^1_{\mathbb{Z}}(G, A)$, and take a lift $\widetilde{x} \in \mathrm{Hom}(F_1, A)$, so that $\delta(\widetilde{x}) = x$. Then define $\alpha(x) = \tau(\widetilde{x})$. To see that this is well defined, suppose $\widetilde{x}, \widetilde{y}$ are both lifts. Then

$$\delta(\widetilde{x} - \widetilde{y}) = 0 \implies \widetilde{x} - \widetilde{y} \in \ker \delta = \mathrm{im}\,\mathrm{Res} = \ker \tau \implies \tau(\widetilde{x} - \widetilde{y}) = 0 \implies \tau(\widetilde{x}) = \tau(\widetilde{y})$$

Hence α is well defined. By construction, the square involving α commutes. Now we claim that α is injective. Let $x \in \ker \alpha$. Then there exists $\widetilde{x} \in \mathrm{Hom}(F_1, A)$ such that $\delta(\widetilde{x}) = x$ and $\tau(\widetilde{x}) = 0$, so $\widetilde{x} \in \ker \tau = \mathrm{im}\,\mathrm{Res} = \ker \delta$. That is, $\delta(\widetilde{x}) = x = 0$, so α is injective.

Now observe that $\ker \mathrm{Inf} = \mathrm{im}\,\tau = \mathrm{im}(\alpha\delta) = \mathrm{im}\,\alpha$ since δ is surjective. Thus α gives an isomorphism between $\mathrm{Ext}^1_{\mathbb{Z}}(G, A)$ and $\ker \mathrm{Inf}$.

Leaving α and the previous diagram aside for the moment, note that $H_1(G, \mathbb{Z}) \cong G$ and $H_1(F_0, \mathbb{Z}) \cong F_0$ by Proposition 3.6.7. From the universal coefficient theorem 3.6.10, we get $H^2(F_0, A) \cong \mathrm{Hom}(H_2(F_0, \mathbb{Z}), A)$ because the Ext term vanishes. Again using the universal coefficient theorem 3.6.10, we have a split short exact sequence in the top row of the following commutative diagram. Our next step is to define β making this diagram commute.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Ext}^1_{\mathbb{Z}}(G, A) & \longrightarrow & H^2(G, A) & \xrightarrow{\gamma} & \mathrm{Hom}_{\mathbb{Z}}(H_2(G, \mathbb{Z}), A) & \longrightarrow & 0 \\
 & & \cong\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{Id}} & & \vdots{\scriptstyle \beta} & & \\
0 & \longrightarrow & \ker \mathrm{Inf} & \longrightarrow & H^2(G, A) & \xrightarrow{\mathrm{Inf}} & H^2(F_0, A) & &
\end{array}$$

We define $\beta : \mathrm{Hom}(H_2(G,\mathbb{Z}),A) \to H^2(F_0,A)$ as follows. For $x \in \mathrm{Hom}(H_2(G,\mathbb{Z}),A)$, take a lift $\widetilde{x}$ so that $\gamma(\widetilde{x}) = x$, then set $\beta(x) = \mathrm{Inf}(\widetilde{x})$. This is well defined by the same argument as for α: if $\widetilde{x}, \widetilde{y}$ are both lifts, then

$$\widetilde{x} - \widetilde{y} \in \ker\gamma = \ker \mathrm{Inf} \implies \mathrm{Inf}(\widetilde{x}) = \mathrm{Inf}(\widetilde{y})$$

It is injective by the same argument as for α as well: if $x \in \ker\beta$, then there exists a lift $\widetilde{x}$ such that $\mathrm{Inf}(\widetilde{x}) = 0$, but then $0 = \mathrm{Inf}(\widetilde{x}) = x$. Using the isomorphism $H_2(F_0,A) \cong \mathrm{Hom}(H_2(F_0,\mathbb{Z}),A)$, β gives an injection

$$\mathrm{Hom}(H_2(G,\mathbb{Z}),A) \hookrightarrow \mathrm{Hom}(H_2(F_0,\mathbb{Z}),A)$$

Now since A was arbitrary, this is true for all abelian groups A. Then by a standard result about left exactness of the hom functor (see Lang [6] Proposition 2.1 of Chapter III), the map inducing these, namely $H_2(F_0,\mathbb{Z}) \to H_0(G,\mathbb{Z})$, is surjective, which is what we wanted to prove originally. □

3.10 Cohomological triviality

The main result of this section is Theorem 3.10.10, which gives equivalent conditions for when a module has vanishing cohomology for all subgroups of the given group. Most of the intermediate results to get there are forgettable, or at least, not that easy to remember since they all blend together.

In this section, all references to Cassels & Frohlich [1] are from chapter IV, section 9, which is the main source for this whole section. We also roughly follow Section 1.11 of Sharifi [15].

Definition 3.10.1. Let G be a finite group. A G-module A is **cohomologically trivial** if $\widehat{H}^i(H,A) = 0$ for all subgroups $H \subset G$ and all $i \in \mathbb{Z}$. (In particular, $\widehat{H}^i(G,A) = 0$ for all $i \in \mathbb{Z}$.)

Warning: It is NOT the case that if $\widehat{H}^i(G,A) = 0$ for all $i \in \mathbb{Z}$, then $\widehat{H}^i(H,A) = 0$ for all $i \in \mathbb{Z}$ and all subgroups. The cohomology groups $\widehat{H}^i(G,A)$ could all vanish, but for subgroups $H \subset G$, cohomology groups need not vanish.

Intuitively making G "smaller" should make $H^i(G,A)$ ''smaller", but this intuition needs to be abandoned because it's just not true. There is a containment on the level of cochains

$$C^i(H,A) \subset C^i(G,A)$$

and even a containment of cocycles

$$Z^i(H,A) \subset Z^i(G,A)$$

but the coboundaries $B^i(H,A)$ and $B^i(G,A)$ are not so simply related, and the quotients $H^i(G,A) = Z^i(G,A)/B^i(G,A)$ and $H^i(H,A) = Z^i(H,A)/B^i(H,A)$ are not related by any obvious containments.

Note: The following lemma is a repeat of Corollary 3.9.19, but we include it since this version of the proof has some nice diagrams.

Lemma 3.10.2 (Sharifi [15] 1.8.24)**.** *Let p be a prime, let G be a finite group, and let G_p be a Sylow p-subgroup. The restriction map* $\mathrm{Res} : H^r(G, M) \to H^r(G_p, M)$ *is injective on the p-primary component of $H^r(G, M)$.*

Proof. We know that $\mathrm{Cor} \circ \mathrm{Res} = [G : G_p]$.

$$H^r(G, M) \xrightarrow{\mathrm{Res}} H^r(G_p, M) \xrightarrow{\mathrm{Cor}} H^r(G, M), \qquad [G:G_p]$$

Since $\gcd([G : G_p], p) = 1$, restricting to the primary component, $\mathrm{Res} \circ \mathrm{Cor}$ is an isomorphism.

$$H^r(G, M)[p] \xrightarrow{\mathrm{Res}} H^r(G_p, M) \xrightarrow{\mathrm{Cor}} H^r(G, M)[p], \qquad [G:G_p], \quad \cong$$

Thus Res is injective and Cor is surjective in this situation. □

Remark 3.10.3. We will frequently use the hypothesis that an abelian group (or G-module) satisfies $pA = 0$ for a prime p. This is equivalent to saying that A is an $\mathbb{F}_p$-vector space.

Lemma 3.10.4 (Cassels & Frohlich [1] Lemma 1; Sharifi [15] 1.11.4)**.** *Let p be a prime number, G a p-group, and A a G-module such that $pA = 0$. Then the following are equivalent.*

1. $A = 0$
2. $H^0(G, A) = 0$
3. $H_0(G, A) = 0$

Proof. It is clear that (1) $\implies$ (2), (3).

(2) $\implies$ (1) Suppose $A \neq 0$, and let $x \in A$ be a nonzero element. Let B be the submodule generated by x. Then B is finite, with order p^n for some $n > 0$. The element $0 \in B$ is a fixed point of the G-action, and by Lemma 3.13.6, the number of fixed points is congruent to $|B| = p^n \bmod p$, so there are at least $p \geq 2$ fixed points. Thus $H^0(G, A) = A^G$ is nonzero.

(3) $\implies$ (1) Let $A' = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ be the $\mathbb{F}_p$-dual of A, and note $pA' = 0$. Then

$$H^0(G, A') \cong (A')^G \cong \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{Z}[G]}(H_0(G, A), \mathbb{F}_p)$$

Since $H_0(G, A) = 0$, this implies $H^0(G, A') = 0$. Then by (2) $\implies$ (1), $A' = 0$. Since A' is the dual of A, this implies $A = 0$. □

Lemma 3.10.5 (Cassels & Frohlich [1] Lemma 2; Sharifi [15] 1.11.15)**.** *Let p be a prime number, G a p-group, and A a G-module such that $pA = 0$. If $H_1(G, A) = 0$, then A is free as an $\mathbb{F}_p[G]$-module.*

Proof. Note that $H_0(G,A) = A_G = A/I_G A$ is an abelian group annihated by $|G| = p$, which is to say, it is an $\mathbb{F}_p$-module, so it has an $\mathbb{F}_p$-basis $\{e_i\}_{i\in I}$. For each e_i, let $a_i \in A$ be a lift.

Let $B \subset A$ be the submodule generated by all the a_i. Then the inclusion $B \hookrightarrow A$ induces an isomorphism $H_0(G,B) \to H_0(G,A)$. Consider the long exact sequence on homology associated to $0 \to B \to A \to B/A \to 0$.

$$\cdots \to H_0(G,B) \xrightarrow{\cong} H_0(G,A) \to H_0(G,A/B) \to 0$$

Since the first map is an isomorphism, by exactness $H_0(G,A/B) = 0$. Then by Lemma 3.10.4, $A/B = 0$, which is to say, the a_i generate A as an $\mathbb{F}_p[G]$-module.

Let F be the free $\mathbb{F}_p[G]$-module generated by the a_i, and let $\pi : F \to A, a_i \mapsto a_i$ be the quotient map, and let $R = \ker \pi$, so we have an exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \to R \to F \to A \to 0$$

By hypothesis $H_1(G,A) = 0$, so the long exact sequence on homology gives an exact sequence

$$0 \to H_0(G,R) \to H_0(G,F) \to H_0(G,A) \to 0$$

By construction of the a_i, the induced map $H_0(G,F) \to H_0(G,A)$ is an isomorphism, so by exactness $H_0(G,R) = 0$. Since $pR = 0$, by Lemma 3.10.4 this implies $R = 0$, which is to say, $F \cong A$ so A is free as an $\mathbb{F}_p[G]$-module. □

Theorem 3.10.6 (Cassels & Frohlich[1] Theorem 6; Sharifi [15] 1.11.6)**.** *Let p be a prime number, G a p-group, and A a G-module such that $pA = 0$. Then the following are equivalent.*

1. *A is a free $\mathbb{F}_p[G]$-module.*
2. *A is a coinduced G-module.*
3. *A is cohomologically trivial.*
4. *$\widehat{H}^n(G,A) = 0$ for some $n \in \mathbb{Z}$.*

Proof. We prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (1) and (3) $\iff$ (4).
(1) $\implies$ (2) We have an isomorphism

$$\mathrm{CoInd}^G(\mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{F}_p) \to \mathbb{F}_p[G] \qquad \phi \mapsto \sum_{g\in G} \phi(g)g$$

Then using $\oplus$-linearity of Hom, if A is a free $\mathbb{F}_p[G]$-module,

$$A \cong \bigoplus \mathbb{F}_p[G] \cong \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G], \bigoplus \mathbb{F}_p\right) = \mathrm{CoInd}^G\left(\bigoplus \mathbb{F}_p\right)$$

(2) $\implies$ (3) Previous result, immediate from Shapiro's lemma.
(3) $\implies$ (1) $H_1(G,A) \cong \widehat{H}^{-2}(G,A) = 0$, so by Lemma 3.10.5, A is a free $\mathbb{F}_p[G]$-module.
(3) $\implies$ (4) Obvious.

(4) $\implies$ (3) Recall the modules $A_* \cong I_G \otimes_{\mathbb{Z}} A$ and $A^* \cong \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$ used for dimension shifting, along with the exact sequences

$$0 \to A_* \to \mathrm{Ind}^G(A) \to A \to 0 \qquad 0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$$

Since $pA = 0$, we get $pA_* = 0$ and $pA^* = 0$ as well. Thus by dimension shifting, there is a G-module B (constructed by some interation of A_* or A^*) such that $pB = 0$ and

$$\widehat{H}^{j-2}(G, B) \cong \widehat{H}^{j+n}(G, A) \tag{3.10.1}$$

for all $j \in \mathbb{Z}$. In particular, $H_1(G, B) = \widehat{H}^{-2}(G, B) = \widehat{H}^n(G, A) = 0$, using the hypothesis (4). Then by Lemma 3.10.5, B is a free $\mathbb{F}_p[G]$-module, so by (1) $\implies$ (2), $\widehat{H}^i(B) = 0$ for all $i \in \mathbb{Z}$, so by isomorphism 3.10.1, $\widehat{H}^i(A) = 0$ for all $i \in \mathbb{Z}$. □

Theorem 3.10.7 (Cassels & Frohlich [1] Theorem 7; Sharifi [15] 1.11.7)**.** *Let p be a prime number, G a p-group, and A a G-module so that A is p-torsion free as an abelian group. Then the following are equivalent.*

1. *A is cohomologically trivial.*
2. *$\widehat{H}^n(G, A) = \widehat{H}^{n+1}(G, A) = 0$ for some $n \in \mathbb{Z}$.*
3. *A/pA is a free $\mathbb{F}_p[G]$-module.*

Proof. We prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).
(1) $\implies$ (2) Obvious.
(2) $\implies$ (3) Since A is p-torsion free, the sequence

$$0 \longrightarrow A \xrightarrow{\ p\ } A \longrightarrow A/pA \longrightarrow 0 \tag{3.10.2}$$

is exact. Using our hypothesis $\widehat{H}^n(G, A) = \widehat{H}^{n+1}(G, A) = 0$, part of the long exact sequence on Tate cohomology looks like

$$0 = \widehat{H}^n(G, A) \to \widehat{H}^n(G, A/pA) \to \widehat{H}^{n+1}(G, A) = 0$$

so $\widehat{H}^n(G, A/pA) = 0$ by exactness. Then by (4) $\implies$ (1) of Theorem 3.10.6, A/pA is a free $\mathbb{F}_p[G]$-module.
(3) $\implies$ (1) By (1) $\implies$ (3) of Theorem 3.10.6, $\widehat{H}^n(G, A/pA) = 0$ for all n, for any subgroup $H \subset G$ the long exact sequence on Tate cohomology $\widehat{H}^i(H, -)$ associated to the exact sequence 3.10.2 looks like

$$\cdots \longrightarrow 0 \longrightarrow \widehat{H}^n(H, A) \xrightarrow[\cong]{p} \widehat{H}^n(H, A) \longrightarrow 0 \longrightarrow \cdots$$

Since H is a p-group, $\widehat{H}^n(H, A)$ is annihilated by some power of p, which is to say, iterating the isomorphism above enough times makes it zero. But this is only possible of $\widehat{H}^n(H, A) = 0$ (for all $n \in \mathbb{Z}$), thus A is cohomologically trivial. □

Corollary 3.10.8 (Cassels & Frohlich [1]; Sharifi [15] 1.11.9)**.** *Let p be a prime number, G a p-group, and A a G-module which is a free abelian group and cohomologically trivial. Then if B is a p-torsion free G-module, the G-module $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ is cohomologically trivial.*

Proof. As B is p-torsion free, we have a short exact sequence of abelian groups

$$0 \longrightarrow B \xrightarrow{p} B \longrightarrow B/pB \longrightarrow 0$$

Since A is a free abelian group, it is projective, so the functor $\mathrm{Hom}_{\mathbb{Z}}(A,-)$ is exact, thus we have the following exact sequence of abelian groups, which also happens to be a sequence of G-modules.

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A,B) \xrightarrow{p} \mathrm{Hom}_{\mathbb{Z}}(A,B) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \longrightarrow 0$$

In particular, $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ has no p-torsion. Since any $\mathbb{Z}$-homomorphism $A \to B/pB$ factors through A/pA,

$$\mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB)$$

By (1) $\implies$ (3) of Theorem 3.10.7, A/pA is a free $\mathbb{F}_p[G]$-module. Let I be an indexing set for a basis of A/pA as an $\mathbb{F}_p[G]$-module. Then

$$\begin{aligned}
\mathrm{Hom}_{\mathbb{Z}}(A,B/pB) &\cong \mathrm{Hom}_{\mathbb{Z}}(A/pA,B/pB) \\
&\cong \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{i\in I}\mathbb{F}_p[G],B/pB\right) && A \text{ is free} \\
&\cong \prod_{i\in I}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{F}_p[G],B/pB) && \text{Hom commutes with products} \\
&\cong \prod_{i\in I}\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G],B/pB) && \text{Every } \mathbb{Z}\text{-hom on } \mathbb{F}_p \text{ lifts to a hom on } \mathbb{Z} \\
&\cong \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G],\prod_{i\in I}B/pB\right) && \text{Hom commutes with products}
\end{aligned}$$

Thus $\mathrm{Hom}_{\mathbb{Z}}(A,B/pB)$ is a coinduced G-module, and it is annihilated by p, so by (2) $\implies$ (1) of Theorem 3.10.6 it is a free $\mathbb{F}_p[G]$-module. By the first isomorphism theorem applied to the sequence 3.10,

$$\mathrm{Hom}_{\mathbb{Z}}(A,B/pB) \cong \mathrm{Hom}_{\mathbb{Z}}(A,B)/p\,\mathrm{Hom}_{\mathbb{Z}}(A,B)$$

Thus by (3) $\implies$ (1) of Theorem 3.10.7 (where the A of the theorem is our $\mathrm{Hom}_{\mathbb{Z}}(A,B)$), $\mathrm{Hom}_{\mathbb{Z}}(A,B)$ is cohomologically trivial. □

Theorem 3.10.9 (Cassels & Frohlich [1] Theorem 8; Sharifi [15] 1.11.8, 1.11.10)**.** *Let G a finite group, and A a G-module so that A is a free abelian group. For each prime p, choose a Sylow p-subgroup $G_p \subset G$. Then the following are equivalent.*

1. *A is cohomologically trivial.*

2. *A is cohomologically trivial as a G_p-module for each prime p.*

3. *A is a projective G-module.*

4. *A is a projective G_p-module for each prime p.*

Proof. We prove (2) $\implies$ (1) $\iff$ (3) $\implies$ (4) $\implies$ (2). Although proving (3) $\implies$ (1) is not necessary to complete the circle, we use it to prove (4) $\implies$ (2). Also, (1) $\implies$ (2) is not strictly necessarily, but it is immediate from the definition.

(2) $\implies$ (1) Let $H \subset G$ be a subgroup and let $H_p \subset H$ be a p-Sylow subgroup. The restriction map $\mathrm{Res} : \widehat{H}^i(H, A) \to \widehat{H}^i(H_p, A)$ is injective on the p-primary component. Since $H_p \subset G_p$, by cohomological triviality of G_p, $\widehat{H}^i(H_p, A) = 0$, so $\widehat{H}^i(H, A) = 0$.

(1) $\implies$ (3) Choose an exact sequence of G-modules $0 \to Q \to F \xrightarrow{\pi} A \to 0$ where F is a free G-module. Since A is $\mathbb{Z}$-free, the functor $\mathrm{Hom}_{\mathbb{Z}}(A, -)$ is exact, so the following sequence is an exact sequence of abelian groups, which also happens to be a sequence of G-modules.

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(A, Q) \to \mathrm{Hom}_{\mathbb{Z}}(A, F) \to \mathrm{Hom}_{\mathbb{Z}}(A, A) \to 0$$

Note that F is $\mathbb{Z}$-free, so Q is also $\mathbb{Z}$-free, in particular, Q is p-torsion free for any prime p. Since A is cohomologically trivial (by hypothesis), by Corollary 3.10.8, $\mathrm{Hom}_{\mathbb{Z}}(Q, A)$ is cohomologically trivial as a G_p-module for each p. Then by (2) $\implies$ (1), $\mathrm{Hom}_{\mathbb{Z}}(Q, A)$ is cohomologically trivial. From the long exact sequence on (non-Tate) group cohomology associated the previous sequence, we get an exact sequence

$$H^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, F) \to H^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) \to 0$$

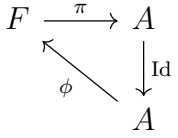
We may identify these with

$$H^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, F)) = \mathrm{Hom}_{\mathbb{Z}}(A, F)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, F)$$
$$H^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) = \mathrm{Hom}_{\mathbb{Z}}(A, A)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(A, A)$$

so the surjection on H^0 says that

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A, F) \to \mathrm{Hom}_{\mathbb{Z}[G]}(A, A) \qquad f \mapsto \pi \circ f$$

is surjective. In particular, the identity map $A \to A$ lifts to a map $\phi : A \to F$ such that $\pi \circ \phi = \mathrm{Id}$.



Thus the sequence $0 \to Q \to F \to A \to 0$ splits, so A is a direct summand of F, hence A is a projective $\mathbb{Z}[G]$-module.

(3) $\implies$ (4) Suppose $A \oplus Q = F$ is a free $\mathbb{Z}[G]$-module. Then F is also a free $\mathbb{Z}[G_p]$-module, hence A is also projective as a $\mathbb{Z}[G_p]$-module.

(3) $\implies$ (1) Let P be a projective $\mathbb{Z}[G]$-module, and choose Q so that $P \oplus Q$ is a free $\mathbb{Z}[G]$-module. Then since free $\mathbb{Z}[G]$-modules are cohomologically trivial,

$$\widehat{H}^i(G, P) \hookrightarrow \widehat{H}^i(G, P) \oplus \widehat{H}^i(G, Q) \cong \widehat{H}^i(G, P \oplus Q) = 0$$

which proves that P is cohomologically trivial.

(4) $\implies$ (2) Immediate from (3) $\implies$ (1). $\square$

Finally we have the main result of the section, which gives a very local criterion for cohomological triviality of a module A. It turns out that you just need vanishing of two consecutive cohomology groups for each p-Sylow subgroup, and that forces all of the cohomology groups for A to be zero.

Theorem 3.10.10 (Cassels & Frohlich [1] Theorem 9; Sharifi [15] 1.11.11)**.** *Let G be a finite group and A a G-module. For each prime p, fix a Sylow p-subgroup $G_p \subset G$. Then the following are equivalent.*

1. *A is cohomologically trivial.*
2. *For each prime p, there exists $n \in \mathbb{Z}$ such that $\widehat{H}^n(G_p, A) = \widehat{H}^{n+1}(G_p, A) = 0$.*
3. *There is an exact sequence $0 \to P_1 \to P_0 \to A \to 0$ where P_0, P_1 are projective G-modules.*

Proof. We prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).
(1) $\implies$ (2) Immediate from the definition.
(2) $\implies$ (3) Let $0 \to R \to F \to A \to 0$ be a short exact sequence of G-modules where F is $\mathbb{Z}[G]$-free. Note that F is also $\mathbb{Z}$-free, so R is also $\mathbb{Z}$-free as a subgroup of a free $\mathbb{Z}$-module. Then F is cohomologically trivial, so by considering the LES of Tate cohomology,

$$\widehat{H}^{j-1}(G_p, A) \cong \widehat{H}^j(G_p, R)$$

for every $j \in \mathbb{Z}$. Then by the hypothesis, $\widehat{H}^j(G_p, R)$ vanishes for two consecutive values of j. Since R is $\mathbb{Z}$-free, by Theorem 3.10.7, R is cohomologically trivial. Then by Theorem 3.10.9, R is a projective G-module.
(3) $\implies$ (1) Let $H \subset G$ be any subgroup. Since P_0, P_1 are cohomologically trivial, the LES of Tate cohomology $\widehat{H}^i(H, -)$ associated to $0 \to P_1 \to P_0 \to A \to 0$ implies that A is cohomologically trivial. $\square$

3.11 Cup products

The analogies with singular homology and algebraic topology continue - just as in that context, our cohomology theory has a cup product. This is perhaps the place where the geometric version has the biggest advantage, since they can often visualize cup products via intersections of subspaces or submanifolds, whereas for group cohomology the cup product has no such intuition.

Because of this, it is best to think of the cup product in group cohomology as simply the unique function with a laundry list of very nice properties. We will eventually show that just a few of the properties suffice to uniquely determine the cup product.

Of course, we also have a construction in terms of cochains. Despite this being very explicit, it is extremely rare for it to be useful for concrete computations. Unfortunately,

there are just not a lot of situations where we can explicitly compute cup products for specific examples.

Despite this, cup products are useful and important. Many important isomorphisms can be realized via cup product maps, such as Tate's theorem (see Theorem 3.7.10 and Theorem 3.7.12) and 2-periodicity of Tate cohomology for finite groups (see Proposition 3.7.8 and Proposition 1.10.3 of Sharifi [15]). Much later, we will also use cup products to realize isomorphisms involving Brauer groups and formulating the Merkurjev-Suslin theorem (see Proposition 5.8.16).

3.11.1 Construction of cup product

We start by constructing a somewhat explicit map in terms of projective resolutions and/or in terms of cochains. These will lead to the same place, but we include both for full disclosure.

Definition 3.11.1. Let G be a group, and consider the standard projective resolution $P_\bullet \to \mathbb{Z} \to 0$ where $P_i = \mathbb{Z}[G^{i+1}]$ (3.1.11). Define

$$\kappa_{ij} : P_{i+j} \to P_i \otimes_{\mathbb{Z}} P_j \qquad \kappa_{ij}(g_0, \dots, g_{i+j}) = (g_0, \dots, g_i) \otimes (g_i, \dots, g_{i+j})$$

Let A, B be G-modules. Define the map

$$\begin{aligned} \psi_{ij} : \operatorname{Hom}_{\mathbb{Z}[G]}(P_i, A) \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}[G]}(P_j, B) &\to \operatorname{Hom}_{\mathbb{Z}[G]}(P_i \otimes_{\mathbb{Z}} P_j, A \otimes_{\mathbb{Z}} B) \\ \phi \otimes \phi' &\mapsto \Big(\alpha \otimes \beta \mapsto \phi(\alpha) \otimes \phi'(\beta)\Big) \end{aligned}$$

Finally, define the **"preliminary" cup product** map by

$$\operatorname{Hom}_{\mathbb{Z}[G]}(P_i, A) \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}[G]}(P_j, B) \xrightarrow{\cup} \operatorname{Hom}_{\mathbb{Z}[G]}(P_{i+j}, A \otimes_{\mathbb{Z}} B)$$

$$\phi \cup \phi' = \Big(\psi_{ij}(\phi \otimes \phi')\Big) \circ \kappa_{ij}$$

More explicitly,

$$\phi \cup \phi'(g_0, \dots, g_{i+j}) = \phi(g_0, \dots, g_i) \otimes \phi'(g_i, \dots, g_{i+j})$$

Note that this isn't the "real" or "final" version of the cup product. This is just the version we use to induce a map on cohomology.

Definition 3.11.2. Here is an alternate definition of the **preliminary cup product** map, using cochains. Let A, B be G-modules, and define

$$C^i(G, A) \otimes_{\mathbb{Z}} C^j(G, B) \xrightarrow{\cup} C^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

for $f \in C^i(G, A), f' \in C^j(G, B)$ by

$$(f \cup f')(g_1, g_2, \dots, g_{i+j}) = f(g_1, \dots, g_i) \otimes g_1 g_2 \cdots g_i f'(g_{i+1}, \dots, g_{i+j})$$

Note that by some uninspiring equations, one verifies that these two definitions "agree" in the sense that they correspond under the natural isomorphism of functors $\operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}, -) \cong C^i(G, -)$.

Now, using our explicit version in terms of projectives/cochains, we get the real version of the cup product on cohomology groups.

Definition 3.11.3. Let A, B be G-modules, and let $\cup$ be the preliminary cup product defined on cochains. The **cup product** is the induced map

$$H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) \xrightarrow{\cup} H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

defined in terms of the preliminary cup product map by

$$\overline{f} \cup \overline{f'} := \overline{f \cup f'}$$

On the RHS, the cup is the preliminary cup product map, and bars denote equivalence class in the quotient $H^i(G, A) = Z^i(G, A)/B^i(G, A)$. This is well defined because the preliminary cup product of two cocycles is a cocycle, and the preliminary cup product of a cocycle with a coboundary is a coboundary.

Often there is some obvious map $\theta : A \otimes_{\mathbb{Z}} B \to C$ for some other G-module C, and we consider the composition

$$H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) \xrightarrow{\cup} H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \xrightarrow{\theta^*} H^{i+j}(G, C)$$

which is $\alpha \otimes \beta \mapsto \theta(\alpha \cup \beta)$. For some weird reason, often the θ^* is omitted when it is understood to be there, and one just writes $\cup$ for the composition, so people will write things like

$$H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) \xrightarrow{\cup} H^{i+j}(G, C)$$

For example, if $B = \mathbb{Z}$, then $A \otimes_{\mathbb{Z}} \mathbb{Z} \cong A$ so there is an obvious map $\theta : A \otimes_{\mathbb{Z}} \mathbb{Z} \to A$ which is an isomorphism, and the induced θ^* is also an isomorphism, so we could just write

$$H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, \mathbb{Z}) \xrightarrow{\cup} H^{i+j}(G, \mathbb{Z})$$

Remark 3.11.4. Let G be a finite group, and A, B be G-modules. Similarly to the above, one may define a cup product on Tate cohomology.

$$\widehat{H}^i(G, A) \otimes_{\mathbb{Z}} \widehat{H}^j(G, B) \xrightarrow{\cup} \widehat{H}^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

We omit the details for this. The best way to go about it would probably be to use dimension shifting isomorphisms and the long exact sequence to induce cup products on negative degree Tate cohomology groups.

3.11.2 Cohomology as a graded ring (sometimes)

Let G be a group and A a G-module. Then there are cup product maps

$$\cup : H^i(G, A) \times H^j(G, A) \to H^{i+j}(G, A \otimes_{\mathbb{Z}} A)$$

Assume we have a morphism of G-modules

$$A \otimes_{\mathbb{Z}} A \to A$$

For example, this happens if A is cyclic group [3]. Then this induces a map on cohomology

$$H^i(G, A \otimes_{\mathbb{Z}} A) \to H^i(G, A)$$

We are just going to be sloppy and denote the composition of these by $\cup$.

$$H^i(G, A) \times H^j(G, A) \xrightarrow{\cup} H^{i+j}(G, A)$$

Thus we have a graded (anticommutative) ring structure on

$$\bigoplus_{i=0}^{\infty} H^i(G, A)$$

In principle, the structure of this ring could differentiate between G-modules which have the same cohomology groups. Even if $H^i(G, A) \cong H^i(G, B)$ for all i, the cup products could be different, so we would conclude $A \ncong B$ as G-modules.

Warning! This ring structure only exists when there is a map $A \otimes A \to A$. It is tempting to think there is a natural choice of map here, but this is not true. For example, the obvious choice $a \otimes b \mapsto a + b$ is not well defined, because $A \times A \to A, (a, b) \mapsto a + b$ is not a $\mathbb{Z}$-balanced map.

3.11.3 Properties of cup product

As we mentioned before, group cohomology cup products are notoriously difficult to compute even for rather basic concrete examples. Because of this, the best hope for an intuition about cup products is just heavily absorbing the long list of properties characterizing the cup product.

We skip a lot of the proofs for these, because they aren't that important to know and understand for later, and don't really illustrate techniques that get reused later. Sharifi [15] is a good source for proofs of most of these.

Proposition 3.11.5 (Cup product in degree zero)**.** *In the case $i = j = 1$, the cup product is just the inclusion*

$$A^G \otimes_{\mathbb{Z}} B^G \hookrightarrow (A \otimes_{\mathbb{Z}} B)^G$$

Proof. There's nothing complicated to prove here, just some thinking to do. In terms of cochains, an element $f \in C^0(G, A)$ is a function $G^0 \to A$. By convention, G^0 is the trivial group, so $f \in C^0(G, A)$ is essentially a point in A. Lying in the kernel of $d^0 : C^0(G, A) \to C^1(G, A)$ means that

$$(d^0 f)(g) = gf - f = 0 \qquad \forall g \in G$$

[3] If A is cyclic, then $A \otimes A \cong A$, which, given a choice of generator for A, gives a morphism $A \otimes A \to A$.

which is to say, $gf = f$, which is to say, $f \in A^G$. Of course, we already knew this. But now thinking about the definition of cup product in terms of cochains, for $f, f' \in C^0(G, A)$,

$$(f \cup f') = f \otimes f' \in A^G \otimes B^G \subset (A \otimes B)^G$$

□

Proposition 3.11.6 (Naturality of cup product)**.** *The cup product is "natural" in A and B. More precisely, if $\phi : A \to A'$ is a morphism of G-modules and $\phi_* : H^i(G, A) \to H^i(G, A')$ is the induced map on homology, then $\phi \otimes 1 : A \otimes B \to A' \otimes B$ is a morphism of G-modules, and $(\phi \otimes 1)_* : H^i(G, A \otimes B) \to H^i(G, A' \otimes B)$ is the induced map on homology, then for $\alpha \in H^i(G, A)$ and $\beta \in H^j(G, B)$,*

$$\phi_*(\alpha) \cup \beta = (\phi \otimes 1)_*(\alpha \cup \beta)$$

Equivalently, the following diagram commutes.

$$\begin{array}{ccc} H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow{\scriptstyle \phi_* \otimes \mathrm{Id}} & & \downarrow{\scriptstyle (\phi \otimes \mathrm{Id})_*} \\ H^i(G, A') \otimes_{\mathbb{Z}} H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A' \otimes_{\mathbb{Z}} B) \end{array}$$

The analogous property holds for a morphism $\psi : B \to B'$.

Proof. Theorem 1.9.5 of Sharifi [**?**]. □

Proposition 3.11.7 (Cup product "commutes" with connecting homomorphisms)**.** *If*

$$0 \to A_1 \to A_2 \to A_3 \to 0$$

is a short exact sequence of G modules, and B is a G-module such that the sequence

$$0 \to A_1 \otimes B \to A_2 \otimes B \to A_3 \otimes B \to 0$$

is also exact, then for $\alpha \in H^i(G, A_3)$ and $\beta \in H^j(G, B)$,

$$\delta(\alpha \cup \beta) = (\delta\alpha) \cup \beta \in H^{i+j+1}(G, A_1 \otimes B)$$

where the δ maps are connecting homomorphism coming from the long exact sequences. We can write this as a commutative diagram

$$\begin{array}{ccc} H^i(G, A_3) \otimes H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A_3 \otimes B) \\ \downarrow{\scriptstyle \delta \otimes 1} & & \downarrow{\scriptstyle \delta} \\ H^{i+1}(G, A_1) \otimes H^j(G, B) & \xrightarrow{\cup} & H^{i+j+1}(G, A_1 \otimes B) \end{array}$$

Proof. This is basically proved by reproving the snake lemma. You work through the whole process of lifing, etc. that the snake lemma uses to construct the connecting homomorphisms. Nothing too fancy, though not super easy to follow. See Theorem 1.9.5 of Sharifi [**?**]. □

Remark 3.11.8. There is an analogous property with tensoring applied on the other side of the exact sequence, though there is a slight issue of a sign, so the resulting equation becomes

$$\delta(\alpha \cup \beta) = (-1)^i \alpha \cup (\delta\beta)$$

where $\alpha \in H^i(G, A), \beta \in H^j(G, B_3)$.

Remark 3.11.9. While the hypotheses of Proposition 3.11.7 seem strange and unlikely to occur in useful situations, there are several situations where this does happen. First, if B is a flat (such as free or projective) G-module, then by definition the sequence after tensoring with B remains exact.

Alternately, if the original sequence $0 \to A_1 \to A_2 \to A_3 \to 0$ is split exact, then since $- \otimes B$ is an additive functor, the sequence after tensoring with B remains split exact. This happens in the case of the dimension-shifting sequences

$$0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0 \qquad 0 \to A_* \to \mathrm{Ind}^G(A) \to A \to 0$$

In particular, the previous proposition applied to these split exact sequences is the main ingredient for why cup products are uniquely determined by these properties, by using a clever dimension shifting induction.

Proposition 3.11.10 (Uniqueness of cup product)**.** *The cup products we have defined are the unique family of maps satisfying the properties above (naturality, description in degree zero, and interaction with connecting homomorphisms).*

Proof. Suppose we have a product with these properties. We show by dimension shifting that the cup products in degree (i, j) determine cup products in degrees $(i + 1, j)$ and $(i, j + 1)$. Consider the short exact sequence

$$0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$$

and recall from earlier that it remains exact after tensoring with any B.

$$0 \to A \otimes B \to \mathrm{CoInd}^G(A) \otimes B \to A^* \otimes B \to 0$$

So by Proposition 3.11.7, we get

$$\begin{array}{ccc} H^i(G, A^*) \otimes H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A^* \otimes B) \\ \downarrow{\scriptstyle \delta \otimes 1} & & \cong \downarrow{\scriptstyle \delta} \\ H^{i+1}(G, A) \otimes H^j(G, B) & \xrightarrow{\cup} & H^{i+j+1}(G, A \otimes B) \end{array}$$

Recall that the connecting homomorphisms in the LES associated to $0 \to A \to \mathrm{CoInd}^G(A) \to A^* \to 0$ are isomorphisms for $i \geq 1$ and surjective for $i = 0$. Thus the cup product on the bottom is determined by the cup product on the top.

A similar argument using the other cup product property interacting with connecting homomorphisms shows that the cup products in degree (i, j) determine those in degree $(i, j + 1)$. □

Proposition 3.11.11 (Antisymmetry of cup product)**.** *Let $\tau : A \otimes B \to B \otimes A$ be the canonical isomorphism ("twist map") $a \otimes b \mapsto b \otimes a$, and let $\tau_* : H^k(G, A \otimes B) \to H^k(G, B \otimes A)$ be the induced isomorphism on cohomology. For $\alpha \in H^i(G, A)$ and $\beta \in H^j(G, B)$,*

$$\tau_*(\alpha \cup \beta) = (-1)^{ij} \beta \cup \alpha$$

Since τ, τ_* are such natural/canonical isomorphisms, this is usually just written as

$$\alpha \cup \beta = (-1)^{ij} \beta \cup \alpha$$

Proof. Prove first in case $i = j = 0$, then use some dimension shifting to induct. See Corollary 1.9.7 of Sharifi [15]. □

Proposition 3.11.12 (Associativity of cup product)**.** *The cup product is associative. More precisely, let C be another G-module, and let $\alpha \in H^i(G, A), \beta \in H^j(G, B), \gamma \in H^k(G, C)$. Then*

$$(\alpha \cup \beta) \cup \gamma = \alpha \cup (\beta \cup \gamma) \in H^{i+j+k}(G, A \otimes B \otimes C)$$

Really, these things don't quite live in the same homology group, but canonical isomorphisms $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ induced canonical isomorphisms between the homology groups that they live in.

Proof. This can be checked directly on the level of cochains, which is tedious. See Proposition 1.9.7 of Sharifi [15]. □

As our final list of properties of cup products, we describe how cup product interacts with Res, Cor, and Inf. For Res and Inf, the relationship is about as simple and convenient as it could be, though spelling it out in detail requires some careful tracking of where various cup products are coming and going. The interaction with Cor is a bit weirder, but hey, what can you do. Math is strange sometimes.

Proposition 3.11.13 (Cup product and Res, Inf, Cor)**.** *Under suitable hypotheses and sufficient abuse of notation,*

$$\begin{aligned} \mathrm{Res}(\alpha \cup \beta) &= \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta) \\ \mathrm{Inf}(\alpha \cup \beta) &= \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta) \\ \mathrm{Cor}(\alpha) \cup \beta &= \mathrm{Cor}(\alpha \cup \mathrm{Res}(\beta)) \end{aligned}$$

We now spell out the suitable hypotheses and various abuses of notation in gory detail, which may be skipped. Let A, B be G-modules.

1. *Let $H \subset G$ be a subgroup. Consider the restriction maps*

$$\begin{aligned} \mathrm{Res}_A &: H^i(G, A) \to H^i(H, A) \\ \mathrm{Res}_B &: H^i(G, B) \to H^i(H, B) \\ \mathrm{Res}_{A \otimes B} &: H^i(G, A \otimes_{\mathbb{Z}} B) \to H^i(H, A \otimes_{\mathbb{Z}} B) \end{aligned}$$

For $\alpha \in H^i(G, A)$ and $\beta \in H^j(G, B)$,

$$\mathrm{Res}_{A\otimes B}(\alpha \cup \beta) = \mathrm{Res}_A(\alpha) \cup \mathrm{Res}_B(\beta) \in H^{i+j}(H, A \otimes_{\mathbb{Z}} B)$$

We have slightly abused notation by using $\cup$ to refer to two different maps. Usually, notation is further abused by using Res *to refer to all three restriction maps, and this is written as*

$$\mathrm{Res}(\alpha \cup \beta) = \mathrm{Res}(\alpha) \cup \mathrm{Res}(\beta)$$

This can also be expressed by the following commutative diagram.

$$\begin{array}{ccc} H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow \mathrm{Res} \quad \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ H^i(H, A) \otimes_{\mathbb{Z}} H^j(H, B) & \xrightarrow{\cup} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

This is a bit confusing. It is just saying that the following two squares commute.

$$\begin{array}{ccc} H^i(G, A) & \xrightarrow{-\cup\beta} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ H^i(H, A) & \xrightarrow{-\cup \mathrm{Res}(\beta)} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array} \qquad \begin{array}{ccc} H^i(G, B) & \xrightarrow{\alpha\cup-} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ H^i(H, B) & \xrightarrow{\mathrm{Res}(\alpha)\cup-} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

2. *Let $N \subset G$ be a normal subgroup. Consider the inflation maps*

$$\begin{aligned} &\mathrm{Inf}_A : H^i(G/N, A^N) \to H^i(G, A) \\ &\mathrm{Inf}_B : H^i(G/N, B^N) \to H^i(G, B) \\ &\mathrm{Inf}_{A\otimes B} : H^i(G/N, (A \otimes_{\mathbb{Z}} B)^N) \to H^i(G, A \otimes_{\mathbb{Z}} B) \end{aligned}$$

and the inclusion

$$\iota : A^N \otimes_{\mathbb{Z}} B^N \hookrightarrow (A \otimes_{\mathbb{Z}} B)^N$$

with induced map

$$\iota^* : H^i\left(G/N, A^N \otimes_{\mathbb{Z}} B^N\right) \to H^i\left(G/N, (A \otimes_{\mathbb{Z}} B)^N\right)$$

For $\alpha \in H^i(G/N, A^N)$ and $\beta \in H^j(G/N, B^N)$,

$$\mathrm{Inf}_{A\otimes B}(\iota^*(\alpha \cup \beta)) = \mathrm{Inf}_A(\alpha) \cup \mathrm{Inf}_B(\beta) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

We have slightly abused notation by using $\cup$ to refer to two different maps. Usually, notation is further abused by using Inf *to refer to all three inflation maps, and the ι^* map is "obvious," so this is written as*

$$\mathrm{Inf}(\alpha \cup \beta) = \mathrm{Inf}(\alpha) \cup \mathrm{Inf}(\beta)$$

This can also be expressed by the following commutative diagram.

$$\begin{array}{ccc} H^i(G/N, A^N) \otimes_{\mathbb{Z}} H^j(G/N, B^N) & \xrightarrow{\cup} & H^{i+j}(G/N, A^N \otimes_{\mathbb{Z}} B^N) \\ \downarrow{\scriptstyle \text{Inf}} \quad \downarrow{\scriptstyle \text{Inf}} & & \downarrow{\scriptstyle \text{Inf} \circ \iota^*} \\ H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

This is a bit confusing. It is just saying that the following two squares commute.

$$\begin{array}{ccc} H^i(G/N, A^N) & \xrightarrow{-\cup\beta} & H^{i+j}(G/N, A^N \otimes_{\mathbb{Z}} B^N) \\ \downarrow{\scriptstyle \text{Inf}} & & \downarrow{\scriptstyle \text{Inf} \circ \iota^*} \\ H^i(G, A) & \xrightarrow{-\cup \text{Inf}(\beta)} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array} \qquad \begin{array}{ccc} H^i(G/N, B^N) & \xrightarrow{\alpha\cup-} & H^{i+j}(G/N, A^N \otimes_{\mathbb{Z}} B^N) \\ \downarrow{\scriptstyle \text{Inf}} & & \downarrow{\scriptstyle \text{Inf} \circ \iota^*} \\ H^i(G, B) & \xrightarrow{\text{Inf}(\alpha)\cup-} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

3. *Let $H \subset G$ be a subgroup of finite index. Consider the corestriction and restriction maps*

$$\begin{aligned} &\text{Cor}_A : H^i(H, A) \to H^i(G, A) \\ &\text{Cor}_{A\otimes B} : H^i(H, A \otimes_{\mathbb{Z}} B) \to H^i(G, A \otimes_{\mathbb{Z}} B) \\ &\text{Res}_B : H^j(G, B) \to H^j(H, B) \end{aligned}$$

For $\alpha \in H^i(H, A)$ and $\beta \in H^j(G, B)$,

$$\text{Cor}_A(\alpha) \cup \beta = \text{Cor}_{A\otimes B}(\alpha \cup \text{Res}_B(\beta)) \in H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$$

We have slightly abused notation by using $\cup$ to refer to two different maps. Usually, notation is further abused by writing

$$\text{Cor}(\alpha) \cup \beta = \text{Cor}(\alpha \cup \text{Res}(\beta))$$

This can also be expressed by the following commutative diagram.

$$\begin{array}{ccc} H^i(G, A) \otimes_{\mathbb{Z}} H^j(G, B) & \xrightarrow{\cup} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ {\scriptstyle \text{Cor}}\uparrow \quad \downarrow{\scriptstyle \text{Res}} & & {\scriptstyle \text{Cor}}\uparrow \\ H^i(H, A) \otimes_{\mathbb{Z}} H^j(H, B) & \xrightarrow{\cup} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

The diagram above is a bit confusing. It is really just saying that the following two squares commute.

$$\begin{array}{ccc} H^i(G, A) & \xrightarrow{-\cup\beta} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ {\scriptstyle \text{Cor}}\uparrow & & {\scriptstyle \text{Cor}}\uparrow \\ H^i(H, A) & \xrightarrow{-\cup \text{Res}(\beta)} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array} \qquad \begin{array}{ccc} H^j(G, B) & \xrightarrow{\text{Cor}(\alpha)\cup-} & H^{i+j}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow{\scriptstyle \text{Res}} & & {\scriptstyle \text{Cor}}\uparrow \\ H^j(H, B) & \xrightarrow{\alpha\cup-} & H^{i+j}(H, A \otimes_{\mathbb{Z}} B) \end{array}$$

Proof. Sharifi 1.9.10 [15]. Can you imagine going through a detailed proof of this? Just thinking about it makes me want to crawl into bed. □

3.12 Profinite cohomology

Now that we have various tools of group cohomology under our belts, it is time to get some topology involved. This is not the connection to algebraic topology and homology/cohomology theories there. Instead, we will add additional structure to our group cohomology groups $H^i(G, A)$ by adding topological structure to the group G.

In particular, we will study the case where G is a profinite group, which comes with associated topological data. There will also be a little bit of topological structure on our module A, but not really, because we will only really care about the discrete topology on A. This topological structure translates to some restriction of the G-action on A, that is, will we require it to be "continuous," whatever that will mean. Basically, the action plays nicely with the topologies.

This additional structure is not so much motivated by the additional results we get by adding these constraints, but more motivated by the fact that profinite groups arise in the context that we want to know about. That context is Galois groups. We already know that infinite Galois groups are profinite groups (Proposition 2.3.1). In particular, we'll look at the absolute Galois group of a field K and various modules for it, and the associated cohomology groups.

The group cohomology groups in this context are invariants of the field K, and very important invariants at that. First, there are some cohomological reinterpretations of classical results, such as Hilbert's Theorem 90. But the really big part of it is the connection to the Brauer group of K. Much later, we will see that one of the H^2 groups is isomorphic to the Brauer group. This will be extremely useful for knowing things about the Brauer group, because we have so many great tools in group cohomology.

3.12.1 Definition of profinite cohomology

The first thing to do is reworking a little bit of our definition of cohomology groups to take into account the additional structure involved when G is a profinite group. This will be a mostly small change. After this, we will mostly just assert that all of our tools for regular group cohomology translate/have analogs in profinite cohomology.

Definition 3.12.1. Let G be a topological group [4]. A **topological G-module** A is a topological abelian group with G-action such that the G-action is a continuous map $G \times A \to A$. A **discrete topological G-module** is an abelian group A which is a topological G-module with respect to the discrete topology on A.

Proposition 3.12.2. *Let G be a topological group and A be a G-module. The following are equivalent.*

1. *Giving A the discrete topology makes A into a discrete topological G-module.*
2. *The stabilizer of each $a \in A$ is an open subgroup of G.*

[4] A topological group is a group with a topology such that the multiplication and inversion maps are continuous.

Proof. Sharifi 2.2.3 [15]. □

Definition 3.12.3. Let A be a topological G-module. For $i \in \mathbb{Z}$ the group of **continuous i-cochains** with coefficients in A is

$$C^i_{\text{cts}}(G, A) = \left\{ f : G^i \to A \mid f \text{ is continuous} \right\}$$

The same formula for the differential as in Definition 3.2.4 gives boundary maps making $C^\bullet_{\text{cts}}(G, A)$ into a chain complex. The **profinite cohomology** group $H^i_{\text{cts}}(G, A)$ is the ith homology of $C^\bullet_{\text{cts}}$.

Because writing the subscript cts is tedious, whenever G is a profinite group, we just write $H^i(G, A)$ instead of $H^i_{\text{cts}}(G, A)$. However, the careful reader should note that in general, these may be very different groups. If G is a discrete group (such as a finite group), then the two meanings for $H^i(G, A)$ agree, so this is not a terrible abuse of notation.

Remark 3.12.4. The notion of compatible pairs for profinite groups and topological modules are defined in analogy with the case where no topology is involved, with the requirement that all the maps involved be continuous. As before, compatible pairs now induce maps on profinite cohomology. In particular, there are inflation, restriction, etc. maps as before, as long as the subgroup involved is a closed subgroup.

Alternately, one can define inflation/restriction maps on profinite cohomology by taking the direct limit of inflation/restriction maps, with direct limit taken in the context of Proposition 3.12.6. Thankfully, these definitions are equivalent (proof omitted).

Remark 3.12.5. The following proposition may viewed as an alternate approach to defining profinite cohomology (such as the approach in Gille and Szamuely [4]). In our approach, we view the following as a theorem instead.

Proposition 3.12.6. *Let G be a profinite group, and let $\mathcal{U}$ be the set of open normal subgroups of G. Let A be a discrete G-module. Then*

$$H^i(G, A) \cong \varinjlim_{N \in \mathcal{U}} H^i(G/N, A^N)$$

where the maps of the directed system are inflation maps.

Proof. Proposition 2.2.16 of Sharifi [15]. □

Remark 3.12.7. In particular, in the case where L/K is a Galois extension and $G = \text{Gal}(L/K)$, by the Galois correspondence, the set of open normal subgroups of G is the set of subgroups $\text{Gal}(L/E)$ where E/K is finite Galois. For the modules $(L, +)$ and $(L^\times, \times)$, the above isomorphism is

$$H^i(\text{Gal}(L/K), L^\times) \cong \varinjlim_{E \in \mathcal{E}} H^i\left(\frac{\text{Gal}(L/K)}{\text{Gal}(L/E)}, (L^\times)^{\text{Gal}(L/E)}\right) \cong \varinjlim_{E \in \mathcal{E}} H^i(\text{Gal}(E/K), E^\times)$$

$$H^i(\text{Gal}(L/K), L) \cong \varinjlim_{E \in \mathcal{E}} H^i\left(\frac{\text{Gal}(L/K)}{\text{Gal}(L/E)}, L^{\text{Gal}(L/E)}\right) \cong \varinjlim_{E \in \mathcal{E}} H^i(\text{Gal}(E/K), E)$$

where $\mathcal{E}$ is the set of finite Galois intermediate extensions $K \subset E \subset L$.

One place this is very useful is if we want to show that $H^1(Gal(L/K), L^\times)$ is zero (which we will do later in Theorem 3.12.12). Because it is determined by the cohomology groups for E/K finite Galois, it suffices to show that all of the cohomology groups for $H^1(\mathrm{Gal}(E/K), E)$ are zero, since the direct limit of trivial groups is the trivial group. And it is easier to work with the finite group $\mathrm{Gal}(E/K)$ rather than to work with $\mathrm{Gal}(L/K)$ if $[L : K]$ is infinite.

As we mentioned before, most of our tools from regular group cohomology translate perfectly into profinite cohomology. One such tool is the long exact sequence.

Proposition 3.12.8 (Long exact sequence on profinite cohomology)**.** *Let G be a profinite group. A short exact sequence $0 \to A \to B \to C \to 0$ of discrete topological G-modules induces a long exact sequences on profinite cohomology.*

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to \cdots$$

Remark 3.12.9. The analog of the inflation restriction exact sequence (3.9.20) holds in the case of profinite cohomology.

3.12.2 $H^1(G, M)$ for G profinite, M discrete, torsion free, finitely generated

On a first pass reading, this section can be skipped without any issues. It's just an application of the inflation restriction sequence for profinite cohomology to get a finiteness result.

Remark 3.12.10. Let G be a profinite group. Recall Proposition 2.2.2, which tells us that that a subgroup is open if and only if it is closed and of finite idex.

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\}$$

Additionally, a closed subset of a compact set is compact, and since G is Hausdorff, a compact set is closed. Thus

$$\{\text{closed subgroups}\} = \{\text{compact subgroups}\}$$

$$\{\text{open subgroups}\} = \{\text{closed subgroups of finite index}\} = \{\text{compact subgroups of finite index}\}$$

Proposition 3.12.11. *Let G be a profinite group and M a discrete G-module which is torsion free and finitely generated as an abelian group. Then $H^1(G, M)$ is finite.*

Proof. Let $m_1, \ldots, m_n$ be a set of generators for M. Set $G_i = \mathrm{stab}(m_i)$. Since M is a discrete module, G_i is open in G. Then set

$$G_M = \bigcap_{i=1}^{n} G_i$$

and note that G_M is also open, since it is a finite intersection of open sets. G_M acts trivially on generators of M, so it acts trivially on all of M. Consider the conjugation action of G on its set of subgroups.

$$G \times \{\text{subgroups } H \subset G\} \to \{\text{subgroups } H \subset G\} \qquad g \cdot H = gHg^{-1}$$

For the subgroup G_M, the stabilizer of this action is the normalizer $\text{stab}(G_M) = N_G(G_M)$, and the orbit is the set of conjugate subgroups. Because G_M is open, it has finite index, and because $G_M \subset N_G(G_M)$, the normalizer also has finite index. By the orbit-stabilizer theorem, the size of the orbit is equal to the index of the stabilizer, so the size of the orbit is finite, which is to say, G_M has finitely many conjugate subgroups. Thus we have a finite intersection

$$N = \bigcap_{g \in G} g G_M g^{-1}$$

so N is a finite index open subgroup. It is clear that N is normal, and that N acts trivially on M, so $M^N = M$. Since N acts trivially on M, the decomposition $M \cong \oplus\mathbb{Z}$ is a decomposition of N-modules, so

$$H^1(N, M) = H^1(N, \oplus\mathbb{Z}) \cong \bigoplus H^1(N, \mathbb{Z}) \cong \text{Hom}_{\text{cts}}(N, \mathbb{Z})$$

Since N is an open subgroup of a finite index in a profinite group, it is also compact, so the image of N under a continuous homomorphism $N \to \mathbb{Z}$ is a compact subgroup of $\mathbb{Z}$, which is to say, it is trivial. Thus $\text{Hom}(N, \mathbb{Z}) = 0$, so $H^1(N, M) = 0$. Now consider the first three nonzero terms of the Inflation-Restriction sequence.

$$0 \longrightarrow H^1(G/N, M^N) \longrightarrow H^1(G, M) \longrightarrow H^1(N, M) = 0$$

By exactness, $H^1(G, M) \cong H^1(G/N, M^N) = H^1(G/N, M)$. Recall that G/N is finite, so from the restriction-corestriction sequence, we know that $H^1(G/N, M)$ is torsion of exponent dividing $|G/N|$. Since M is finitely generated, $H^1(G/N, M)$ is finitely generated. Thus $H^1(G/N, M)$ is a torsion and finitely generated abelian group, so it is finite. Thus $H^1(G, M)$ is also finite. □

3.12.3 Hilbert 90

Now we return to the situation which we really care about, which is profinite cohomology for infinite Galois groups. As mentioned previously, it is very useful to know that the profinite cohomology is the direct limit of regular cohomology groups with finite groups.

We start with a generalization of Hilbert Theorem 90, from which we derive the classical Hilbert Theorem 90. Then we also have an "additive" verison of Hilbert 90, which not necessarily useful, but tells us that there is "nothing to see" in terms of cohomology for the absolute Galois group acting on the additive group of a field, because all of the cohomology groups vanish.

In contrast, the multiplicative Hilbert 90 (our original generalization) says that the first cohomology group (of the absolute Galois group acting on the multiplicative group of a field) vanishes, but higher groups need not vanish. So it is somewhat natural to expect that these higher cohomology groups are interesting invariants of the field, and this is indeed the case. In particular, just the next cohomology group turns out to be isomorphic to the Brauer group.

Theorem 3.12.12 (Profinite multiplicative Hilbert 90)**.** *Let L/K be a Galois extension. Then $H^1(\text{Gal}(L/K), L^\times) = 0$.*

Proof. By Lemma 2.3.1, $G = \mathrm{Gal}(L/K)$ is the inverse limit of Galois groups of finite extensions, so if we prove the result for finite extensions, we get the result on infinite extensions for free. So we may assume L/K is finite (so G is finite).

For clarity, we write $\cdot$ for multiplication in $L^\times$. Let $f : G \to L^\times$ be a cocycle, that is, for $\tau, \sigma \in G$, [5]

$$f(\tau\sigma) = \tau\Big(f(\sigma)\Big) \cdot f(\tau)$$

The elements $\sigma \in G$ are distinct characters $L^\times \to L$, so they are linearly independent by linear independence of characters (Theorem 7 of Section 14.2 of Dummit and Foote [3]). Thus

$$\sum_{\sigma \in G} f(\sigma)\sigma$$

is a nonzero map (since $f(\sigma) \neq 0$). Let $\alpha \in L^\times$ so that

$$\beta = \sum_{\sigma \in G} f(\sigma) \cdot \sigma(\alpha) \neq 0$$

Then for $\tau \in G$,

$$\begin{aligned}
\tau^{-1}(\beta) &= \tau^{-1} \sum_{\sigma \in G} f(\sigma) \cdot \sigma(\alpha) \\
&= \sum_{\sigma \in G} \tau^{-1}\Big(f(\sigma) \cdot \sigma(\alpha)\Big) && \text{linearity} \\
&= \sum_{\sigma \in G} \Big(\tau^{-1} f(\sigma)\Big) \cdot \Big(\tau^{-1}\sigma(\alpha)\Big) && \tau \text{ is a field hom} \\
&= \sum_{g \in G} \Big(\tau^{-1} f(\tau g)\Big) \cdot g(\alpha) && \text{substitute } g = \tau^{-1}\sigma \\
&= \sum_{\sigma \in G} \Big(\tau^{-1} f(\sigma)\Big) \cdot \sigma(\alpha) && \text{substitute } g = \sigma \\
&= \sum_{\sigma \in G} \tau^{-1}\Big(f(\tau) \cdot \tau\big(f(\sigma)\big)\Big) \cdot \sigma(\alpha) && f \text{ is a cocycle} \\
&= \sum_{\sigma \in G} \tau^{-1}(f(\tau)) \cdot f(\sigma) \cdot \sigma(\alpha) && \tau \text{ is a field hom} \\
&= \tau^{-1}\Big(f(\tau)\Big) \cdot \sum_{\sigma \in G} f(\sigma) \cdot \sigma(\alpha) && \text{linearity} \\
&= \tau^{-1}\Big(f(\tau)\Big) \cdot \beta
\end{aligned}$$

Applying τ to both sides,

$$\beta = f(\tau) \cdot \tau(\beta) \qquad f(\tau) = \frac{\beta}{\tau(\beta)} = \frac{\tau(\beta^{-1})}{\beta^{-1}}$$

[5] This may be confusing, since usually the cocycle condition would be written $f(\tau\sigma) = \tau f(\sigma) + f(\tau)$ but this is when the G-module is written additively, and here we are writing our G-module $L^\times$ multiplicatively.

Thus f is a coboundary. [6] $\square$

The vanishing of this cohomology group leads back to the classical version of Hilbert Theorem 90 by using our knowledge of Tate cohomology for finite cyclic groups.

Theorem 3.12.13 (Classical multiplicative Hilbert 90)**.** *Let L/K be a finite cyclic Galois extension, let $\mathrm{N}_K^L : L^\times \to K^\times$ be the norm map, and let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Then*

$$\ker \mathrm{N}_K^L = \left\{ \frac{\sigma\beta}{\beta} \;\middle|\; \beta \in L^\times \right\}$$

Proof. Let $G = \mathrm{Gal}(L/K)$ and $n = [L : K] = |G|$. Since σ generates G, the element $\sigma - 1 \in \mathbb{Z}[G]$ generates I_G, hence right hand side is exactly $I_G L^\times$. Thus the claim is equivalent to either of the following.

$$\ker \mathrm{N}_K^L = I_G L^\times \qquad \ker \mathrm{N}_K^L / I_G L^\times = 0$$

Note that the field norm map N_K^L coincides with the group norm map N_G, as shown below.

$$N_G(\beta) = \left(\sum_{i=0}^{n-1} \sigma^i \right) \beta = \prod_{i=0}^{n-1} (\sigma^i \beta) = \mathrm{N}_K^L(\beta)$$

(Since we write $L^\times$ multiplicatively, the sum becomes a product). By definition of Tate cohomology,

$$\widehat{H}^{-1}(G, L^\times) = \ker N_G / I_G L^\times = \ker \mathrm{N}_K^L / I_G L^\times$$

Thus the claim reduces to showing $\widehat{H}^{-1}(G, L^\times) = 0$. Since G is cyclic,

$$\widehat{H}^{-1}(G, L^\times) \cong \widehat{H}^1(G, L^\times) = H^1(G, L^\times) = 0$$

with the final equality from Theorem 3.12.12. $\square$

Before we can prove the additive version of Hilbert Theorem 90, we need to cite a result without proof.

Theorem 3.12.14 (Normal basis theorem)**.** *Let L/K be a finite Galois extension. Then there exists $\alpha \in L$ such that*

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$$

is a K-basis of L.

Proof. (Not a proof.) Usually the proof is broken into cases where K is finite/infinite. The finite case is not hard, since in that case G is cyclic. (Sorry, I couldn't find a good reference for this. Probably in Lang somewhere, but I don't have my copy handy at the moment.) $\square$

[6] Again, this looks a bit strange since things are written multiplicatively instead of additively, but it is right. The usual coboundary condition for f to be a degree one coboundary is that there exists x in the module such that $f(\tau) = \tau(x) - x$, but in multiplicative notation it becomes $f(\tau) = \frac{\tau x}{x}$.

Remark 3.12.15. Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Then L is a $K[G]$-module via

$$K[G] \times L \to L \qquad \left(\sum_{\sigma \in G} \lambda_\sigma \sigma\right) \cdot x = \sum_{\sigma \in G} \lambda_\sigma \sigma(x)$$

where $\lambda_\sigma \in K$. Another way to interpret the normal basis theorem is that $L \cong K[G]$ as a $K[G]$-module. Let α be the element of the normal basis theorem. Then

$$L \to K[G] \qquad \sum_{\sigma \in G} \lambda_\sigma \sigma(\alpha) \mapsto \sum_{\sigma \in G} \lambda_\sigma \sigma$$

is an isomorphism of $K[G]$-modules.

Theorem 3.12.16 (Generalized additive Hilbert 90)**.** *Let L/K be a Galois extension. Then*

$$H^i(\mathrm{Gal}(L/K), L) = 0$$

for all $i \geq 1$.

Proof. As in the previous proof, Remark 3.12.7, which says

$$H^i(\mathrm{Gal}(L/K), L) \cong \varinjlim H^i(\mathrm{Gal}(E/K), E)$$

allows us to reduce to the case of a finite Galois extension. So assume L/K is finite, and let $G = \mathrm{Gal}(L/K)$. By the normal basis theorem, $L \cong K[G]$ as a $K[G]$-module, and this is also an isomorphism of G-modules. Thus

$$L \cong K[G] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} K \cong \mathrm{Ind}^G(K) \qquad (\cong \text{ of G-modules})$$

Thus $H^i(G, L) = 0$ for $i \geq 1$ since cohomology always vanishes for induced/coinduced modules. □

3.12.4 Kummer theory

One way to think about the starting point for Kummer theory is the following: hey, I noticed that Hilbert 90 says that $H^1(\mathrm{Gal}(L/K), L^\times) = 0$, maybe I can fit this into a long exact sequence somewhere and make some conclusions from the fact that some of the terms are zero.

This is often a great way to obtain results in homological algebra, and this case is no exception. We can in fact fit $H^1(\mathrm{Gal}(L/K), L^\times)$ into some long exact sequences, and get some quite interesting results out of doing so.

Definition 3.12.17. Let n be a positive integer and let K be a field of characteristic not dividing n, and let $\mu_n \subset K^{\mathrm{sep}}$ be the group of nth roots of unity. The **Kummer sequence** is the short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \longrightarrow 1$$

This is a short exact sequence of discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules.

Remark 3.12.18. The requirement that $\operatorname{char} K$ not divide n is just so that the polynomial $x^n - 1 \in K[x]$ is separable. The formal derivative is $nx^{n-1} = 0$ if n divides the characteristic, so in this case $x^n - 1$ is not separable. The requirement is satsified in any field of characteristic zero, such as a number field, as an important example.

For the next result, we are going to jump ahead and use Proposition 4.5.9, which says that

$$\operatorname{Br}(K) \cong H^2(\operatorname{Gal}(K^{\text{sep}}/K), (K^{\text{sep}})^\times)$$

For the moment, it is totally reasonable to just think of this as the definition of $\operatorname{Br}(K)$. Eventually we will have another definition which is not in terms of group cohomology at all, but that takes a lot of build up to define, which we will get to later.

Theorem 3.12.19 (Kummer isomorphisms)**.** *Let K be a field of characteristic not dividing n and let $G_K = \operatorname{Gal}(K^{\text{sep}}/K)$ be the absolute Galois group. Then*

$$H^1(G_K, \mu_n) \cong K^\times / K^{\times n} \qquad H^2(G_K, \mu_n) \cong {}_n \operatorname{Br}(K)$$

where the ${}_n$ denotes n-torsion.

Proof. This basically follows from considering the long exact sequence on profinite cohomology $H^n(G_K, -)$ associated to the Kummer sequence, along with using the multiplicative version of Hilbert 90 (Proposition 3.12.12). The long exact sequence looks like

$$\begin{aligned}
0 &\longrightarrow H^0(G_K, \mu_n) \longrightarrow H^0(G_K, (K^{\text{sep}})^\times) \xrightarrow{n} H^0(G_K, (K^{\text{sep}})^\times) \\
&\longrightarrow H^1(G_K, \mu_n) \longrightarrow H^1(G_K, (K^{\text{sep}})^\times) \xrightarrow{n} H^1(G_K, (K^{\text{sep}})^\times) \\
&\longrightarrow H^2(G_K, \mu_n) \longrightarrow H^2(G_K, (K^{\text{sep}})^\times) \xrightarrow{n} H^2(G_K, (K^{\text{sep}})^\times) \longrightarrow \cdots
\end{aligned}$$

By basic Galois theory, $H^1(G_K, (K^{\text{sep}})^\times) = K^\times$, and by Hilbert 90, $H^1(G_K, (K^{\text{sep}})^\times) = 0$. From the remark above, $H^2(G_K, (K^{\text{sep}})^\times) = \operatorname{Br}(K)$, so we get two exact sequences

$$\begin{aligned}
K^\times &\xrightarrow{n} K^\times \longrightarrow H^1(G_K, \mu_n) \longrightarrow 0 \\
0 &\longrightarrow H^2(G_K, \mu_n) \longrightarrow \operatorname{Br}(K) \xrightarrow{n} \operatorname{Br}(K)
\end{aligned}$$

By the 1st isomorphism theorem applied to the first sequence, $H^1(G_K, \mu_n) \cong K^\times / K^{\times n}$, and by exactness of the second sequence, $H^2(G_K, \mu_n) \cong {}_n \operatorname{Br}(K)$. □

The next result is an application of the inflation-restriction sequence 3.9.20 and some Kummer theory. It's not nearly as important to read at this stage, so it can be safely skipped over on a first pass.

Proposition 3.12.20 (Exercise 4.3 of Gille & Szamuely [4])**.** *Let $m \in \mathbb{Z}_{\geq 2}$ and let K be a field containing a primitive m^2th root of unity. Let $a \in K$ such that a has no mth root in K, and let α be a root of $x^m - a = 0$ in K^{sep}, and let $L = K(\alpha)$, so that $\operatorname{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z}$. Then*

1. *$(L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}$ is generated by (the image of) $K^\times$ and α.*

2. *The cokernel of $K^\times/K^{\times m} \to (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}$ is (isomorphic to) $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Let $\mu_m \subset K$ be the group of mth roots of unity. Consider the tower $K \subset L \subset K^{\mathrm{sep}} = L^{\mathrm{sep}}$, and consider the first four terms of the inflation-restriction sequence 3.9.20.

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), \mu_m) \xrightarrow{\mathrm{Inf}} H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mu_m)$$
$$\xrightarrow{\mathrm{Res}} H^1(\mathrm{Gal}(K^{\mathrm{sep}}/L), \mu_m)^{\mathrm{Gal}(L/K)} \longrightarrow H^2(\mathrm{Gal}(L/K), \mu_m)$$

Since $\mu_m \subset K$, the action of $\mathrm{Gal}(L/K)$ on it is trivial, so

$$H^1(\mathrm{Gal}(L/K), \mu_m) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m) \cong \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

By the computation of Tate cohomology for finite cyclic groups 3.7.8,

$$H^2(\mathrm{Gal}(L/K), \mu_m) \cong \widehat{H}^0(\mathrm{Gal}(L/K), \mu_m) \cong \mu_m^{\mathrm{Gal}(L/K)}/N_G\mu_m \cong \mu_m/m\mu_m \cong \mathbb{Z}/m\mathbb{Z}$$

By Kummer theory,

$$H^1(\mathrm{Gal}(K^{\mathrm{sep}}/K, \mu_m) \cong K^\times/K^{\times m} \qquad H^1(\mathrm{Gal}(K^{\mathrm{sep}}/L), \mu_m) \cong L^\times/L^{\times m}$$

So the inflation restriction sequence may be rewritten as

$$0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{j} K^\times/K^{\times m} \xrightarrow{i} (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)} \xrightarrow{f} \mathbb{Z}/m\mathbb{Z}$$

with i induced by the inclusion $K^\times \hookrightarrow L^\times$. Let $\zeta \in K$ be a primitive m^2th root of unity, and $\omega = \zeta^m$ be a primitive mth root of unity. Recall from the hypothesis that we have α which is an mth root of some $a \in K^\times$. We claim that $\alpha \in (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}$. The Galois conjugates of α are $\omega\alpha, \ldots, \omega^{m-1}\alpha$ but $\omega = \zeta^m$ so α differs from its Galois conjugates by an element of $L^{\times m}$. Thus the class of α in $L^\times/L^{\times m}$ is fixed by $\mathrm{Gal}(L/K)$.

Now consider the subgroup $A = \langle a \rangle$ generated by the class of a in $K^\times/K^{\times m}$. Since $x^m - a$ is irreducible, this subgroup has order m. Since $a = \alpha^m \in L^{\times m}$, $A \subset \ker i = \mathrm{im}\, j$. Thus $\ker i \cong \mathbb{Z}/m\mathbb{Z}$. Then by the 1st isomorphism theorem,

$$\mathrm{coker}\, i = (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}/\mathrm{im}\, i = (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}/\ker f \cong \mathrm{im}\, f \subset \mathbb{Z}/m\mathbb{Z}$$

Now consider the subgroup $B = \langle \alpha \rangle$ generated by the class of α in $(L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}$. Since no lower power than m is an mth power in $L^\times$, $B \cong \mathbb{Z}/m\mathbb{Z}$. Since $\ker f = \mathrm{im}\, i$ and $\alpha, \alpha^2, \ldots, \alpha^{m-1} \notin \mathrm{im}\, i$, they are not in the kernel of f, so $f(\alpha)$ generates a cyclic subgroup of $\mathbb{Z}/m\mathbb{Z}$ of order m, hence f is surjective, and $\mathrm{coker}\, i \cong \mathbb{Z}/m\mathbb{Z}$. This proves (2) in the original statement. Now we have an exact sequence

$$0 \to \mathrm{im}\, i \to (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)} \to (L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}/B \to 0$$

Thus $(L^\times/L^{\times m})^{\mathrm{Gal}(L/K)}$ is generated by $i(K^\times)$ and α, which proves (1). □

3.13 Computations of group cohomology

In this section we collect some group cohomology computations which are not important for later, but useful as exercises and ways to practice using various tools in group cohomology.

First, we do a computation of the matrix group $\mathrm{GL}_n(K)$ acting via left multiplication on column vectors K^n, which turns out to be zero most of the time. Then we have a result which is not about computation cohomology, but rather about what a particular cohomology group implies about the original group.

3.13.1 $H^r(\mathrm{GL}_n(K), K^n) = 0$ for $r \geq 0, \mathrm{char}\, K \neq 2$

One somewhat common group is the group of invertible matrices $\mathrm{GL}_n(K)$ with entries from an arbitrary field K. This group acts on the space of column vectors K^n by left multiplication, so we have a situation where we can take group cohomology.

However, it turns out that the cohomology groups are all zero, at least when the field K does not have characteristic 2. There is not much our method can say about that case, unfortunately.

Definition 3.13.1. Let G be a group and M a G-module. Fix $x \in G$, and define

$$\begin{aligned} \alpha &: G \to G & g &\mapsto xgx^{-1} \\ \beta &: M \to M & m &\mapsto x^{-1}m \end{aligned}$$

Then α, β form a compatible pair, which is to say, the following diagram commutes for any $g \in G$.

$$\begin{array}{ccc} M & \xrightarrow{\beta} & M \\ {\scriptstyle \alpha(g)}\downarrow & & \downarrow{\scriptstyle g} \\ M & \xrightarrow{\beta} & m \end{array}$$

Consequently, the maps

$$C^r(G, M) \to C^r(G, M) \qquad f \mapsto \beta f \alpha^r$$

on cochains induce maps on homology

$$\psi_{\alpha,\beta,r} : H^r(G, M) \to H^r(G, M) \qquad [f] \mapsto [\beta f \alpha^r]$$

Proposition 3.13.2. *Let G, M, α, β be as above. The maps $\psi_{\alpha,\beta,r} : H^r(G, M) \to H^r(G, M)$ are the identity for all G-modules M and all $r \geq 0$.*

Proof. We prove this by induction on r using the technique of dimension shifting. For $r = 0$, a cocycle $f : G^0 \to M$ is identified with an element of M^G, and

$$\beta f \alpha^0 = x^{-1} f = f$$

hence the induced map on cochains is the identity, so the induced map on H^0 is also the identity. Let $r \geq 1$ and assume that the maps $\psi_{\alpha,\beta,r-1} : H^{r-1}(G, M) \to H^{r-1}(G, M)$ are the identity for all M. Consider the usual short exact sequence

$$0 \to M \to \mathrm{CoInd}^G(M) \to M_* \to 0$$

Since $r \geq 1$, $H^r(G, \mathrm{CoInd}^G(M)) = 0$, so using the long exact sequences of cohomology we have the following diagram with exact rows, where δ is the connecting homomorphism.

$$\begin{array}{ccccc} H^{r-1}(G, M_*) & \xrightarrow{\delta} & H^r(G, M) & \longrightarrow & 0 \\ {\scriptstyle \psi_{\alpha,\beta,r}=\mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \psi_{\alpha,\beta,r}} & & \\ H^{r-1}(G, M_*) & \xrightarrow{\delta} & H^r(G, M) & \longrightarrow & 0 \end{array}$$

By thinking about how the connecting homomorphism is constructed, we see that this diagram commutes (for more details, see Lemma 3.13.3). Thus since $\psi_{\alpha,\beta,r}$ is the identity on $H^{r-1}(G, M_*)$, by commutativity, it is the identity on $H^r(G, M)$. This completes the induction. □

Lemma 3.13.3. *The diagram from the previous proposition commutes.*

$$\begin{array}{ccc} H^{r-1}(G, M_*) & \xrightarrow{\delta} & H^r(G, M) \\ {\scriptstyle \psi_{\alpha,\beta,r}=\mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \psi_{\alpha,\beta,r}} \\ H^{r-1}(G, M_*) & \xrightarrow{\delta} & H^r(G, M) \end{array}$$

Proof. We call the map $\mathrm{CoInd}^G(M) \to M_*$ by χ. Recall the description of the connecting homomorphism from the snake lemma: if $[\phi] \in H^{r-1}(G, M_*)$ is represented by a cocycle $\phi : G^{r-1} \to M_*$, there is a lift $\widetilde{\phi} : G^{r-1} \to M_*$, which is to say, $\chi\widetilde{\phi} = \phi$. (The lift $\widetilde{\phi}$ is not unique, but we are free to choose any lift.)

$$\begin{array}{ccc} & & \mathrm{CoInd}^G(M) \\ & \overset{\widetilde{\phi}}{\nearrow} & \downarrow{\scriptstyle \chi} \\ G^{r-1} & \xrightarrow[\phi]{} & M \end{array}$$

Then δ can be desribed by

$$\delta[\phi] = [d\widetilde{\phi}]$$

where d is the boundary map of $C^\bullet(G, M_*)$. So going around the top of the square, we get

$$\psi_{\alpha,\beta,r}\delta[\phi] = \psi_{\alpha,\beta_r}\left[d\widetilde{\phi}\right] = \left[\beta \circ d\widetilde{\phi} \circ \alpha^r\right]$$

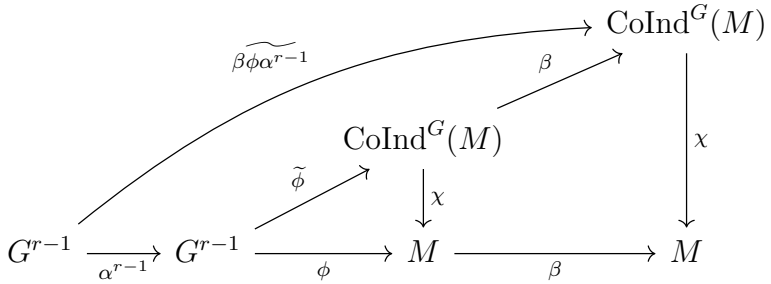
and from the bottom of the square we get

$$\delta\psi_{\alpha,\beta,r}[\phi] = \delta\left[\beta\phi\alpha^r\right] = \left[d\left(\widetilde{\beta\phi\alpha^{r-1}}\right)\right]$$

where $\widetilde{\beta\phi\alpha^{r-1}}$ is any lift making the following diagram commute.

$$\begin{array}{ccc} & & \mathrm{CoInd}^G(M) \\ & \overset{\widetilde{\beta\phi\alpha^{r-1}}}{\nearrow} & \downarrow{\scriptstyle \chi} \\ G^{r-1} & \xrightarrow[\beta\phi\alpha^{r-1}]{} & M \end{array}$$

Now observe the following hideous diagram.



Since χ is a G-homomorphism, $\chi\beta = \beta\chi$, so this whole diagram commutes. That is to say,

$$\beta\widetilde{\phi}\alpha^{r-1} = \widetilde{\beta\phi\alpha^{r-1}}$$

is a suitable lift of $\beta\phi\alpha^{r-1}$ for computing δ, so

$$\delta\psi_{\alpha,\beta_r}[\phi] = \left[d\left(\widetilde{\beta\phi\alpha^{r-1}}\right)\right] = \left[d\left(\beta\widetilde{\phi}\alpha^{r-1}\right)\right]$$

Thus to complete the proof of commutativity, it suffices to show that

$$\beta \circ d\widetilde{\phi} \circ \alpha^r = d\left(\beta\widetilde{\phi}\alpha^{r-1}\right)$$

for any cochain $\widetilde{\phi}$. This equality is "immediate" from the definitions of d, α, β, in the sense that it takes a fair amount of boring and/or trivial algebraic manipulation. □

Remark 3.13.4. The previous lemma didn't actually use any special properties of the sequence $0 \to M \to \mathrm{CoInd}^G(M) \to M_* \to 0$, or any particular aspect of the map χ, so the lemma could be stated more generally in terms of any short exact sequence, saying that the maps $\psi_{\alpha,\beta}$ commute with connecting homomorphisms. In more sophisticated language, this says that the maps $\psi_{\alpha,\beta}$ give a morphism of δ-functors from $H^r(G, -)$ to itself.

Proposition 3.13.5. *Let K be a field and let $G = \mathrm{GL}_n(K), M = K^n$ with the usual G-action by left matrix multiplication. Let $x = -\mathrm{Id} \in \mathrm{GL}_n(K)$, and consider the corresponding maps α, β associated to x as in Definition 3.13.1. Then*

1. *For $r \geq 0$, the maps $H^r(G, M) \to H^r(G, M)$ induced by the compatible pair α, β are $-\mathrm{Id}$.*
2. *If $\mathrm{char}\, K \neq 2$, $H^r(G, M) = 0$ for $r \geq 0$.*

Proof. (1) On the level of cochains, the maps induced by $, \alpha, \beta$ are

$$C^r(G, M) \to C^r(G, M) \qquad \phi \mapsto \beta \circ \phi \circ \alpha^r$$

In this instance, since g_0 is central, $\alpha : G \to G$ is the identity map, so $\alpha^r : G^r \to G^r$ is the identity map. The map $\beta : K^n \to K^n$ is just multiplication by $(-\mathrm{Id})^{-1} = -\mathrm{Id}$, so the map on cochains is just $-\mathrm{Id}$. Thus the induced map $H^r(G, M) \to H^r(G, M)$ is also $-\mathrm{Id}$.

(2) By Proposition 3.13.2, the induced maps $H^r(G, M) \to H^r(G, M)$ from α, β are the identity, but by part (1), the same induced maps are also $-\mathrm{Id}$. Since $\mathrm{char}\, K \neq 2$,

$$\mathrm{Id} = -\mathrm{Id} \implies 2\,\mathrm{Id} = 0 \implies \mathrm{Id} = 0$$

Thus identity map on $H^r(G, M)$ is the zero map, which is to say, it is the trivial group. □

3.13.2 $H^1(G, \mathbb{F}_p) \cong \mathbb{F}_p^n$ gives generators for a p-group G

Let p be a prime. Recall that a p-group is a group G whose order is a power of p. We view $\mathbb{F}_p$ (or by another name $\mathbb{Z}/p\mathbb{Z}$) as a trivial module for any group. In this section, we investigate what happens if $H^1(G, \mathbb{F}_p) \cong \mathrm{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, \mathbb{Z}/p\mathbb{Z})$ happens to be isomorphic to $\mathbb{F}_p^n$. This happens, for example, if $G^{\mathrm{ab}} \cong \mathbb{Z}/p\mathbb{Z}^n$. We start with some classic fixed point results and results about subgroups of p-groups.

Lemma 3.13.6. *Let G be a finite p-group.*

1. *If G acts on a finite set X, then $|X| \equiv |X^G| \bmod p$, where X^G is the set of fixed points.*
2. *If $H \subset G$ is a proper subgroup, then $N_G(H) \neq H$.*
3. *If $H \subset G$ is a proper subgroup, then H is contained in a normal subgroup. In particular, if H is not normal, then H is contained in a proper normal subgroup.*
4. *G has a nontrivial proper normal subgroup.*
5. *Let $N \subset G$ be a nontrivial proper normal subgroup. Then G has a chain of subgroups*

$$1 \subset H_2 \subset H_3 \subset \cdots \subset N \subset \cdots \subset G$$

   where $|H_i| = p^i$. (There is a subgroup of each p-power order in the chain.)

6. *G has a chain of subgroups*

$$1 \subset H_2 \subset H_3 \subset \cdots \subset G$$

   where $|H_i| = p^i$. (There is a subgroup of each p-power order in the chain.)

7. *If $H \subset G$ is a proper subgroup, then H is contained in a normal subgroup of index p.*

Proof. (1) Write X as a disjoint union of orbits, which gives an equality in terms of sizes.

$$X = \bigsqcup_{x \in I} \mathrm{orb}(x) \implies |X| = \sum_{x \in I} |\mathrm{orb}(x)|$$

If we let $J \subset I$ denote the subset corresponding to orbits of size greater than one, this gives

$$|X| = |X^G| + \sum_{x \in J} |\mathrm{orb}(x)| \tag{3.13.1}$$

By the orbit-stabilizer theorem,

$$|\mathrm{orb}(x)| = \frac{|G|}{|\mathrm{stab}(x)|}$$

Since G is a p group, this implies $|\mathrm{orb}(x)| \equiv 0 \bmod p$ for $x \in J$. Thus by equation 3.13.1, the terms of the sum all vanish modulo p, and we obtain $|X| \equiv |X^G| \bmod p$.

(2) If H is the trivial subgroup, the normalizer is all of G and the result is immediate, so we may assume H is nontrivial. Let $X = G/H$ be the set of left cosets of H in G, and let H act on X by left multiplication.

$$H \times G/H \to G/H \qquad h \cdot gH = hgH$$

Note that the coset H is a fixed point of this action. Since $|G/H| \equiv 0 \bmod p$, and there is at least one fixed point, there are at least p fixed points by (1). Thus there is a coset $gH \neq H$ which is a fixed point, with a representative $g \in G \setminus H$, that is, $hgH = gH$ for all $h \in H$. Rearranging this to $g^{-1}hgH = H$ says that $g^{-1}hg \in H$ for all $h \in H$, which is to say, $g \in N_G(H)$. Thus $g \in N_G(H) \setminus H$ so $N_G(H) \neq H$.

(3) Consider the chain of subgroups

$$H \subset N_G(H) \subset N_G(N_G(H)) \subset \cdots \subset G$$

Since this is a finite chain, some normalizer N appearing has $N_G(N) = G$, hence N is normal. Thus H is contained in a normal subgroup. If H is not normal, then $N_G(H) \neq G$, so one of the normalizers is a proper normal subgroup containing H.

(4) By Cauchy's theorem, G has an element of order p which generates a subgroup H of order p. If H is normal, then we are done. If H is not normal, then by (3) H is contained in a nontrivial proper normal subgroup.

(5) We proceed by induction on the order of G. The case $|G| = p$ is trivial. Now assume the result holds for $|G| < p^k$ for some k, and let G be a group of order p^k.

By inductive hypothesis, N (and hence G) has a full chain of subgroups of p-power order up to $|N|$. Also by inductive hypothesis, G/N has a full chain of subgroups of p-power order up to $|G/N|$, and by the correspondence between subgroups of G/N and subgroups of G containing N, the chain of subgroups of G/N corresponds to a full chain subgroups from N to G.

(6) Immediate from (5).

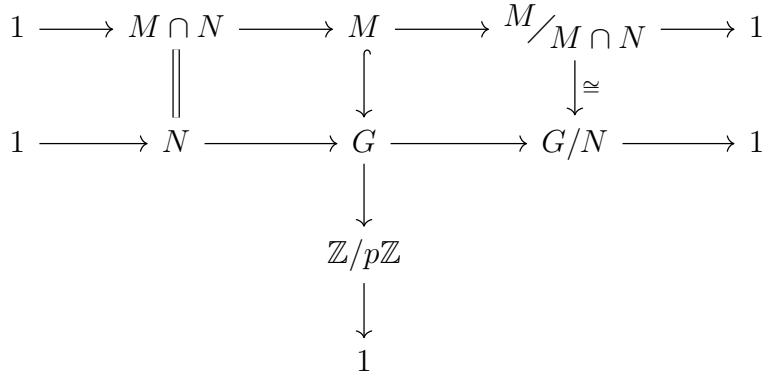
(7) Any subgroup whose index is the smallest prime dividing $|G|$ is normal, so any subgroup of G of order $|G|/p$ is normal, so it suffices to show that a proper subgroup H is contained in a subgroup of order $|G|/p$. By (3), H is contained in a normal subgroup, and then by (5) that normal subgroup is contained in a subgroup of index p. □

Proposition 3.13.7. *Let G be a finite p-group and let $L = G^{\mathrm{ab}} \otimes \mathbb{F}_p = G/G^p[G,G]$. Let $N = G^p[G,G]$. Suppose $x_1, \ldots, x_n \in G$ are such that $x_1N, \ldots, x_nN$ generate L. Then $x_1, \ldots, x_n$ generate G.*

Proof. Let $H = \langle x_1, \ldots, x_n \rangle$ be the subgroup generated by $x_1, \ldots, x_n$, and suppose $H \neq G$. Then by Lemma 3.13.6 part 7, there exists a proper normal subgroup M of index p such that $H \subset M$.

Since $H \subset M$, $M/(M \cap N) \cong G/H$. Also, $G/M \cong \mathbb{Z}/p\mathbb{Z}$, and since this is abelian, $[G,G] \subset M$. Also G^p is in the kernel of $G \to G/M$, which is M, so $N \subset M$, so $M \cap N = N$.

Then we have the following commutative diagram with exact rows.



But by the five lemma (for groups), the middle map must be an isomorphism, which is a contradiction. Hence $H = G$. □

Remark 3.13.8. There is another way to prove Proposition 3.13.7 by developing some theory about Frattini subgroups. The Frattini subgroup $\Phi(G)$ is the intersection of all proper maximal subgroups. Roughly, the outline of that approach is as follows.

1. If G is a p-group and $H \subset G$ such that $G/H \cong \oplus \mathbb{Z}/p\mathbb{Z}$ (G/H is elementary abelian), then $H \subset \Phi(G)$.
2. For a p-group G, $\Phi(G) = G^p[G, G]$.
3. $\Phi(G)$ is equal to the set of nongenerators, hence any set of generators for $G/\Phi(G)$ is lifts to a set of generators of G.

But of course, we can do this without reference to Frattini subgroups, so we return to ignoring the existence of Frattini subgroups, and proceed to our main result.

Proposition 3.13.9. *Let G be a finite p-group, and suppose $\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) = n$ where $\mathbb{F}_p$ is a trivial G-module. Then G has a set of generators $x_1, \ldots, x_n$.*

Proof. We switch to using $\mathbb{Z}/p\mathbb{Z}$ instead of $\mathbb{F}_p$. Since $\mathbb{Z}/p\mathbb{Z}$ is a trivial G-module,

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z}/p\mathbb{Z})$$

Since $\mathbb{Z}/p\mathbb{Z}$ is abelian, any homomorphism $G \to \mathbb{Z}/p\mathbb{Z}$ factors through G^{ab}, thus

$$\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, \mathbb{Z}/p\mathbb{Z})$$

Any $\mathbb{Z}$-homomorphism $X \to \mathbb{Z}/p\mathbb{Z}$ factors through X/pX, and may then be viewed as a $\mathbb{Z}/p\mathbb{Z}$-homomorphism, so

$$\mathrm{Hom}_{\mathbb{Z}}(G^{\mathrm{ab}}, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}}\left(G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p, \mathbb{Z}/p\mathbb{Z}\right) = \left(G^{\mathrm{ab}}/(G^{\mathrm{ab}})^p\right)^*$$

where $*$ denotes the dual. Since $\mathbb{Z}/p\mathbb{Z}$ is a vector space, any module is isomorphic to its dual. Combining all our isomorphisms,

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong {G^{\text{ab}}}/{(G^{\text{ab}})^p}$$

Finally, consider the short exact sequence of groups

$$\begin{array}{ccccccccc} 1 & \longrightarrow & {G^p[G,G]}/{[G,G]} & \longrightarrow & {G}/{[G,G]} & \longrightarrow & \dfrac{{G}/{[G,G]}}{{G^p[G,G]}/{[G,G]}} & \longrightarrow & 1 \\ & & = & & = & & \cong & & \\ & & \left(G^{\text{ab}}\right)^p & & G^{\text{ab}} & & {G}/{G^p[G,G]} & & \end{array}$$

The isomorphism for the final term is from the 3rd isomorphism theorem. By the 1st isomorphism theorem applied to this sequence,

$${G^{\text{ab}}}/{\left(G^{\text{ab}}\right)^p} \cong {G}/{G^p[G,G]}$$

Let $L = G^p[G,G]$ as in Proposition 3.13.7. Putting this all together,

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong L$$

Finally, we use our main hypothesis, that $H^1(G, \mathbb{Z}/p\mathbb{Z})$ is n-dimensional over $\mathbb{Z}/p\mathbb{Z}$, which is to say,

$$H^1(G, \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^n \cong L$$

So L has a set of generators $x_1N, \ldots, x_nN$. Then by Proposition 3.13.7, the elements $x_1, \ldots, x_n$ generate G. $\square$

Chapter 4

Brauer groups

Now we turn to something that is at first look, unrelated to group cohomology, which is the Brauer group of a field. There will be no group rings, projective resolutions, or long exact sequences. Instead, we will talk about fields, matrix algebras, and endomorphism rings. However, one of the great insights is that these two sets of language are connected in a key way - the Brauer group, as defined in terms of algebras over a field K, is also isomorphic to the second profinite cohomology group $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times})$.

Philosophically speaking, what is the Brauer group? It is an abelian group denoted $\mathrm{Br}(K)$ associated to a field K, so it is an algebraic invariant of K. What does it measure? In some sense, it measures how "algebraically complicated" K is. For example, the Brauer group of an algebraically closed field (such as $\mathbb{C}$) is the trivial group, and the Brauer group of the real numbers $\mathbb{R}$ will be $\mathbb{Z}/2\mathbb{Z}$.

So $\mathrm{Br}(K)$ somehow detects that $\mathbb{R}$ is not algebraically closed, but $\mathbb{R}$ is "close" to being algebraically closed, in the sense that it only takes a degree 2 field extension of $\mathbb{R}$ to get an algebraically closed field ($\mathbb{C}$). The Brauer group of a field which is "further" from being algebraically closed is usually "bigger," whatever that means. Obviously, this is an imprecise statement, just intended to provide intuition and motivation.

Just defining the Brauer group in terms of central simple algebras takes a fair bit of set up, so that is the concern of the first several sections of this chapter. We need some key results about central simple algebras, like Wedderburn's theorem, the Skolem-Noether theorem, and the double centralizer theorem, before we can even define $\mathrm{Br}(K)$.

Even after that, it is not that easy to compute Brauer groups. We can compute it for $\mathbb{R}$ and finite fields, but not too much more. To compute any more, we need to establish the isomorphism with $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times})$ to make more calculations. Once we have that, we can compute the Brauer group of a local field, which leads into local class field theory (though we don't go into local class field theory here).

4.1 Wedderburn's theorem

Throughout, let K be a field. We will rarely put any additional assumptions on K, such as the characteristic, or algebraically closed. An algebra A over K, also called a K-algebra, is a K-vector space which also has a multiplication operation which makes A into a ring. We

will always assume that K-algebras have a unit, and are associative. However, we will NOT assume they are commutative, in fact, it is reasonable to say that "most" of them will not be commutative.

If A is a K-algebra as we have described, we use 1 to denote the unit element of A. Then there is an embeddings $K \hookrightarrow A, x \mapsto 1x$, and we midly abuse language by referring to K as a subset of A by identifying K with its image under this embedding. In particular, since multiplying elements of A by elements of K is commutative, K is contained in the center of A. However, the center of A may be strictly bigger than K. This leads to our first main definition.

Definition 4.1.1. A K-algebra A is **central** if the center of A is exactly K.

Since A is a ring, we can talk about ideals. Since we rarely assume A is commutative, it can have left ideals, right ideals, and two sided ideals, all of which are often distinct concepts.

Definition 4.1.2. A K-algebra A is **simple** if it has no proper two sided ideals (except the trivial ideal).

The goal of this section is to prove a very strong structure theorem for central simple algebras, called Wedderburn's theorem. Basically, it says that all central simple algebras arise in a very similar way as matrix algebras. Before that, some examples.

Example 4.1.3. Let D be a division algebra over K. Then D is clearly a simple K-algebra, since any nonzero element is a unit and generates all of D as an ideal. The center of D is a field, though not necessarily equal to K. We can at least say that D is a central simple algebra over $Z(D)$.

Example 4.1.4. The complex numbers $\mathbb{C}$ are a simple $\mathbb{R}$-algebra, but not central because $\mathbb{C}$ is commutative. However, the Hamilton quaternions $\mathbb{H}$ is a central simple $\mathbb{R}$-algebra. They have a presentation

$$\mathbb{H} = \langle 1, i, j, ij \mid i^2 = j^2 = -1, ij = -ji \rangle$$

It is a division algebra, so by the previous example, it is simple. To show that $\mathbb{H}$ is a division algebra, define the conjugate of a quaternion $q = a + bi + cj + dij$ to be $\overline{q} = a - bi - cj - dij$, and define the norm map

$$N : \mathbb{H} \to \mathbb{R} \qquad q \mapsto q\overline{q}$$

Then show that $q \in \mathbb{H}$ is a unit if and only if $N(q) \neq 0$, and show that N only vanishes for $q = 0$. To see that $\mathbb{H}$ is also central, it mostly suffices to observe that i, j, ij are not central since i, j anti-commute.

Example 4.1.5. Let A be any K-algebra. We will show that $M_n(A)$ is central. For $1 \leq i, j \leq n$, let $e_{ij} \in M_n(A)$ denote the matrix with a 1 in the ijth entry and zeros elsewhere. Note that for $X = (x_{ij}) \in M_n(A)$,

$$e_{ii}X = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ x_{i1} & \cdots & x_{in} \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \qquad Xe_{ii} = \begin{pmatrix} 0 & \cdots & x_{1i} & \cdots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & x_{ni} & \cdots & 0 \end{pmatrix}$$

with the nonzero entries appearing in the ith row and ith column, respectively. Suppose $X \in M_n(D)$ is central, so $e_{ii}X = Xe_{ii}$ for $1 \leq i \leq n$. This forces all of the off-diagonal elements of X in the ith row and ith column to be zero. Hence X is diagonal. Then since X commutes with permutation matrices, all the diagonal elements have to be the same. For example,

$$\begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & \mathrm{Id} \end{pmatrix} X = \begin{pmatrix} 0 & x_{22} & \\ x_{11} & 0 & \\ & & * \end{pmatrix} = X \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & \mathrm{Id} \end{pmatrix} = \begin{pmatrix} 0 & x_{11} & \\ x_{22} & 0 & \\ & & * \end{pmatrix}$$

Thus $X = \lambda \,\mathrm{Id}$ for some $\lambda \in K$, which shows that $M_n(A)$ is central.

Example 4.1.6. Let D be a division algebra over K. By the previous example, $M_n(D)$ is central. We also claim that is is simple. It suffices to show that for $X = (x_{ij}) \in M_n(D)$ nonzero, the two sided ideal $\langle X \rangle$ generated by X contains e_{ij} for all i, j, since the e_{ij} give a D-basis of $M_n(D)$. Because of the relation

$$e_{ki}e_{ij}e_{j\ell} = e_{k\ell}$$

if one e_{ij} lies in $\langle X \rangle$, then all of them do, so suffices to show that $e_{ij} \in \langle X \rangle$ for some i, j. Choose i, j so that $x_{ij} \neq 0$. Then

$$x_{ij}^{-1} e_{ii} X e_{jj} = e_{ij}$$

so $e_{ij} \in \langle X \rangle$.

As we already alluded, Wedderburn's theorem is a powerful structure theorem for central simple algebras, which is a sort of "converse" to the previous example. The previous example said that $M_n(D)$ is central simple, and Wedderburn says that this is actually not special - all central simple algebras are some matrix algebra over a division algebra. We state it now, but delay the proof a bit more.

Theorem 4.1.7 (Wedderburn)**.** *Let A be a finite dimensional simple algebra over a field K. Then $A \cong M_n(D)$ for a unique $n \geq 1$ and a unique up to isomorphism division K-algebra D. Conversely, any algebra of the form $M_n(D)$ where D is a division algebra, is simple.*

Before the proof, we need a few technical lemmas, which we omit proofs for.

Definition 4.1.8. Let A be a K-algebra. For A considered as a left A-module, we write ${}_AA$.

Lemma 4.1.9. *Let A be a (finite dimensional, unital, associative) simple K-algebra, and let $M \subset A$ be a minimal left ideal. Then*

1. *There exists $n > 0$ so that ${}_AA \cong \bigoplus_{i=1}^n M$ as A-modules.*
2. *Any A-module is iosmorphic to a direct sum of copies of M. In particular, M is the only simple A-module.*

Proof. Proposition 1 of Rapinchuk [12]. □

Lemma 4.1.10. *Let A be a K-algebra and let M be a left A-module. Then there is an isomorphism of K-algebras*

$$\mathrm{End}_A(M^n) \cong M_n(\mathrm{End}_A(M))$$

Proof. Stated and proved in somewhat more generality in Lemma 1 of Rapinchuk [12]. □

Lemma 4.1.11. *Let $A = M_n(D)$ where D is a division ring, and let $V = D^n$ be the space of n-columns on which A acts by left multiplication. Then V is a simple A-module and $\mathrm{End}_A(V) \cong D^{\mathrm{op}}$.*

Proof. Lemma 2 of Rapinchuk [12]. □

Now we finally prove Wedderburn's theorem.

Theorem 4.1.12 (Wedderburn)**.** *Let A be a finite dimensional simple algebra over a field K. Then $A \cong M_n(D)$ for a unique $n \geq 1$ and a unique up to isomorphism division K-algebra D. Conversely, any algebra of the form $M_n(D)$ where D is a division algebra, is simple.*

Proof. First, we claim that

$$\mathrm{End}_A({}_AA) \to A^{\mathrm{op}} \qquad \phi \mapsto \phi(1)$$

is an isomorphism of K-algebras. If $\phi \in \mathrm{End}_A({}_AA)$, then for $a \in A$,

$$\phi(a) = a\phi(1)$$

so ϕ is determined by $\phi(1)$, so the claimed map is certainly bijective. It is K-linear because $K \hookrightarrow A$ and ϕ is A-linear. Finally, we show it is a homomorphism. We use $\cdot$ to denote multiplication in A^{op}. Then

$$\phi \circ \psi \mapsto \phi(\psi(1)) = \psi(1)\phi(1) = \phi(1) \cdot \psi(1)$$

so this establishes $\mathrm{End}_A({}_AA) \cong A^{\mathrm{op}}$ as K-algebras. By Proposition 4.1.9 part (1), ${}_AA \cong M^n$ as an A-module, so $\mathrm{End}_A({}_AA) \cong \mathrm{End}_A(M^n)$. By Lemma 4.1.10, we have $\mathrm{End}_A(M^n) \cong M_n(\mathrm{End}_A(M))$. Putting these isomorphisms together,

$$A^{\mathrm{op}} \cong \mathrm{End}_A({}_AA) \cong \mathrm{End}_A(M^n) \cong M_n(\mathrm{End}_A(M))$$

For any ring R, we have an isomorphism

$$M_n(R) \to M_n(R^{\mathrm{op}}) \qquad m \mapsto m^T$$

which in the case $R = \mathrm{End}_A(M)$, gives

$$M_n(\mathrm{End}_A(M))^{\mathrm{op}} \cong M_n(\mathrm{End}_A(M)^{\mathrm{op}})$$

so

$$A \cong (A^{\mathrm{op}})^{\mathrm{op}} \cong M_n(\mathrm{End}_A(M))^{\mathrm{op}} \cong M_n(\mathrm{End}_A(M)^{\mathrm{op}})$$

By Schur's lemma, $\mathrm{End}_A(M)$ is a division ring, so it's opposite is also a division algebra. Thus $A \cong M_n(D)$ for some division algebra D.

Now for uniqueness. Suppose $A \cong M_{n_1}(D_1) \cong M_{n_2}(D_2)$. Let $V_1 = D_1^{n_1}, V_2 = D_2^{n_2}$. By Lemma 4.1.11, V_1, V_2 are simple A-modules. Then by Proposition 4.1.9 part (2), $V_1 \cong V_2$ as A-modules. Using Lemma 4.1.11 again,

$$D_1^{\mathrm{op}} \cong \mathrm{End}_A(V_1) \cong \mathrm{End}_A(V_2) \cong D_2^{\mathrm{op}}$$

hence $D_1 \cong D_2$ as K-algebras, proving uniqueness of D. Also,

$$\dim_K A = n_1^2 \dim_K D_1 = n_2^2 \dim_K D_2$$

implies $n_1 = n_2$ since $D_1 \cong D_2$. □

Wedderburn's theorem is very powerful and imposes a lot of structure on an arbitrary central simple algebra. Already, we have the following corollary which restricts the possible dimensions of central simple algebras to squares.

Corollary 4.1.13 (Dimension of central simple algebra is a square)**.** *Let A be a finite dimensional central simple K-algebra. Then $\dim_K A$ is a perfect square.*

Proof. Let $\overline{K}$ be an algebraic closure of K, and let $B = A \otimes_K \overline{K}$. By Proposition 4.3.3, B is simple, so by Wedderburn's theorem, $B \cong M_n(D)$. By Proposition 4.6.1, $D = \overline{K}$. Then

$$\dim_K A = (\dim_K A)(\dim_{\overline{K}} \overline{K}) = \dim_{\overline{K}} B = n^2$$

□

4.2 Skolem-Noether theorem and double centralizer theorem

Similar to Wedderburn's theorem, though not quite as powerful, are the following theorems which we will use ubiquitously in what follows. We leave out the proofs, since they are rather boring.

Theorem 4.2.1 (Skolem-Noether)**.** *Let A, B be finite dimensional simple K-algebras with B central. If $f, g : A \to B$ are two K-algebra homomorphisms, then there exists $b \in B^\times$ such that*

$$g(a) = bf(a)b^{-1} \qquad \forall a \in A$$

Definition 4.2.2. Let A be a K-algebra, and let $B \subset A$ be any subset. The **centralizer of B in A is**

$$Z_A(B) = \{x \in A \mid xb = bx,\ \forall b \in B\}$$

Theorem 4.2.3 (Double centralizer)**.** *Let A be a central simple simple K-algebra, and let $B \subset A$ be a simple subalgebra. Then*

1. $Z_A(B) \otimes_K M_{\dim_K B}(K) \cong A \otimes B^{\mathrm{op}}$
2. *$Z_A(B)$ is a simple subalgebra of A of dimension $\frac{\dim_K A}{\dim_K B}$.*
3. $Z_A(Z_A(B)) = B$. *(This is the result usually known as the double centralizer theorem.)*

4.3 Defining the Brauer group

We now have most of the background tools we need to define the Brauer group, although the official definition has to wait until Definition 4.3.9. Given a field K, the Brauer group $\mathrm{Br}(K)$ is going to be equivalence classes of central simple algebras. Roughly speaking, the equivalence relation declares matrix algebras $M_n(K)$ to be "trivial."

The operation in $\mathrm{Br}(K)$ is essentially tensor product - given two central simple K-algebras A, B, the product of them in the Brauer group is the equivalence class of $A \otimes_K B$. Making this precise is most of the work before the official definition - we need to prove that the tensor product algebra $A \otimes_K B$ is central simple, which takes some doing. We also need to verify that this operation repects the equivalence relation, and we need to locate inverse elements. Once we do that, we'll have a a definition for the Brauer group.

4.3.1 Lemmas needed to define the Brauer group

The first question we address is how centers of algebras and central algebras interact with taking tensor products of algebras, which is definitively resolved in Proposition 4.3.2.

Lemma 4.3.1. *Let V, W be K-vector spaces. Let $w_1, \ldots, w_n \in W$ be linearly independent. If there exist $v_1, \ldots, v_n \in V$ such that*

$$\sum_{i=1}^{n} v_i \otimes w_i = v_1 \otimes w_n + \cdots + v_n \otimes w_n = 0 \in V \otimes_K W$$

then $v_1 = \cdots = v_n = 0$.

Proof. Extend $w_1, \ldots, w_n$ to a basis $w_1, \ldots, w_n, \ldots, w_{\dim W}$ of W. Let $x_1, \ldots, x_{\dim V}$ be a basis of V, and write v_i as

$$v_i = \sum_j \alpha_{ij} x_j \qquad \alpha_{ij} \in K$$

Then

$$0 = \sum_i v_i \otimes w_i = \sum_i \left(\sum_j \alpha_{ij} x_j \right) \otimes w_i = \sum_{i,j} \alpha_{ij} (x_j \otimes w_i)$$

Since the simple tensors $x_j \otimes w_i$ form a basis of $V \otimes_K W$, by linear independence $\alpha_{ij} = 0$ for all i, j. That is, $v_i = 0$ for all i. □

Proposition 4.3.2 (Tensor product of central algebras is central)**.** *Let A, B be algebras over K. Then*

$$Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$$

In particular, the tensor product of central algebras is central.

Proof. The inclusion $\supset$ is easy, so we dispatch it first. If $a \otimes b \in Z(A) \otimes Z(B)$, then for any $x \otimes y \in A \otimes B$,

$$(x \otimes y)(a \otimes b) = xa \otimes yb = ax \otimes by = (a \otimes b)(x \otimes y)$$

thus $a \otimes b \in Z(A \otimes B)$. The reverse inclusion is not so immediate. Let $z \in Z(A \otimes B)$, and write it as

$$z = \sum_{i=1}^{n} a_i \otimes b_i \qquad a_i \in A, b_i \in B$$

and choose this so that n is minimal. We claim that the set $\{a_1, \ldots, a_n\}$ is linearly independent over K, as is the set $\{b_1, \ldots, b_n\}$. Suppose not, so that $b_1, \ldots, b_n$ are linearly independent, so we can write b_1 as a K-linear combination

$$b_1 = \beta_2 b_2 + \cdots + \beta_n b_n \qquad \beta_i \in K$$

Then we can write z as

$$z = \left(a_1 \otimes \sum_{i=2}^{n} \beta_i b_i \right) + \sum_{i=2}^{n} a_i \otimes b_i = \sum_{i=2}^{n} (\beta_i a_1 + a_i) \otimes b_i$$

contradicting the minimality of n from earlier. The same argument with roles reversed shows the linear independence of the a_i. Now we claim that $a_i \in Z(A)$ and $b_i \in Z(B)$ for $i = 1, \ldots, n$. For any $a \in A$, since $z \in Z(A \otimes B)$, we have

$$0 = (a \otimes 1)z - z(a \otimes 1) = \sum_{i=1}^{n} (aa_i - a_i a) \otimes b_i$$

Then by linear indepence of the b_i and Lemma 4.3.1, the we have $aa_i - a_i a = 0$ for all i, that is, $aa_i = a_i a$ which says that $a_i \in Z(A)$ for all i. By the same argument with roles reversed, $b_i \in Z(B)$ for all i. Hence $z \in Z(A) \otimes Z(B)$. □

Having resolved the interaction of central-ness and tensor products, we need to know a similar relationship for simple-ness. The relationship is not quite as clean, but good enough. The proof is very technical so we leave it out.

Proposition 4.3.3 (Tensor product of simple algebras is simple, if one is central)**.** *Let A, B be simple K-algebras, at least one of which is also central. Then $A \otimes_K B$ is a simple K-algebra.*

Proof. See Theorem 2 of Rapinchuk [12]. □

We mentioned earlier that the equivalence relation in the Brauer group is going to force matrix algebras $M_n(K)$ to be trivial in $\mathrm{Br}(K)$. The next lemma explains why this has to be the case - tensoring with a matrix algebra over K does not really change the algebra in a "significant" way. That is, it does not change the associated division algebra (coming from Wedderburn's theorem), it just increases the dimension. A good way to think of (1) in the next lemma is that it says that $M_n(K)$ represents the identity element of $\mathrm{Br}(K)$.

Lemma 4.3.4 (Identity for Brauer group)**.** *Let K be a field. Then*

1. *For any K-algebra R and positive integer n, $R \otimes_K M_n(K) \cong M_n(R)$.*
2. *For any positive integers m, n, $M_m(K) \otimes_K M_n(K) \cong M_{mn}(K)$.*

Proof. (1) An isomorphism is given by

$$R \otimes_K M_n(K) \to M_n(R) \qquad r \otimes x \mapsto rx$$

with inverse given by

$$M_n(R) \mapsto R \otimes_K M_n(K) \qquad (r_{ij}) \mapsto \sum_{i,j} r_{ij} \otimes e_{ij}$$

where e_{ij} is the matrix with 1 in the ijth entry and zeroes elsewhere.

(2) Up to choice of basis, $M_m(K) \cong \mathrm{End}_K(K^m)$, so we work with the endomorphism rings instead. There is a homomorphism

$$\mathrm{End}_K(K^m) \otimes_K \mathrm{End}_K(K^n) \to \mathrm{End}_K(K^m \otimes K^n) = \mathrm{End}_K(K^{mn})$$
$$\phi \otimes \psi \mapsto \Big(x \otimes y \mapsto \phi(x) \otimes \psi(y)\Big)$$

Note that by Proposition 4.3.3, the domain is a simple algebra. Then since the map is nonzero, it is injective (since the domain is simple). Then since the dimensions are equal, it is an isomorphism. □

Before we even define the Brauer group, we're going to address the question of inverses. Of course, we haven't described the equivalence relation yet, but we do know that the identity element should be represented by a matrix algebra $M_n(K)$.

So given an algebra A, how to find an algebra which we can tensor with A to obtain a matrix algebra? Is there some algebra associated to A which is a clear candidate? Perhaps the reader sees this as coming out of thin air, but the opposite algebra A^{op} is one algebra we might consider, and it turns out to be the right choice.

A^{op} is the same as A as a set, but the multiplication operation is reversed. This reversal doesn't affect what the center is, or affect two-sided ideals, so A^{op} is central simple (as long as A was).

Proposition 4.3.5 (Inverses for Brauer group)**.** *Let A be a central simple K-algebra of dimension d. Then*

$$A \otimes_K A^{\mathrm{op}} \cong \mathrm{End}_K(A) \cong M_d(K)$$

Note that these are isomorphisms of K-algebras.

Proof. For $a \in A$, define

$$L_a : A \to A \qquad x \mapsto ax$$
$$R_a : A \to A \qquad x \mapsto xa$$

Note that $L_a, R_a \in \mathrm{End}_K(A)$. Then define

$$L : A \to \mathrm{End}_K(A) \qquad a \mapsto L_a$$
$$R : A^{\mathrm{op}} \to \mathrm{End}_K(A) \qquad a \mapsto R_a$$

We claim that L, R are K-algebra homomorphisms. First we verify K-linearity. Let $a \in A, \lambda \in K$.

$$L_{\lambda a} = (x \mapsto \lambda a x) = \lambda(x \mapsto ax) = \lambda L_a$$
$$R_{\lambda a} = (x \mapsto x\lambda a) = \lambda(x \mapsto xa) = \lambda R_a$$

Now we verify that they preserve multiplication. Let $a, b \in A$. We denote multiplication in A^{op} by $a \cdot b = ba$. (Adjacent letters with no symbol denotes usual multiplication in A.)

$$L_{ab} = (x \mapsto abx) = (x \mapsto ax) \circ (x \mapsto bx) = L_a L_b$$
$$R_{a \cdot b} = (x \mapsto x(a \cdot b)) = (x \mapsto xba) = (x \mapsto xa) \circ (x \mapsto xb) = R_a R_b$$

Now we note that for $a, b \in A$, L_a, R_b commutes in $\text{End}_K(A)$.

$$L_a R_b(x) = L_a(bx) = abx = R_b(ax) = R_b L_a(x)$$

Thus we have a K-algebra homomorphism

$$F : A \otimes_K A^{\text{op}} \to \text{End}_K(A) \qquad a \otimes b \mapsto L_a R_b = R_b L_a = (x \mapsto axb)$$

Since A is simple, so is A^{op}, so by Proposition 4.3.3, $A \otimes_K A^{\text{op}}$ is simple (this is where we use the fact that A is central). Hence since F is not the zero morphism, it is injective. But then by dimension counting, it is also surjective, so

$$A \otimes_K A^{\text{op}} \cong \text{End}_K(A)$$

As a K-vector space, A is just K^d, so the final isomorphism $\text{End}_K(A) \cong M_d(K)$ is the usual basis-dependent isomorphism between K-linear maps $K^d \to K^d$ and $d \times d$ matrices with entries in K. □

4.3.2 Definition of Brauer equivalence

Now that we've done the hard part of addressing aspects of Brauer group multiplication, we can address the easier part, which is just what the right equivalence relation $\text{Br}(K)$ should have. The first somewhat reasonable choice is to use the division algebra invariant associated to a central simple algebra A by Wedderburn's theorem - the uniqueness aspect makes it a good invariant, so we could declare central simple algebras to be equivalent if they have the same associated division algebra. This is exactly what our equivalence relation is, though we also give another equivalent condition in terms of tensoring with matrix algebras $M_n(K)$ which is frequently given as the definition in other sources.

Lemma 4.3.6 (Equivalent conditions for Brauer group equivalence)**.** *Let A_1, A_2 be central simple algebras over a field K, with $A_1 \cong M_{n_1}(D_1), A_2 \cong M_{n_2}(D_2)$ for unique integers n_1, n_2 and unique up to isomorphism division algebras D_1, D_2 (by Wedderburn's theorem 4.1.7). The following are equivalent.*

1. *$D_1 \cong D_2$*

2. *There exist integers m_1, m_2 such that $A_1 \otimes_K M_{m_1}(K) \cong A_2 \otimes_K M_{m_2}(K)$.*

Proof. First we prove (1) $\implies$ (2). Suppose $D_1 \cong D_2$. Then using Lemma 4.3.4 a few times,

$$\begin{aligned} A_1 \otimes_k M_{n_2}(K) &\cong M_{n_1}(D_1) \otimes_K M_{n_2}(K) \cong \Big(D_1 \otimes_K M_{n_1}(K)\Big) \otimes_K M_{n_2}(K) \\ &\cong D_1 \otimes_K \Big(M_{n_1}(K) \otimes_K M_{n_2}(K)\Big) \cong D_1 \otimes_K M_{n_1 n_2}(K) \\ &\cong M_{n_1 n_2}(D_1) \cong M_{n_1 n_2}(D_2) \cong D_2 \otimes_K M_{n_1 n_2}(K) \\ &\cong D_2 \otimes_K \otimes_K M_{n_2}(K) \otimes_K M_{n_1}(K) \cong A_2 \otimes_K M_{n_1}(K) \end{aligned}$$

which proves (2). For the converse, suppose $A_1 \otimes_K M_{m_1}(K) \cong A_2 \otimes_K M_{m_2}(K)$. Then using a similar chain of isomorphisms to the above,

$$M_{m_1 n_1}(D_1) \cong A_1 \otimes_K M_{m_1}(K) \cong A_2 \otimes_K M_{m_2}(K) \cong M_{m_2 n_2}(D_2)$$

By the uniqueness of Wedderburn's theorem 4.1.7, this implies $D_1 \cong D_2$. □

Definition 4.3.7. Two central simple algebras are **similar** if either the previous two conditions hold. That is, $A_1 \sim A_2$ if the associated division algebras are isomorphic, or if A_1, A_2 become isomorphic after tensoring with some matrix rings over K.

Lemma 4.3.8. *Similarity as defined above is an equivalence relation.*

Proof. Thinking in terms of condition (1), this is immediate from the uniqueness aspect of Wedderburn's theorem and the fact that isomorphism is an equivalence relation. □

Finally all our work has paid off, and we can define $\mathrm{Br}(K)$ properly.

Definition 4.3.9. The **Brauer group** of a field K is the set of equivalence classes of central simple algebras under the previous equivalence. The product operation is given by

$$[A][B] = [A \otimes_K B]$$

We show this is well defined in the next proposition.

Proposition 4.3.10. *The Brauer group product operation is well defined, associative, and commutative. It has unit $[M_n(K)]$, and an inverse for $[A]$ is given by $[A^{\mathrm{op}}]$.*

Proof. By Proposition 4.3.3, $A \otimes_K B$ is simple, and by Proposition 4.3.2, $A \otimes_K B$ is central, so taking the equivalence class of $A \otimes_K B$ at least makes sense.

We need to verify that this product is independent of the choice of representative algebras A, B. Suppose A', B' are other representatives with $[A] = [A'], [B] = [B']$. Then there are integers m, m', n, n' so that

$$A \otimes_K M_m(K) \cong A' \otimes_K M_{m'}(K) \qquad B \otimes_K M_n(K) \cong B' \otimes_K M_{n'}(K)$$

Then

$$(A \otimes_K B) \otimes_K M_{mn}(K) \cong (A' \otimes_K B') \otimes_K M_{m'n'}(K)$$

hence $[A \otimes_K B] = [A' \otimes_K B']$, so the product is well defined. Associativity and commutativity follow immediately from associativity and commutativity of $\otimes_K$. $[M_n(K)]$ is an identity element by Lemma 4.3.4. $[A^{\mathrm{op}}]$ is an inverse for $[A]$ by Proposition 4.3.5. □

Remark 4.3.11. An equivalence class of central simple K-algebras corresponds, via Wedderburn's theorem 4.1.7 to an isomorphism class of division algebras over K. Thus the points of the Brauer group $\mathrm{Br}(K)$ are in one-to-one correspondence with isomorphism classes of division algebras over K.

4.4 Relative Brauer group

We now have an associated abelian group $\mathrm{Br}(K)$ to any field K, so we have "half a functor." The half missing is that if we have a morphism of fields $K \to L$, there should be an associated morphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$. Of course, the category of fields doesn't have complicated morphisms, because everything is just an embedding, so really the question is, how are $\mathrm{Br}(K)$ and $\mathrm{Br}(L)$ related if L/K is a field extension? This is measured by the relative Brauer group $\mathrm{Br}(L/K)$.

Lemma 4.4.1. *Let L/K be a finite extension and let A, B be K-algebras. Then there is an isomorphism of L-algebras*

$$(A \otimes_K B) \otimes_K L \cong (A \otimes_K L) \otimes_L (B \otimes_K L)$$

Thus

$$\mathrm{Br}(K) \to \mathrm{Br}(L) \qquad [A] \mapsto [A \otimes_K L]$$

is a group homomorphism.

Proof. The isomorphism is straightforward to write down in terms of elements. The homomorphism property follows immediately. □

Definition 4.4.2. Let L/K be a finite field extension. The **relative Brauer group** $\mathrm{Br}(L/K)$ is defined to be the kernel of the homomorphism

$$\mathrm{Br}(K) \to \mathrm{Br}(L) \qquad [A] \mapsto [A \otimes_K L]$$

If we want to emphasize that we're talking about a Brauer group which is not relative, we sometimes refer to $\mathrm{Br}(K)$ as the **absolute Brauer group**.

Since it is not always so easy to tell when an algebra A becomes trivial (becomes isomorphic to a matrix algebra) after tensoring with L, we would like to to characterize $\mathrm{Br}(L/K)$ as a subset of $\mathrm{Br}(K)$ in a way that is easier to check for individual algebras. The following result gives a very convenient characterization.

Loosely speaking, $\mathrm{Br}(L/K)$ is subset of $\mathrm{Br}(K)$ of algebras which "contain" (an isomorphic copy) of L. This isn't really true, though, because it doesn't make sense for an element of $\mathrm{Br}(K)$ to contain an isomorphic copy of L, since an element of $\mathrm{Br}(K)$ is not an algebra, but rather an equivalence class of algebras. So what is more accurate to say is that $\mathrm{Br}(L/K)$ is the subset of $\mathrm{Br}(K)$ for which there exists an algebra in each equivalence class containing a copy of L. The next theorem makes this precise.

Theorem 4.4.3. *Let L/K be a a finite extension and let $n = [L : K]$.*

1. *If A is a central simple K-algebra with $\dim_K A = n^2$ and $L \subset A$, then $A \otimes_K L \cong M_n(L)$.*

2. *If $A \otimes_K L \cong M_n(L)$, then there exists a unique (up to isomorphism) central simple K-algebra A' such that $A \sim A'$, $\dim_K A' = n^2$, and $L \subset A'$.*

Thus

$$\mathrm{Br}(L/K) = \left\{ [A] \in \mathrm{Br}(K) : \dim_K A = n^2, L \subset A \right\}$$

Proof. Theorem 6 of Rapinchuck [12] or Proposition 2.2.9 of Gilles & Szamuely [4]. □

Based on how we just characterized the relative Brauer group $\mathrm{Br}(L/K)$ in terms of subfields of K-algebras, it might be useful later to understand when algebras contain fields and that sort of thing. The main result is the following, which guarantees the existence of a maximal subfield whose dimension is the square root of the dimension of the algebra.

Proposition 4.4.4. *Let D be a central division algebra over a field K of dimension $\dim_K D = d^2$. Then D contains a maximal subfield L which is a separable extension of K, and $\dim_K L = d$.*

$$\begin{array}{c} D \\ \Big| d \\ L \\ \Big| d \\ K \end{array}$$

Proof. Corollary 5 and Proposition 3 of Rapinchuk [12]. Note that there is no uniqueness of L; there may be many maximal subfields, though they must all have dimension d. □

There is a parallel, as we will see more later, between Brauer groups and Galois groups. For a field K with separable closure K^{sep}, the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ is the inverse limit of $\mathrm{Gal}(L/K)$ for all L/K finite Galois, so the absolute Galois group is determined by an collection of finite groups. Similarly, the absolute Brauer group $\mathrm{Br}(K)$ is determined by the collection of the relative Brauer groups $\mathrm{Br}(L/K)$ for all L/K finite Galois, as the next proposition makes precise.

Proposition 4.4.5. *Let K be a field, and let $\mathcal{L}$ be the set of all finite Galois extensions of K. Then*

$$\mathrm{Br}(K) = \bigcup_{L \in \mathcal{L}} \mathrm{Br}(L/K)$$

Proof. Proposition 5 of Rapinchuk [12]. □

The analogy is even better, since the absolute Brauer group $\mathrm{Br}(K)$, which we said corresponds in some way to the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, is equal to the relative Brauer group $\mathrm{Br}(K^{\mathrm{sep}}/K)$, as the next corollary tells us.

Corollary 4.4.6. *Let K be a field with separable closure K^{sep}. Then $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{sep}}/K)$.*

Proof. The inclusion $\supset$ is obvious from the definitions. For the reverse inclusion, we basically repeat the proof of Proposition 5 from Rapinchuk [12].

Let $[A] \in \mathrm{Br}(K)$ with representative central simple algebra A. By Wedderburn's theorem, $A \cong M_d(D)$ for a division algebra D. Let $\ell^2 = \dim_K D$. By Proposition 4.4.4, D contains a subfield P so that P/K is separable, so $P \subset K^{\mathrm{sep}}$. By Theorem 4.4.3 part 1,

$$D \otimes_K P \cong M_\ell(P)$$

Then

$$\begin{aligned} A \otimes_K P &\cong M_d(D) \otimes_K P \\ &\cong (M_d(K) \otimes_K D) \otimes_K P && \text{Lemma 4.3.4} \\ &\cong (M_d(K) \otimes_K P) \otimes_P (D \otimes_K P) && \text{Lemma 4.4.1} \\ &\cong M_d(P) \otimes_P M_\ell(P) && \text{Lemma 4.3.4} \\ &\cong M_{d\ell}(P) && \text{Lemma 4.3.4} \end{aligned}$$

Then since $P \subset K^{\mathrm{sep}}$,

$$A \otimes_K K^{\mathrm{sep}} \cong (A \otimes_K P) \otimes_P K^{\mathrm{sep}} \cong M_{d\ell}(P) \otimes_P K^{\mathrm{sep}} \cong M_{d\ell}(K^{\mathrm{sep}})$$

which is to say, $[A] \in \mathrm{Br}(K^{\mathrm{sep}}/K)$. □

4.5 Brauer group as Galois cohomology group

Before getting to details, we describe the end goal of this section, which is to identify $\mathrm{Br}(K)$ with a certain profinite cohomology group. In particular,

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$$

More generally, we have an isomorphism involving relative Brauer groups.

$$\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times)$$

This isomorphism arises from an isomorphism of inversely directed systems, of which $\mathrm{Br}(L/K)$ and $H^2(\mathrm{Gal}(L/K), L^\times)$ are the respective direct limits. That is, first we will find an isomorphism for L/K finite, then using direct limits we will obtain the general case.

As usual, we omit many details, since the construction of the isomorphism above in the finite case is quite involved, and the proof that the map constructed is an isomorphism is also involved.

4.5.1 2-cocycle (factor set) associated to a central simple algebra

In this section, we associate an element of $H^2(\mathrm{Gal}(L/K), L^\times)$ to an element $[A] \in \mathrm{Br}(L/K)$.

Definition 4.5.1. Let L/K be a finite Galois extension, and recall that

$$\mathrm{Br}(L/K) = \left\{[A] \in \mathrm{Br}(K) : \dim_K A = n^2, L \subset A\right\}$$

Let $[A] \in \mathrm{Br}(L/K)$ with representative A so that $\dim_K A$ and $L \subset A$. Let $\sigma \in \mathrm{Gal}(L/K)$. Since A is central simple over K and L is simple over K, we can apply the Skolem-Noether theorem 4.2.1 to the two homomorphisms

$$\begin{aligned} L &\hookrightarrow A \qquad a \mapsto a \\ L &\hookrightarrow A \qquad a \mapsto \sigma(a) \end{aligned}$$

By Skolem-Noether, these are conjugate, which is to say, there exists $x_\sigma \in A^\times$ so that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \qquad \forall a \in L$$

Then for $\sigma, \tau \in \mathrm{Gal}(L/K)$, define

$$a_{\sigma,\tau} = x_\sigma x_\tau x_{\sigma\tau}^{-1}$$

The collection $\{a_{\sigma,\tau}\}$ is the **factor set of A relative to L.**

Here are some facts which we state without proof to explain various aspects of the previous definition. Let $G = \mathrm{Gal}(L/K)$.

1. (Lemma 6 [12]) The elements x_σ (for $\sigma \in G$) give a basis of A over L, that is,

$$A = \bigoplus_{\sigma \in G} L x_\sigma$$

2. The elements $a_{\sigma,\tau}$ lie in $L^\times$, so they may be viewed as functions

$$G \times G \to L^\times \qquad (\sigma, \tau) \mapsto a_{\sigma,\tau}$$

3. The products $x_\sigma x_\tau$ for $\sigma, \tau \in G$ determine all the multiplication in A, and

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$$

   hence the collection $\{a_{\sigma,\tau}\}$ captures all information about multiplication in A.

4. The functions $a_{\sigma,\tau}$ are in fact 2-cocycles (elements of $Z^2(G, L^\times)$), since they satisfy the relations

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau}$$

   for $\rho, \sigma, \tau \in G$.

5. If we replace the central simple algebra A with another Brauer-equivalent central simple algebra A' (that is, $[A] = [A']$), and repeat the construction to obtain a factor set $\left\{a'_{\sigma,\tau}\right\}$ for A', then there are elements $b_\sigma \in L^\times$ such that

$$a'_{\sigma,\tau} = \left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right) a_{\sigma,\tau}$$

Since $\left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right)$ is a 2-coboundary, this says that

$$[a'_{\sigma,\tau}] = [a_{\sigma,\tau}] \qquad \text{in } H^2(G, L^\times)$$

Thus we have a well-defined map

$$\mathrm{Br}(L/K) \to H^2(G, L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$

For more details behind all of these facts, see pages 13-14 of Rapinchuk [12].

Definition 4.5.2. We give a name to the map defined/constructed above.

$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(\mathrm{Gal}(L/K), L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$

Eventually, we want to show that $\beta_{L/K}$ is an isomorphism.

Lemma 4.5.3. *$\beta_{L/K}$ is injective.*

Proof. Lemma 7 of Rapinchuk [12]. □

4.5.2 Algebra (crossed product) associated to a 2-cocycle (factor set)

To show that $\beta_{L/K}$ is surjective, we construct an algebra from a cocycle/factor set $\{a_{\sigma,\tau}\}$. That is, we're going to construct an inverse map

$$H^2(\mathrm{Gal}(L/K), L^\times) \to \mathrm{Br}(L/K)$$

Definition 4.5.4. Let $\{a_{\sigma,\tau}\}$ be a factor set, thought of as an element of $Z^2(G, L^\times)$. Define the L-vector space

$$A = \bigoplus_{\sigma \in G} L x_\sigma$$

Then define multiplication in A by

$$(a_\sigma x_\sigma)(b_\tau x_\tau) = a_\sigma \sigma(b_\tau) a_{\sigma,\tau} x_{\sigma\tau}$$

and extend this by L-linearity. That is,

$$\left(\sum_\sigma a_\sigma x_\sigma\right)\left(\sum_\tau b_\tau x_\tau\right) = \sum_{\sigma,\tau} a_\sigma \sigma(b_\tau) a_{\sigma,\tau} x_{\sigma\tau}$$

We then view A as a K-algebra. The algebra A is called the **crossed product of L and G relative to the factor set** $\{a_{\sigma,\tau}\}$, and is denoted $(L, G, \{a_{\sigma,\tau}\})$.

Lemma 4.5.5 (Surjectivity of $\beta_{L/K}$)**.** *Let L/K be a finite Galois extension and $G = \mathrm{Gal}(L/K)$, $n = [L:K] = |G|$. Let $\{a_{\sigma,\tau}\}$ be a factor set. The K-algebra $A = (L, G, \{a_{\sigma,\tau}\})$ is an associative, unital [1], central simple K-algebra containing (an isomorphic copy of) L, and with $\dim_K A = n^2$, and*

$$\beta_{L/K}[A] = [\{a_{\sigma,\tau}\}]$$

Hence $\beta_{L/K}$ is surjective.

[1] In particular, $a_{1,1}^{-1} x_1$ is the identity

Proof. Lemma 8 of Rapinchuk [12]. Note that because $(L, G, \{a_{\sigma,\tau}\})$ contains a copy of L and has dimension n^2, we know from Theorem 4.4.3 that it represents a class in $\mathrm{Br}(L/K)$. □

Theorem 4.5.6 (Brauer group isomorphism in finite case)**.** *Let L/K be a finite Galois extension. The map*

$$\beta_{L/K} : \mathrm{Br}(L/K) \to H^2(\mathrm{Gal}(L/K), L^\times) \qquad [A] \mapsto [\{a_{\sigma,\tau}\}]$$

is a group isomorphism.

Proof. By Lemmas 4.5.3, 4.5.5 it suffices to show that $\beta_{L/K}$ is a group homomorphism. Details in Theorem 7 of Rapinchuk [12]. □

This concludes our construction and discussion of the isomorphism

$$\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times)$$

in the case where L/K is finite. All we need to do now is extend this result to the infinite case. This is not so hard, compared to the work needed in the finite case.

4.5.3 Extension to infinite extensions, main isomorphism

Remark 4.5.7. Let L/K be an infinite Galois extension and let $\mathcal{E}$ be the set of intermediate finite Galois extensions $K \subset E \subset L$. If $E_1, E_2 \in \mathcal{E}$ with $E_1 \subset E_2$, then there is a restriction map

$$\mathrm{Gal}(E_2/K) \to \mathrm{Gal}(E_1/K) \qquad \sigma \mapsto \sigma|_{E_1}$$

[2] which induces the inflation map on cohomology

$$\theta_2^1 : H^2(\mathrm{Gal}(E_1/K), E_1^\times) \to H^2(\mathrm{Gal}(E_2/K), E_2^\times) \qquad [\{a_{\sigma,\tau}\}] \mapsto [\{a_{\sigma|_{E_1},\tau|_{E_1}}\}]$$

which makes the groups $H^2(\mathrm{Gal}(E/K), E^\times)$ into a directed system. Furthermore, from the theory of profinite cohomology (Proposition 3.12.6), the direct limit is

$$H^2(\mathrm{Gal}(L/K), L^\times) = \varinjlim_{E \in \mathcal{E}} H^2(\mathrm{Gal}(E/K), E^\times)$$

Remark 4.5.8. Let $L, K, \mathcal{E}$ be as above, with $E_1, E_2 \in \mathcal{E}$ and $E_1 \subset E_2$. There is an inclusion map

$$\iota_2^1 : \mathrm{Br}(E_1/K) \to \mathrm{Br}(E_2/K) \qquad [A] \mapsto [A]$$

so the groups $\mathrm{Br}(E/K)$ form a direct system, with direct limit

$$\mathrm{Br}(L/K) = \bigcup_{E \in \mathcal{E}} \mathrm{Br}(E/K) = \varinjlim_{E \in \mathcal{E}} \mathrm{Br}(E/K)$$

[2] This makes the groups $\mathrm{Gal}(E/K)$ into an inversely directed system and $\mathrm{Gal}(L/K) \cong \varprojlim_{E \in \mathcal{E}} \mathrm{Gal}(E/K)$, see Proposition 2.3.1.

So both $\mathrm{Br}(L/K)$ and $H^2(\mathrm{Gal}(L/K), L^\times)$ are direct limits of directed systems, which are both indexed by intermediate finite Galois extensions E/K. Furthermore, for each pair $\mathrm{Br}(E/K)$ and $H^2(\mathrm{Gal}(E/K), E^\times)$, we have an isomorphism

$$\beta_{E/K} : \mathrm{Br}(E/K) \to H^2(\mathrm{Gal}(E/K), E^\times)$$

Nevertheless, this is not enough to immediately conclude that the direct limits $\mathrm{Br}(L/K)$ and $H^2(\mathrm{Gal}(L/K), L^\times)$ are isomorphic. What we need is an isomorphism of directed systems, which is exactly what the next proposition accomplishes.

Proposition 4.5.9 (Isomorphism of directed systems for Brauer group)**.** *Let L/K be an infinite Galois extension and let $\mathcal{E}$ be the set of intermediate finite Galois extension $K \subset E \subset L$. The isomorphism $\beta_{E/K}$ give an isomorphism of directed systems $\left(H^2(\mathrm{Gal}(E/K), E^\times), \theta^i_j\right) \cong \left(\mathrm{Br}(E/K), \iota^i_j\right)$. That is, for all $E_1, E_2 \in \mathcal{E}, E_1 \subset E_2$, the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Br}(E_1/K) & \xrightarrow{\quad\iota^1_2\quad} & \mathrm{Br}(E_2/K) \\ \downarrow{\scriptstyle \beta_{E_1/K}} & & \downarrow{\scriptstyle \beta_{E_2/K}} \\ H^2(\mathrm{Gal}(E_1/K), E_1^\times) & \xrightarrow{\theta^1_2} & H^2(\mathrm{Gal}(E_2/K), E_2^\times) \end{array}$$

Thus the direct limit of maps $\beta_{E/K}$ gives an isomorphism on the direct limits.

$$\mathrm{Br}(L/K) \xrightarrow[\cong]{\beta_{L/K} = \varinjlim \beta_{E/K}} H^2(\mathrm{Gal}(L/K), L^\times)$$

In particular, since $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{sep}}/K)$ *(Corollary 4.4.6),*

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$$

Proof. Proposition 6 and Theorem 8 of Rapinchuk [12]. □

Remark 4.5.10. One immediate corollary of this is that $\mathrm{Br}(K)$ is a torsion group. From the $\mathrm{Cor} \circ \mathrm{Res}$ composition (Proposition 3.9.17), we know that $H^2(\mathrm{Gal}(E/K), E^\times)$ is torsion for E/K finite Galois, and the direct limit of torsion groups is torsion, so $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), K^{\mathrm{sep}\,\times})$ is torsion, so $\mathrm{Br}(K)$ is torsion.

This is not at all obvious from the description in terms of algebras, since it says that for any central simple algebra A, the tensor product $A \otimes A \otimes \cdots \otimes A$ is eventually isomorphic to a matrix algebra $M_n(K)$ if we tensor enough times.

The isomorphism $\mathrm{Br}(K) \cong H^2(G_K, (K^{\mathrm{sep}})^\times)$ also has some relation to cup products, via the next result. This result really belongs in a discussion of the Merkurjev-Suslin theorem, so we include it there later (see Proposition 5.8.16), but it has some interest at this stage as well.

Definition 4.5.11. Let L/K be a cyclic Galois extension of order m, and fix an isomorphism $\chi : \mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$. Let $b \in K^\times$, and let $\sigma = \chi^{-1}(1)$. The **cyclic algebra** (χ, b) is the algebra with the following presentation. It is generated as an L-algebra by L and an element y, satisfying

$$y^m = b \qquad \sigma(\lambda) = y^{-1}\lambda y, \ \ \forall \lambda \in L$$

Proposition 4.5.12. *Let K be a field, let $m \in \mathbb{Z}_{>0}$, fix a separable closure K^{sep}, and let $G_K = \text{Gal}(K^{\text{sep}}/K)$. Let L/K be a cyclic Galois extension of degree m contained in K^{sep}, and fix an isomorphism*

$$\chi : \text{Gal}(L/K) \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

Then define

$$\widetilde{\chi} : G_K \to \mathbb{Z}/m\mathbb{Z} \qquad \sigma \mapsto \chi(\sigma|_L)$$

so that $\widetilde{\chi} \in H^1(G_K, \mathbb{Z}/m\mathbb{Z})$. Let $\delta : H^1(G_K, \mathbb{Z}/m\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$ be the coboundary map of the LES associated to

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

[3] *Then consider the cup product map*

$$H^2(G_K, \mathbb{Z}) \times H^0(G_K, (K^{\text{sep}})^\times) \xrightarrow{\cup} H^2(G_K, (K^{\text{sep}})^\times)$$

Under the isomorphism

$$H^2(G_K, (K^{\text{sep}})^\times) \cong Br(K)$$

the element $\delta(\widetilde{\chi}) \cup b$ corresponds to the Brauer class of the cyclic algebra (χ, b).

Proof. Proposition 4.7.3 of Gille & Szamuely [4]. □

4.5.4 Restriction maps

For a finite Galois extension L/K, we can give a cohomological interpretation of the map

$$\text{Br}(K) \to \text{Br}(L) \qquad [A] \mapsto [A \otimes_K L]$$

In particular it is "the same" as the Res map on cohomology. This statement is made more precise by the next proposition.

Proposition 4.5.13. *Let $K \subset L \subset M$ be a tower of fields with M/K finite Galois. Consider the homomorphism*

$$\epsilon : \text{Br}(M/K) \to \text{Br}(M/L) \qquad [A] \mapsto [A \otimes_K M]$$

Note that $\text{Gal}(M/L)$ is a subgroup of $\text{Gal}(M/K)$, so there is the (profinite) cohomology map

$$\text{Res} : H^2(\text{Gal}(M/K), M^\times) \to H^2(\text{Gal}(M/L), M^\times)$$

Then the following diagram commutes.

$$\begin{array}{ccc} \text{Br}(M/K) & \xrightarrow{\quad\epsilon\quad} & \text{Br}(M/L) \\ \cong\downarrow\beta_{M/K} & & \cong\downarrow\beta_{M/L} \\ H^2(\text{Gal}(M/K), M^\times) & \xrightarrow{\text{Res}} & H^2(\text{Gal}(M/L), M^\times) \end{array}$$

[3] Note that we are viewing $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ as trivial G_K-modules, and by Proposition 3.2.7 $H^1(G_K, \mathbb{Z}/m\mathbb{Z}) = \text{Hom}_{\mathbb{Z}}(G_K, \mathbb{Z}/m\mathbb{Z})$, so $\widetilde{\chi} \in H^1(G_K, \mathbb{Z}/m\mathbb{Z})$.

In particular, in the case $M = K^{\text{sep}}$, we note that $L^{\text{sep}} = K^{\text{sep}}, \text{Br}(K) = \text{Br}(K^{\text{sep}}/K), \text{Br}(L) = \text{Br}(L^{\text{sep}}/L)$, so the above commutative square becomes

$$\begin{array}{ccc} \text{Br}(K) & \xrightarrow{[A]\mapsto[A\otimes_K L]} & \text{Br}(L) \\ \downarrow\cong & & \downarrow\cong \\ H^2(\text{Gal}(K^{\text{sep}}/K), (K^{\text{sep}})^\times) & \xrightarrow{\text{Res}} & H^2(\text{Gal}(L^{\text{sep}})/L), (L^{\text{sep}})^\times) \end{array}$$

Proof. Proposition 7 of Rapinchuk [12]. □

4.6 Brauer group computations

By now, we have many powerful tools available for computing Brauer groups. We have the Skolem-Noether theorem, Wedderburn's theorem, results about maximal subfields and relative Brauer groups, and most importantly an identification of $\text{Br}(K)$ with a profinite cohomology group.

We start with algebraically closed fields, which are very simple - they have trivial Brauer group. Then we tackle a general case of a relative Brauer group $\text{Br}(L/K)$ in the case where $\text{Gal}(L/K)$ is cyclic, which gives a very computationally useful tool at the end. This allows us to calculate $\text{Br}(\mathbb{R})$ and $\text{Br}(\mathbb{F}_q)$. Finally, we use this tool to calculate the Brauer group of a local field, such as $\mathbb{Q}_p$.

4.6.1 Algebraically closed fields

Proposition 4.6.1. *Let K be an algebraically closed field.*

1. *The only finite dimensional division algebra over K is K itself.*
2. *If A is a finite dimensional simple K-algebra, then $A \cong M_n(K)$ for some n.*
3. *$\text{Br}(K)$ is trivial.*

Proof. (1) Let D be a finite dimensional division algebra over K, and suppose $D \neq K$. Then there exists $\alpha \in D \setminus K$, and then $K(\alpha)/K$ is a finite algebraic extension, which is impossible since K is algebraically closed. Hence $D = K$.

(2) By Wedderburn's theorem, $A \cong M_n(D)$ for some division algebra over K, but then $D = K$ by (1).

(3) $M_n(K)$ represents the identity element of $\text{Br}(K)$, so (2) says that everything in the Brauer group is equivalent to the identity. □

4.6.2 Cyclic algebras - relative Brauer group of cyclic Galois extension

Let L/K be a finite Galois extension with cyclic Galois group, and let N_K^L be the norm map. The goal of this section is to describe an isomorphism

$$\text{Br}(L/K) \cong K^\times / \text{N}_K^L(L^\times)$$

This is useful for computing various absolute Brauer groups. For example, an immediate application is $\mathrm{Br}(\mathbb{R})$, since the separable closure $\mathbb{C}/\mathbb{R}$ is a finite cyclic extension. This can also be utilized to compute the Brauer group of a finite field, or of a local field.

Remark 4.6.2. Using group cohomology, it is easy to see that for L/K finite cyclic Galois

$$\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times) \cong K^\times / \mathrm{N}_K^L(L^\times)$$

We will ignore this for the moment, and attempt to describe this using purely the language of algebras.

Definition 4.6.3. Let L/K be a finite cyclic Galois extension. Let $[A] \in \mathrm{Br}(L/K)$, and choose a representative central simple algebra A with $\dim_K A = n^2$ so that $L \subset A$ (this exists by Theorem 4.4.3). Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Using the Skolem-Noether theorem 4.2.1, choose $x_\sigma \in A^\times$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \qquad \forall a \in L$$

Set $x_{\sigma^i} = (x_\sigma)^{i \bmod n}$, and note that $x_{\sigma^i} a x_{\sigma^i}^{-1} = \sigma^i(a)$ for all $a \in L$ and all i, so as in Definition 4.5.1, the x_{σ^i} for $i = 0, \ldots, n-1$ give an L-basis of A and we obtain a factor set a_{σ^i,σ^j} associated to A. Now set $\alpha = (x_\sigma)^n$, and note that $\alpha \in K^\times$ [4], and that

$$x_{\sigma^i} x_{\sigma^j} = \begin{cases} x_{\sigma^{i+j}} & i+j < n \\ \alpha x_{\sigma^{i+j-n}} & i+j \geq n \end{cases}$$

Thus multiplication for the algebra A is determined by α, and we denote this algebra by $\boldsymbol{(L, \sigma, \alpha)}$ and call it a **cyclic algebra**.

Remark 4.6.4. Since $[A]$ was arbitrary in the previous definition, the discussion shows that every element of $\mathrm{Br}(L/K)$ is of the form $[(L, \sigma, \alpha)]$ for some $\alpha \in K^\times$. We can describe the factor set associated to (L, σ, α) as

$$a_{\sigma^i,\sigma^j} = x_{\sigma^i} x_{\sigma^j} x_{\sigma^{i+j}}^{-1} = (x_\sigma)^{i+j} (x_\sigma)^{-(i+j) \bmod n} = \begin{cases} 1 & i+j < n \\ \alpha & i+j \geq n \end{cases}$$

We denote this factor set by $\left\{a_{\sigma^i,\sigma^j}(\alpha)\right\}$. So under the isomorphism $\mathrm{Br}(L/K) \cong H^2(\mathrm{Gal}(L/K), L^\times)$, the classes $[(L, \sigma, \alpha)]$ and $[a_{\sigma^i,\sigma^j}(\alpha)]$ are mapped to each other.

Definition 4.6.5. The assignment

$$\mathrm{Br}(L/K) \to K^\times \qquad [(L, \sigma, \alpha)] \mapsto \alpha$$

is not quite well defined, because α depends on the choice of x_σ. However, a different choice x'_σ satisfying $x'_\sigma a (x'_\sigma)^{-1}$ for all $a \in L$ must be of the form $x'_\sigma = x_\sigma t$ for some $t \in L^\times$, and then if $\alpha' = (x'_\sigma)^n$ we get

$$\begin{aligned} \alpha' = (x'_\sigma)^n = (x_\sigma t)^n = x_\sigma t x_\sigma t \cdots x_\sigma t = \sigma(t) x_\sigma x_\sigma t \cdots x_\sigma t \\ = \cdots = \sigma(t)\sigma^2(t) \cdots \sigma^n(t)(x_\sigma)^n = N_K^L(t)\alpha \end{aligned}$$

[4] $(x_\sigma)^n a (x_\sigma)^{-n} = \sigma^n(a) = a$ implies that $\alpha \in Z_A(L) = L$ (using Corollary 4 of Rapinchuk [12], and then $\sigma(\alpha) = x_\sigma \alpha x_\sigma^{-1} = x_\sigma x_\sigma^n x_\sigma^{-1} = (x_\sigma)^n = \alpha$ so α is fixed by $\mathrm{Gal}(L/K)$, hence $\alpha \in K$. It cannot be zero because x_σ is a unit, so $\alpha \in K^\times$.

Thus if instead of mapping to $K^\times$, we map to $K^\times/N_K^L(L^\times)K^\times$, we have a well-defined assignment, and we have a map

$$\gamma_{L/K} : \mathrm{Br}(L/K) \to K^\times/N_K^L(L^\times) \qquad [(L,\sigma,\alpha)] \mapsto \alpha N_K^L(L^\times)$$

This map turns out to be an isomorphism.

Theorem 4.6.6. *Let L/K be a finite cyclic Galois extension and let σ be a generator of* $\mathrm{Gal}(L/K)$. *Then there is an isomorphism of groups*

$$\gamma_{L/K} : \mathrm{Br}(L/K) \to K^\times/N_K^L(L^\times) \qquad [(L,\sigma,\alpha)] \mapsto \alpha N_K^L(L^\times)$$

Proof. First we show it is a homomorphism. Let $[(L,\sigma,\alpha)], [(L,\sigma,\beta)] \in \mathrm{Br}(L/K)$ with $\alpha,\beta \in K^\times$. Using the isomorphism with H^2, let $a_{\sigma^i,\sigma^j}(\alpha), a_{\sigma^i,\sigma^j}(\beta)$ be the associated factor sets. Then

$$a_{\sigma^i,\sigma^j}(\alpha)a_{\sigma^i,\sigma^j}(\beta) = a_{\sigma^i,\sigma^j}(\alpha\beta)$$

hence

$$[(L,\sigma,\alpha)] \cdot [(L,\sigma,\beta)] = [(L,\sigma,\alpha\beta)]$$

Thus applying $\gamma_{L/K}$ we get

$$\begin{aligned}
\gamma_{L/K}\Big([(L,\sigma,\alpha)] \cdot [(L,\sigma,\beta)]\Big) &= \gamma_{L/K}[(L,\sigma,\alpha\beta)] \\
&= (\alpha\beta)N_K^L(L^\times) \\
&= \big(\alpha N_K^L(L^\times)\big) \cdot \big(\beta N_K^L(L^\times)\big) \\
&= \big(\gamma_{L/K}[(L,\sigma,\alpha)]\big) \cdot \big(\gamma_{L/K}[(L,\sigma,\beta)]\big)
\end{aligned}$$

Hence $\gamma_{L/K}$ is a group homomorphism. For injectivity, if $\alpha \equiv \alpha' \bmod N_K^L(L^\times)$ and more precisely, $\alpha' = \alpha N_K^L(t)$ for $t \in L^\times$, then the correspondence

$$(x'_\sigma)^i \mapsto (x_\sigma t)^i \qquad i = 0,\dots,n-1$$

extends to an isomorphism of algebras $(L,\sigma,\alpha) \cong (L,\sigma,\alpha')$. Surjectivity of $\gamma_{L/K}$ follows from the fact that $\{a_{\sigma^i,\sigma^j}(\alpha)\}$ is a cocycle for any $\alpha \in K^\times$. Thus $\gamma_{L/K}$ is an isomorphism. □

We don't need the next lemma at the moment, but we will use it later for computing the Brauer group of a local field, so we record it now. It addresses how cyclic algebras behave in towers.

Lemma 4.6.7. *Let $K \subset E \subset F$ be a tower of fields with F/K finite cyclic Galois, and let let $\widehat{\sigma}$ be a generator of* $\mathrm{Gal}(F/K)$. *Let $n = [F:K], m = [F:E]$, and let $\sigma = \widehat{\sigma}|_E \in \mathrm{Gal}(E/K)$.*

$$\begin{array}{c} F \\ \Big|{\scriptstyle n} \\ E \\ \Big|{\scriptstyle m} \\ K \end{array}$$

Then

$$[(E,\sigma,\alpha)] = [(F,\widehat{\sigma},\alpha^{n/m})] \in \mathrm{Br}(F/K)$$

Proof. Lemma 10 of Rapinchuk [12]. □

4.6.3 Real numbers

First we compute $\mathrm{Br}(\mathbb{R})$ using our knowledge of relative Brauer groups of cyclic extensions, since $\mathbb{C}/\mathbb{R}$ is the separable closure, and is a cyclic extension. Then, we re-derive the same result using just some results about algebras, primarily the Skolem-Noether theorem and existence of maximal subfields.

Proposition 4.6.8. $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. The Brauer group is the same as the relative Brauer group of the separable closure, which in this case is the algebraic closure, $\mathbb{C}/\mathbb{R}$. By Theorem 4.6.6,

$$\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}/\mathbb{R}) \cong \mathbb{R}^\times / N_{\mathbb{R}}^{\mathbb{C}}(\mathbb{C}^\times)$$

The image of the norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ is $\mathbb{R}_{>0}$, so

$$\mathrm{Br}(\mathbb{R}) \cong N_{\mathbb{R}}^{\mathbb{C}}(\mathbb{C}^\times) \cong \mathbb{R}^\times/\mathbb{R}_{>0} \cong \{\pm 1\}$$

□

Remark 4.6.9. In the language of division algebras, the previous computation says that there is exactly one (up to isomorphism) noncommutative central division algebra over $\mathbb{R}$. Recall that the Hamilton quaternions may be described as the $\mathbb{R}$-algebra with basis $1, i, j, ij$ satisfying $i^2 = j^2 = -1$ and $ij = -ji$.

$$\mathbb{H} = \langle 1, i, j : i^2 = j^2 = -1, ij = -ji \rangle$$

Since the Hamilton quaternions $\mathbb{H}$ are a central division $\mathbb{R}$-algebra (proof omitted), they are the unique finite dimensional central division algebra over $\mathbb{R}$.

As an exercise, we can also show directly (not using the previous result) that the Hamilton quaternions are the only nontrivial finite dimensional central division algebra over $\mathbb{R}$.

Proposition 4.6.10. *The only nontrivial finite dimensional central division algebra over* $\mathbb{R}$ *is the Hamilton quaternions.*

Proof. Let D be a nontrivial finite dimensional central division algebra over $\mathbb{R}$. By Proposition 4.1.13, $\dim_{\mathbb{R}} D = d^2$ is a perfect square, and by Proposition 4.4.4, D has a maximal subfield P so that $P/\mathbb{R}$ is separable, and $\dim_{\mathbb{R}} P = d$. Since the only nontrivial extension of $\mathbb{R}$ is $\mathbb{C}$, $P = \mathbb{C} = \mathbb{R}(i)$ and $d = 2$, so $\dim_{\mathbb{R}} D = 4$. Now consider the two homomorphisms

$$\begin{aligned} f &: \mathbb{C} \to D \qquad z \mapsto z \\ g &: \mathbb{C} \to D \qquad z \mapsto \overline{z} \end{aligned}$$

where $\overline{z}$ denotes the complex conjugate. By the Skolem-Noether theorem 4.2.1, there exists $j \in D^\times$ so that

$$\overline{z} = jzj^{-1} \qquad \forall z \in \mathbb{C}$$

In particular, $jij^{-1} = -i$. Note that since j does not commute with i, j does not lie in $\mathbb{C}$.

We claim $j^2 \in \mathbb{R}$. Note that since D is central, j (hence j^2) commutes with $\mathbb{R}$. Since $j^2 i j^{-2} = i$, j^2 commutes with $\mathbb{C}$. Since j^2 is a unit, $\mathbb{C}(j^2)$ is a field, but since $\mathbb{C}$ is a maximal subfield of D, $\mathbb{C}(j^2) = \mathbb{C}$, hence $j^2 \in \mathbb{C}$. Since j^2 commutes with j, $jj^2j^{-1} = j^2$. Since $j^2 \in \mathbb{C}$ and conjugation by j is complex conjugation, $jj^2j^{-1} = \overline{j^2}$, hence $j^2 = \overline{j^2}$, so $j^2 \in \mathbb{R}$.

Now we claim $j^2 < 0$. Since $j \notin \mathbb{R}$, its minimal polynomial over $\mathbb{R}$ is $t^2 - j^2$. But if $j^2 > 0$, this would be reducible into $(t-j)(t+j)$, which is a contradiction, so we must have $j^2 < 0$. Replacing j by $\frac{j}{\sqrt{|j^2|}}$, we may assume $j^2 = -1$. We claim that $1, i, j, ij$ are linearly independent over $\mathbb{R}$. Suppose there are $a, b, c, d \in \mathbb{R}$ so that

$$a + bi + cj + dij = 0$$

Then if $c + di \neq 0$, we get

$$(a+bi) + (c+di)j = 0 \implies j = \frac{a+bi}{c+di} \implies j \in \mathbb{C}$$

which is impossible since we know $j \notin \mathbb{C}$, so $c = d = 0$. Then $a + bi = 0 \implies a = b = 0$, hence $1, i, j, ij$ are linearly independent. Thus D is four dimensional $\mathbb{R}$-algebra with basis $1, i, j, ij$ satisfying relations $i^2 = j^2 = -1$ and $ij = -ij$, so $D \cong \mathbb{H}$. □

4.6.4 Finite fields - via field norm

Next we address absolute and relative Brauer groups of finite fields. The arguments are interesting and illustrate the many tools we have, even though the eventual results are somewhat uninteresting (all the groups are trivial). We will prove the following:

Proposition 4.6.11. *Let $K = \mathbb{F}_q$ be the unique (up to isomorphism) finite field of order q. Then $\mathrm{Br}(K) = 0$.*

First, we give a proof which uses the description of $\mathrm{Br}(K)$ as $H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), (K^{\mathrm{sep}})^\times)$, and properties of the field norm map.

Proof. Let q be a prime power, and let $\mathbb{F}_q$ be the field with q elements. By Proposition 3.12.6, we just need to show that H^2 is trivial for the finite Galois subextensions. The finite Galois extensions of $\mathbb{F}_q$ are $\mathbb{F}_{q^n}$ for $n \geq 1$, with cyclic Galois groups. Let

$$G_n = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$$

Then we have

$$\mathrm{Br}(\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_q^{\mathrm{sep}}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = \varinjlim H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = \varinjlim H^2(G_n, \mathbb{F}_{q^n}^\times)$$

Let $N = N_{G_n}$ be the norm element, and recall that multiplication by the norm element of G_n is the same as the field norm map

$$N_G = \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}^\times \to \mathbb{F}_q^\times$$

We know that the Tate cohomology is 2-periodic for finite cyclic groups. Using this and the fact that the fixed field of G_n is exactly $\mathbb{F}_q$, we get

$$H^2(G_n, \mathbb{F}_{q^n}^\times) \cong \widehat{H}^0(G_n, \mathbb{F}_{q^n}^\times) \cong \left(\mathbb{F}_{q^n}^\times\right)^{G_n} / N_G \mathbb{F}_{q^n}^\times = \mathbb{F}_q^\times / \operatorname{im} \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}$$

Thus, we have reduced the problem to showing that the norm map is surjective for finite fields, which is given in a lemma below. □

Remark 4.6.12. As a quicker proof than the above to accomplish the same reduction, we know that

$$\mathrm{Br}(\mathbb{F}_q) = \bigcup_{n \geq 1} \mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q)$$

and each extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic, and by Theorem 4.6.6, the relative Brauer group is

$$\mathrm{Br}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{F}_q / \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\mathbb{F}_{q^n}^\times)$$

Hence if the norm map for finite fields is surjective, all of the relative Brauer groups vanish, and hence the absolute Brauer group vanishes.

Lemma 4.6.13. *The norm map for finite fields is surjective.*

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}^\times \twoheadrightarrow \mathbb{F}_q^\times$$

Proof. Recall that $\mathbb{F}_q^\times$ consists of qth roots of unity. Similarly, $\mathbb{F}_{q^n}$ consists of $(q^n - 1)$th roots of unity. Recall that the Galois group $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated by the Frobenius automorphism

$$\phi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \qquad x \mapsto x^q$$

Let $\alpha \in \mathbb{F}_{q^n}^\times$ be a primitive $(q^n - 1)$th root of unity, that is, a generator of $\mathbb{F}_{q^n}^\times$. The norm is the product of the Galois conjugates, so

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{i=0}^{n-1} \phi^i(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{1+q+q^2+\cdots+q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$$

The last equality comes from the formula for the sum of a finite geometric series. Then observe that

$$\left(\alpha^{\frac{q^n-1}{q-1}}\right)^{q-1} = \alpha^{q^n-1} = 1$$

by definition of α. That is, the image of α under the norm map is a primitive $(q-1)$th root of unity, so it is a generator of $\mathbb{F}_q^\times$. Thus the norm map is surjective. □

4.6.5 Finite fields - via division algebras

For a second approach, we use the characterization of $\mathrm{Br}(K)$ in terms of division algebras. We show that any finite dimensional division algebra over a finite field is commutative, so it is a field (this is a classical result of Wedderburn). Since the elements of $\mathrm{Br}(K)$ correspond to noncommutative central division algebras over K, this will show that $\mathrm{Br}(K) = 0$. First, we need a purely group-theoretic lemma.

Lemma 4.6.14 (Finite group not equal to conjugates of proper subgroup)**.** *Let G be a finite group and $H \subset G$ a proper subgroup. The union of all conjugates of H is not equal to G. That is,*

$$\bigcup_{g \in G} gHg^{-1}$$

is a proper subset of G.

Proof. Let $K_H = \{gHg \in : g \in G\}$ be the set of conjugate subgroups to H. Then G acts on K_H by conjugation. The stabilizer of this action is exactly the normalizer of H in G, which we denote $N_G(H)$. Note that $H \subset N_G(H)$, thus

$$[G : N_G(H)] \leq [G : H]$$

By the orbit-stabilizer theorem,

$$|K_H| = [G : N_G(H)]$$

Each conjugate subgroup of H has the same order as H, and also contains the identity, so the maximum number of non-overlapping elements in each subgroup is $|H| - 1$, and there are $|K_H|$ such conjugate subgroups. Thus

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq \Big(|H| - 1\Big)|K_H| + 1$$

Now we do some trivial manipulations to this using facts established above.

$$\begin{aligned} \Big(|H| - 1\Big)|K_H| + 1 &= \Big(|H| - 1\Big)[G : N_G(H)] + 1 \\ &\leq \Big(|H| - 1\Big)[G : H] + 1 \\ &= |H|[G : H] - [G : H] + 1 \\ &= |G| - [G : H] + 1 \end{aligned}$$

Since H is a proper subgroup, $[G : H] \geq 2$, thus, the expression above is at most $|G| - 1$. Thus the union of all conjugates of G has size strictly less than G, so it is not the whole group. □

Proposition 4.6.15 (Every finite division algebra is a field)**.** *Let D be a finite dimensional central division algebra over a finite field. Then D is commutative, hence a field.*

Proof. Suppose D is a noncommutative finite central division algebra over a finite field F. Let $\dim_F D = n^2$ (Proposition 4.1.13). If $n = 1$ then $D = F$ and we are done, so assume $n > 1$. By Proposition 4.4.4, there is a maximal intermediate subfield $F \subset P \subset D$ with $\dim_F P = n$. Since F has a unique (up to isomorphism) extension of degree n, all maximal subfields of D are isomorphic.

By the Skolem-Noether theorem 4.2.1, any two maximal subfields of D are conjugate. More precisely, if P, P' two maximal subfields with embeddings $\iota : P \hookrightarrow D, \iota' : P \hookrightarrow D$,

and we fix an isomorphism $\phi : P \xrightarrow{\cong} P'$ (isomorphism as K-algebras), then by the Skolem-Noether theorem applied to the homomorphisms ι and $\iota' \circ \phi$, there exists $d \in D$ such that for all $x \in P$,

$$\iota' \circ \phi(x) = d\big(\iota(x)\big)d^{-1}$$

Since ι, ι' are inclusions, we can write this instead as

$$\phi(x) = dxd^{-1}$$

That is to say,

$$P \to P' \qquad x \mapsto dxd^{-1}$$

is an isomorphism, which is what we mean when we say that P, P' are conjugate in D. Thus if P is any one maximal subfield, then all other maximal subfields arise as conjugates dPd^{-1}. Now, every element of D is contained in some maximal subfield, so we obtain

$$D^\times = \bigcup_{\substack{P \text{ maximal} \\ \text{subfield}}} P^\times = \bigcup_{d \in D^\times} dP^\times d^{-1}$$

Since $D^\times$ is a finite group and $P^\times \subset D^\times$ is a proper subgroup, by our group theory lemma 4.6.14, this is a contradiction, so no such D exists. □

Corollary 4.6.16. *Let F be a finite field. Then* $\mathrm{Br}(F) = 0$.

Proof. Nonzero elements of $\mathrm{Br}(F)$ correspond to equivalence classes of (noncommutative) finite dimensional central division algebras, but by Proposition 4.6.15, there are no such division algebras. □

4.6.6 Finite fields - via C_1-fields

Lastly, we give an overly high-powered method to show that the Brauer group of a finite field is trivial, using the notion of C_1-fields. I know very little about this, but chapter 6 of Gille & Szamuely is a good source.

Definition 4.6.17. A field K is a **C_1-field** if every homogeneous polynomial $f \in K[x_1, \ldots, x_n]$ of degree $d < n$ has a nontrivial zero in K^n.

Lemma 4.6.18. *Let K be a C_1-field, and L/K a finite extension. Then L is a C_1-field.*

Proof. Gille and Szamuely 6.2.4 [4]. □

Proposition 4.6.19. *Let K be a C_1-field, and L/K a finite extension. Then* $\mathrm{Br}(L) = 0$.

Proof. Gille and Szamuely 6.2.3 [4]. □

Theorem 4.6.20 (Chevalley-Warning)**.** *Finite fields are C_1-fields.*

Proof. Gille and Szamuely 6.2.6 [4]. □

Of course, an immediate corolary of all of this is that the Brauer group of a finite field is trivial.

4.6.7 Relative Brauer group of maximal unramified extension of a local field

The next section requires some background on local fields and their unramified extensions. By "local field," I mean complete nonarchimedean discretely valued field, such as $\mathbb{Q}_p$. For the reader who hasn't seen this material, see Chapter 6 for an introduction, or chapter 7 of Milne [8], which is where I learned this from.

The main result is that there is a Galois-type correspondence between finite unramified extensions of a local field K and finite extensions of the residue field k, see Proposition 6.4.1. In particular, since local fields (as we use the term) have a finite residue field, there is a unique unramified extension K_n/K of degree n. As long as you're familiar with that result, you probably have enough knowledge of local fields for this section.

Assuming the prerequisites are out of the way, our next goal is to use Theorem 4.6.6 and Lemma 4.6.7 to compute the relative Brauer group of finite unramified extensions, and then put these together to compute the relative Brauer group of the maximal unramified extension.

Definition 4.6.21. We use the notation $\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$ to mean $\mathbb{Z}/n\mathbb{Z}$ generated additively by $\frac{1}{n}$.

$$\frac{1}{n}\mathbb{Z}/\mathbb{Z} = \left\{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n} = 1 = 0\right\}$$

Definition 4.6.22. Let K be a local field with discrete valuation $v : K^\times \to \mathbb{Z}$. Define

$$UK^{\times n} = \left\{\alpha \in K^\times : v(\alpha) \equiv 0 \bmod n\right\}$$

Note that there is an isomorphism

$$UK^{\times n} \xrightarrow{\cong} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \qquad \alpha \mapsto \frac{v(\alpha)}{n} \tag{4.6.1}$$

Proposition 4.6.23 (Relative Brauer group of maximal unramified extension)**.** *Let K be a complete nonarchimedean local field.*

1. *Let K_n/K be the unique unramified extension of degree n. There is an isomorphism*

$$\psi_n : \mathrm{Br}(K_n/K) \xrightarrow{\cong} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \qquad [(K_n, \phi, \alpha)] \mapsto \frac{v(\alpha)}{n} \bmod \mathbb{Z}$$

2. *Let K^{un}/K be the maximal unramified extension. The isomorphisms of (1) give an isomorphism of directed systems, inducing an isomorphism*

$$\mathrm{Br}(K^{\mathrm{un}}/K) = \bigcup_{n\geq 1} \mathrm{Br}(K_n/K) \cong \mathbb{Q}/\mathbb{Z}$$

Proof. As discussed in Example 6.4.3, for each $n \geq 1$, K has a unique unramified extension K_n/K with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z}$, generated by the Frobenius isomorphsim ϕ. Then by Theorem 4.6.6, we have an isomorphism

$$\gamma_{K_n/K} : \mathrm{Br}(K_n/K) \xrightarrow{\cong} K^\times/\,\mathrm{N}_K^{K_n}(K_n^\times) \qquad [(K_n, \phi, \alpha)] \mapsto \alpha\,\mathrm{N}_K^{K_n}(K_n^\times)$$

By Proposition 3c of Chapter V, Section 2 of Serre [14],

$$K^\times / \mathrm{N}_K^{K_n}(K_n^\times) \cong UK^{\times n}$$

so composing this with the isomorphism of 4.6.1, we get an isomorphism

$$\psi_n : \mathrm{Br}(K_n/K) \xrightarrow{\cong} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \qquad [(K_n, \phi, \alpha)] \mapsto \frac{v(\alpha)}{n} \bmod \mathbb{Z}$$

From remark 4.5.8, we know that

$$\mathrm{Br}(K^{\mathrm{un}}/K) = \varinjlim_{n \geq 1} \mathrm{Br}(K_n/K)$$

so next we need to understand the maps of this directed system. The ordering is by divisibility, that is, $m|n \iff K_m \subset K_n$, in which case the Frobenius automorphism ϕ of K_n restricts to the Frobenius automorphism $\phi|_{K_m}$ on K_m. So for $m|n$ we have an embedding $\mathrm{Br}(K_m/K) \hookrightarrow \mathrm{Br}(K_n/K)$, which by Lemma 4.6.7 can be described as

$$j : \mathrm{Br}(K_m/K) \hookrightarrow \mathrm{Br}(K_n/K) \qquad [(K_m, \phi|_{K_m}, \alpha)] \mapsto [(K_n, \phi, \alpha^{n/m})]$$

Thus the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Br}(K_m/K) & \xrightarrow{j} & \mathrm{Br}(K_n/K) \\ \cong\downarrow{\scriptstyle \psi_m} & & \cong\downarrow{\scriptstyle \psi_n} \\ \frac{1}{m}\mathbb{Z}/\mathbb{Z} & \xhookrightarrow[\frac{1}{m}\mapsto\frac{1}{m}]{i} & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \end{array}$$

$$i \circ \psi_m[(K_m, \phi|_{K_m}, \alpha)] = \frac{v(\alpha)}{n}$$

$$\psi_n \circ j[(K_m, \phi|_{K_m}, \alpha^{n/m}] = \psi_n[(K_n, \phi, \alpha^{n/m})] = \frac{v(\alpha^{n/m})}{n} = \frac{\frac{n}{m}v(\alpha)}{n} = \frac{v(\alpha)}{m}$$

That is to say, the maps ψ_n give an isomorphism of directed systems, so $\mathrm{Br}(K^{\mathrm{un}}/K)$ is isomorphic to the direct limit of $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ with respect to inclusion maps, which is $\mathbb{Q}/\mathbb{Z}$. □

4.6.8 (Nonarchimedean, complete) local field

As before, let K be a local field. The next goal is to extend our result about $\mathrm{Br}(K^{\mathrm{un}}/K)$ to a result about $\mathrm{Br}(K) = \mathrm{Br}(K^{\mathrm{sep}}/K)$. The final result will be that $\mathrm{Br}(K^{\mathrm{un}}/K) = \mathrm{Br}(K)$, so $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$, by work from the previous section.

We will do this by studying central division algebras D over K and extending the valuation and an analog of the norm map (called the reduced norm map) to D. We can then talk about ramification degrees and residual degrees for such division algebras, which give us the tools to prove our result.

Definition 4.6.24. Let D be a central division algebra over a field K. A **valuation** on D is a map $w : D^\times \to \mathbb{R}$ satisfying

$$w(ab) = w(a) + w(b)$$
$$w(a+b) \geq \min\big(w(a), w(b)\big) \quad \text{for } a \neq -b$$

(This coincides with the usual definition of a valuation on a ring, just viewing D as a ring.) As in the general setting of rings, a valuation is **discrete** if the image is a discrete subgroup of $(\mathbb{R}, +)$.[5]

Remark 4.6.25. Let K be a nonarchimedean complete local field, and L/K a finite extension with $n = [L : K]$. Recall that by Proposition 6.1.16, the absolute value on K extends uniquely to L via

$$|x|_L = |\,\mathrm{N}_K^L(x)|_K^{1/n} \qquad x \in L^\times$$

In terms of valuations, if $v : K^\times \to \mathbb{R}$ is the valuation corresponding to $|\cdot|_K$ and $\widetilde{v} : L^\times \to \mathbb{R}$ is the valuation corresponding to $|\cdot|_L$, the previous equality translates to

$$\widetilde{v}(x) = \frac{1}{n} v\left(\mathrm{N}_K^L(x)\right) \qquad x \in L^\times$$

Definition 4.6.26. Let K be a field, and D a division algebra over K, with $\dim_K D = n^2$ (Proposition 4.1.13). By Proposition 4.4.4, D contains a maximal subfield P with $\dim_K P = n$, and $D \otimes_K P \cong M_n(P)$ by Theorem 4.4.3. Fix an isomorphism $\phi_P : D \otimes_K P \to M_n(P)$. The **reduced norm map** is

$$\mathrm{Nrd}_K^D : D^\times \to K^\times \qquad \mathrm{Nrd}_K^D(a) = \det\big(\phi_P(a \otimes 1)\big)$$

Proposition 4.6.27. *Let K be a field, and D a division algebra over K. Then*

1. Nrd_K^D *is independent of the choice of P and of ϕ_P.*
2. $\mathrm{Nrd}_K^D : D^\times \to K^\times$ *is a group homomorphism.*
3. *The reduced norm extends the norm map in the following sense: For any maximal subfield $L \subset D$, and for $a \in L^\times$,*

$$\mathrm{Nrd}_K^D(a) = \mathrm{N}_K^L(a)$$

Proof. Proposition 8 of Rapinchuk [12], which refers to Chapter 16 of Pierce [11] for proofs. □

Definition 4.6.28. Let K be a nonarchimedean complete local field with discrete valuation $v : K^\times \to \mathbb{R}$, and D a (finite dimensional) division algebra over K of dimension $\dim_K D = n^2$. The **extended valuation on** D is defined by

$$w : D^\times \to \mathbb{R} \qquad w(a) = \frac{1}{n} v\left(\mathrm{Nrd}_K^D(a)\right)$$

[5] Recall that any discrete subgroup of $(\mathbb{R}, +)$ is infinite cyclic, aka isomorphic to $\mathbb{Z}$.

Proposition 4.6.29. *Let D, K, w, v, n be as above. Let $\Gamma_w = \operatorname{im} w, \Gamma_v = \operatorname{im} v$.*

1. *The extended valuation w is a discrete valuation, which extends v.*
2. *$n\Gamma_w \subset \Gamma_v$.*

Proof. (1) We verify that w extends v. Let $L \subset D$ be a maximal subfield. If $a \in K^\times$, using Proposition 4.6.27, then the fact that $\mathrm{N}_K^L(a) = a^n$ for $a \in K$, we get

$$w(a) = \frac{1}{n} v\left(\mathrm{Nrd}_K^D(a)\right) = \frac{1}{n} v\left(\mathrm{N}_K^L(a)\right) = \frac{1}{n} v\left(a^n\right) = v(a)$$

Thus w extends v. The fact that w is a homomorphism follows immediately from the fact that v and Nrd_K^D are homomorphisms. All that remains is to verify the inequality

$$w(a+b) \geq \min\left(w(a), w(b)\right)$$

for $a \neq -b$. Let $a, b \in D$ with $a \neq -b$, then

$$w(a+b) = w\Big(a(1+a^{-1}b)\Big) = w(a) + w(1+a^{-1}b)$$

Let $L \subset D$ be a maximal subfield containing $a^{-1}b$, with extended valuation $\widetilde{v}(x) = \frac{1}{n} v(\mathrm{N}_K^L(x))$. For $x \in L^\times$, by Proposition 4.6.27,

$$w(x) = \frac{1}{n} v\left(\mathrm{Nrd}_K^D(x)\right) = \frac{1}{n} v\left(\mathrm{N}_K^L(x)\right) = \widetilde{v}(x)$$

Applying this to $1, a^{-1}b, 1 + a^{-1}b \in L^\times$, we get

$$w(1+a^{-1}b) = \widetilde{v}(1+a^{-1}b) \geq \min\left(\widetilde{v}(1), \widetilde{v}(a^{-1}b)\right) = \min\left(w(1), w(a^{-1}b)\right) = \min\left(w(1), w(b) - w(a)\right)$$

Thus

$$\begin{aligned} w(a+b) = w(a) + w(1+a^{-1}b) &\geq w(a) + \min\left(w(1), w(b) - w(a)\right) \\ &\geq \min\left(w(1) + w(a), w(b)\right) \geq \min\left(w(a), w(b)\right) \end{aligned}$$

(2) This is an immediate consequence of (1), since

$$nw(a) = v\left(\mathrm{Nrd}_K^D(a)\right)$$

Note that (2) also resolves the question of whether w is discrete. □

Definition 4.6.30. Let $D, K, w, v, n, \Gamma_w, \Gamma_v$ be as above. The **ramification index** of D over K is

$$e(D|K) = [\Gamma_w : \Gamma_v]$$

A **uniformizer** for D is an element $\Pi \in D^\times$ such that $w(\Pi)$ is the positive generator for Γ_w. The **valuation ring** $\mathcal{O}_w$ of D is the subring

$$\mathcal{O}_w = \left\{a \in D^\times : w(a) \geq 0\right\} \cup \{0\}$$

with unit group [6]

$$\mathcal{O}_w^\times = \left\{a \in D^\times : w(a) = 0\right\}$$

The **valuation ideal** $\mathfrak{P}_w$ of D is the two sided prinicipal ideal of $\mathcal{O}_w$ generated by Π (for any choice of uniformizer).

$$\mathfrak{P}_w = \Pi\mathcal{O}_w = \mathcal{O}_w\Pi = \left\{a \in D^\times : w(a) > 0\right\} \cup \{0\}$$

The **residue algebra** of D is $\overline{D} = \mathcal{O}_w/\mathfrak{P}_w$. Note that $\overline{D}$ is a division ring, because every nonzero element $x\mathfrak{P}_w$ is represented by a unit $x \in \mathcal{O}_w^\times$. It is an algebra over the residue field $k = \mathcal{O}_v/\mathfrak{p}_v$. For $a \in \mathcal{O}_w$, the image of a in $\overline{D}$ is denoted $\overline{a}$. The **residual degree** of D over K is

$$f(D|K) = \dim_k \overline{D}$$

Lemma 4.6.31. *Let D, K, v, w be as above; in particular, $\dim_K D$ is finite.*

1. *If $a_1, \ldots, a_r \in \mathcal{O}_w$ are such that $\overline{a}_1, \ldots, \overline{a}_r \in \overline{D} = \mathcal{O}_w/\mathfrak{P}_w$ are linearly independent over $k = \mathcal{O}_v/\mathfrak{p}_v$, then $a_1, \ldots, a_r$ are linearly independent over K.*

2. *The residual degree $f(D|K)$ is finite.*

Proof. (1) Let $a_1, \ldots, a_r \in \mathcal{O}_w$ be as in the statement of the proposition. Suppose $a_1, \ldots, a_r$ are not linearly independent, so that there are $\lambda_1, \ldots, \lambda_r \in K$ not all zero so that

$$\sum_{i=1}^{r} \lambda_i a_i = 0$$

Set

$$J = \{j : \lambda_j \neq 0\} \neq \emptyset$$

so that

$$\sum_{j \in J} \lambda_j a_j = 0 \tag{4.6.2}$$

with all nonzero terms. For $j \in J$, we can choose a unit $u_j \in \mathcal{O}_v^\times$ so that

$$\lambda_j = \pi^{v(\lambda_j)} u_j$$

Then set

$$n = \max\{-v(\lambda_j) : j \in J\}$$

so that for all $j \in J$, we have

$$n \geq -v(\lambda_j) \implies n + v(\lambda_j) \geq 0 \implies \pi^n \lambda_j = \pi^{n+v(\lambda_j)} u_j \in \mathcal{O}_v$$

since $v(\pi^{n+v(\lambda_j)} u_j) = n + v(\lambda_j) \geq 0$. Let $j_0 \in J$ such that $n = -v(\lambda_{j_0})$. Then

$$\pi^n \lambda_{j_0} = \pi^{-v(\lambda j_0)+v(\lambda_{j_0})} u_{j_0} = u_{j_0} \in \mathcal{O}_v \setminus \mathfrak{p}_v$$

[6] We justify that this set is the group of units. If $w(a) = 0$, then $0 = w(1) = w(aa^{-1}) = w(a) + w(a^{-1}) = w(a^{-1})$ so a^{-1} is also in $\mathcal{O}_w$, so $a \in \mathcal{O}_w^\times$.. Conversely, if $a \in \mathcal{O}_w^\times$ is a unit, then $a^{-1} \in \mathcal{O}_w$. By the previous equalities, $w(a) = -w(a^{-1})$, and since $a, a^{-1} \in \mathcal{O}_w$, $w(a), w(a^{-1}) \geq 0$, which is only possible if both zero.

since $v(u_{j_0}) = 0$. Now multiply the linear relation 4.6.2 by π^n, to obtain

$$\sum_{j \in J} \pi^n \lambda_j a_j = 0$$

As we noted, $\pi^n \lambda_j \in \mathcal{O}_v$, so we obtain a linear relation in $\overline{D}$.

$$\sum_{j \in J} \overline{\pi^n \lambda_j} \overline{a_j} = 0 \qquad \overline{\pi^n \lambda_j} \in k,\ \overline{a_j} \in \overline{D}$$

By linear independence of $\overline{a}_1, \ldots, \overline{a}_r$ over k, it follows from this relation that $\overline{\pi^n \lambda_j} = 0 \in k$, that is, $\pi^n \lambda_j \in \mathfrak{p}_v$ for all $j \in J$. But this is a contradiction, since we know that $\pi^n \lambda_{j_0}$ is not in $\mathfrak{p}_v$. (2) follows immediately from (1), since (1) implies $\dim_k \overline{D} \leq \dim_K D$, and $\dim_K D$ is finite by assumption. □

Proposition 4.6.32. *Let K be a complete nonarchimedean local field and D a finite dimensional central division algebra over K. Then*

$$e(D|K) = f(D|K) = n$$

and D contains an unramified extension of K of degree n.

Proof. Proposition 10 of Rapinchuk [12]. □

Now we obtain the main result of this section, which identifies $\mathrm{Br}(K)$ with the relative Brauer group of the maximal unramified extension, which we already know about.

Corollary 4.6.33. *Let K be a complete nonarchimedean local field, with K_n the unique unramified extension of degree n, and K^{un} the maximal unramified extension. Then*

$$\mathrm{Br}(K) = \bigcup_n \mathrm{Br}(K_n/K) = \mathrm{Br}(K^{\mathrm{un}}/K)$$

Proof. Elements of $\mathrm{Br}(K)$ correspond to isomorphism classes of division algebras D over K. By Proposition 4.6.32, if D is such a division algebra with $\dim_K D = n^2$, then D contains K_n, and by Theorem 4.4.3, $D \in \mathrm{Br}(K_n/K)$. Hence

$$\mathrm{Br}(K) \subset \bigcup_n \mathrm{Br}(K_n/K)$$

and the opposite inclusion is by definition, so they are equal. The second equality comes from Proposition 4.6.23. □

The next theorem mostly just reiterates the previous corollary. It also answers the following question: if K is a local field and L/K is a finite extension, we know L is also a local field, so now we know L, K have the same Brauer group, namely $\mathbb{Q}/\mathbb{Z}$. So what exactly is the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ in terms of the isomorphism with $\mathbb{Q}/\mathbb{Z}$?

It turns out to be just multiplication by the degree $[L : K]$. This is somewhat surprising - the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$, at least in terms of the isomorphism with $\mathbb{Q}/\mathbb{Z}$, does not depend on any features of L except $[L : K]$. For instance, it does not depend on whether L/K is ramified or unramified, so not that much information about L is captured in the relative Brauer group $\mathrm{Br}(L/K)$.

Theorem 4.6.34. *Let K be a complete nonarchimedean local field with discrete valuation v.*

1. *There is an isomorphism $i_K : \mathrm{Br}(K) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}$.*
2. *If L/K is an extension of degree n, and $\epsilon : \mathrm{Br}(K) \to \mathrm{Br}(L)$ is the usual extension map $[A] \mapsto [A \otimes_K L]$, then the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{i_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle n} \\ \mathrm{Br}(L) & \xrightarrow{i_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Proof. (1) In Proposition 4.6.23, we constructed an isomorphism of directed systems

$$\psi_n : \mathrm{Br}(K_n/K) \xrightarrow{\cong} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \qquad [(K_n, \phi_n, \alpha)] \mapsto \frac{v(\alpha)}{n} \bmod \mathbb{Z}$$

where ϕ_n is the Frobenius automorphism of K_n and $\alpha \in K^\times$ is arbitrary. This induces an isomorphism on the direct limits,

$$i_K : \mathrm{Br}(K^{\mathrm{un}}/K) = \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z} \qquad [(K_n, \phi_n, \alpha)] \mapsto \frac{v(\alpha)}{n} \bmod \mathbb{Z}$$

(2) By Proposition 6.4.4, we can decompose L/K into an unramified and totally ramified extension.

$$\begin{array}{c} L \\ \big| \text{totally ramified} \\ M \\ \big| \text{unramified} \\ K \end{array}$$

If (2) holds for the extensions M/K and L/M, then combining the two commutative squares gives a commutative square for L/K, so it suffices to prove (2) in the two separate cases of totally ramified extensions, and unramified extensions. For details, see Theorem 10 of Rapinchuk [12]. □

Example 4.6.35. Let p be a prime. By the previous result, $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$.

As previously discussed, the relative Brauer group $\mathrm{Br}(L/K)$ (when L, K are local) does n't capture very much information about L. The next corollary makes this a bit more precise. As we already noted, the map $\mathrm{Br}(K) \to \mathrm{Br}(L)$ only "sees" the degree $[L : K]$, so it makes sense that the kernel $\mathrm{Br}(L/K)$ would also "see" $[L : K]$, which is what the corollary says.

Corollary 4.6.36. *Let K be a complete nonarchimedean local field, and let K_n be the unique unramified extension of degree n. If L/K is an extension of degree n, then $\mathrm{Br}(L/K) \cong \mathrm{Br}(K_n/K)$. That is, any two relative Brauer groups $\mathrm{Br}(L/K), \mathrm{Br}(E/K)$ are isomorphic as long as $[L : K] = [E : K]$.*

Proof. By the commutative diagram of Theorem 4.6.34, the we have the following commutative diagram with exact rows.

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Q}/\mathbb{Z}[n] = \ker n = \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \\ & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong \\ 0 & \longrightarrow & \mathrm{Br}(L/K) = \ker \epsilon & \longrightarrow & \mathrm{Br}(K) & \xrightarrow{\epsilon} & \mathrm{Br}(L) \end{array}$$

By Proposition 4.6.23,

$$\mathrm{Br}(K_n/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathrm{Br}(L/K)$$

□

Corollary 4.6.37. *Let K be a complete nonarchimedean local field and let L/K be a Galois extension of degree n. Then*

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathbb{Z}/n\mathbb{Z}$$

Proof. By Proposition 4.5.6,

$$H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K)$$

By Corollary **??**,

$$\mathrm{Br}(L/K) \cong \mathrm{Br}(K_n/K) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$$

□

Remark 4.6.38. The main application of Corollary 4.6.37 is to verify the one of the hypotheses of Tate's theorem 3.7.10 in the follow situation, which is important in local class field theory.

Let K be a complete nonarchimedean discretely valued local field (such as $\mathbb{Q}_p$), and let L/K be a finite extension. Let $G = \mathrm{Gal}(L/K)$ and $A = L^\times$, so A is a G-module. By Galois theory, all subgroups $H \subset G$ are of the form $\mathrm{Gal}(L/E)$ where $K \subset E \subset L$ is an intermediate subfield. By Hilbert 90,

$$\widehat{H}^1(H, A) = H^1(\mathrm{Gal}(L/E), L^\times) = 0$$

and by Corollary 4.6.37,

$$\widehat{H}^2(H, A) = H^2(\mathrm{Gal}(L/E), L^\times) \cong \mathbb{Z}/m\mathbb{Z}$$

where $m = [L : E] = |H|$. Thus, all the hypotheses of Tate's theorem 3.7.10 are satisfied in this situation.

4.6.9 Quadratic number field

Let d be a square free integer, and consider the quadratic number field $\mathbb{Q}(\sqrt{d})$, which is a degree two extension of $\mathbb{Q}$. In this section, we say what we can about the relative Brauer group $\mathrm{Br}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Though we do not compute it fully, we at least reduce the problem to a purely number theoretic equation solving problem.

The first basic obsevation is that $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is order 2 (so it is $\mathbb{Z}/2\mathbb{Z}$), and we know that

$$\mathrm{Br}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \cong H^2(\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}), \mathbb{Q}(\sqrt{d})^\times)$$

The cohomology group on the right is 2-torsion, because the Galois group is order 2. So $\mathrm{Br}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is some 2-torsion group, or equivalently a vector space over $\mathbb{Z}/2\mathbb{Z}$, or equivalently some big direct sum or product of copies of $\mathbb{Z}/2\mathbb{Z}$. So to determine the structure, we just need to figure out how many copies of $\mathbb{Z}/2\mathbb{Z}$ there are. We might also be interested in how to describe those algebras, but that's a secondary goal.

Now to describe the generators of copies of $\mathbb{Z}/2\mathbb{Z}$ for this group. Since $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ is cyclic, we can use our characterization in terms of the norm map.

$$\mathrm{Br}\left(\mathbb{Q}(\sqrt{d})/\mathbb{Q}\right) \cong H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}(\sqrt{d})^\times) \cong \mathbb{Q}^\times / \mathrm{N}(\mathbb{Q}(\sqrt{d})^\times$$

The norm map is

$$\mathrm{N}(a + b\sqrt{d}) = a^2 - b^2 d$$

Note that

$$\mathbb{Q}^\times = \left\{-1, 2, 3, \ldots | (-1)^2 = 1\right\rangle \cong \mathbb{Z}/2\mathbb{Z}\langle -1\rangle \oplus \bigoplus_{p \text{ prime}} \mathbb{Z}\langle p\rangle$$

It is clear that any prime square p^2 is in the image of the norm (just take $a = p, b = 0$), so the quotient is contained in

$$\bigoplus_{-1, p \text{ prime}} \mathbb{Z}/2\mathbb{Z}$$

That is $\mathrm{Br}(\mathbb{Q}(\sqrt{d})\mathbb{Q})$ is a large direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$, with one copy for each generator (either -1 or a prime p) that is not in the image of the norm map $\mathrm{N} : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{Q}^\times$. So we have reduced the problem to deciding which primes (and -1) can be written as $p = a^2 - b^2 d$ for $a, b \in \mathbb{Q}$. Of course, if a, b are solutions to this, then $a, b \in \mathbb{Z}$.

Example 4.6.39. Let $d = -1$. For $a, b \in \mathbb{Z}$, $a^2 + b^2 \neq -1$, so -1 gives a copy of $\mathbb{Z}/\mathbb{Z}$ in $\mathrm{Br}(\mathbb{Q}(i)/\mathbb{Q})$. By a well known result of Lagrange, a prime is a sum of two squares if and only if $p \equiv 1 \bmod 4$ or $p = 2$. So

$$\mathrm{Br}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\langle -1\rangle \oplus \mathbb{Z}/2\mathbb{Z}\langle 2\rangle \oplus \bigoplus_{p \equiv 1 \bmod 4} \mathbb{Z}/2\mathbb{Z}\langle p\rangle$$

Remark 4.6.40. The cases $d = -2, d = -3$ were conjectured by Fermat and proved by Lagrange. A prime can be written as $p = a^2 + 2b^2$ if and only if $p \equiv 1$ or $p \equiv 3 \bmod 8$. A prime can be written as $p = a^2 + 3b^2$ if and only if $p \equiv 1 \bmod 3$. The case $d = -5$ was also resolved by Lagrange, a prime can be written as $p = a^2 + 5b^2$ if and only if $p \equiv 1$ or $p \equiv 9 \bmod 20$.

A general study of such equations is found in the book *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication* by David Cox [2].

Chapter 5

Classical algebraic K-theory

These notes on algebraic K-theory do not have very many ties to the group cohomology and Brauer group sections above. They are also closer to the sources in terms of material, so this chapter is probably less useful for someone trying to learn algebraic K-theory than just reading Milnor's book [10] or Rosenberg's book [13].

For those who are still here are that rousing endorsement, algebraic K-theory is the study of and attempt to usefully define an infinite sequence of invariants $\mathrm{K}_0(R), \mathrm{K}_1(R), \mathrm{K}_2(R), \ldots$ associated to a ring R, and $\mathrm{K}_i(R)$ is an abelian group. The association $R \mapsto \mathrm{K}_i(R)$ is a functor, as all good invariants are.

In order, we define $\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2$ and derive some properties of them where we can. On the face of it, these three invariants do not seem to "hang together," that is, there is not much connecting them. Ideally, there would be something like the following: given a ring R and an ideal I, we have a short exact sequence $0 \to I \to R \to R/I \to 0$, and maybe there is a long exact sequence

$$\cdots \to \mathrm{K}_1(I) \to \mathrm{K}_1(R) \to \mathrm{K}_1(R/I) \to \mathrm{K}_0(I) \to \mathrm{K}_0(R) \to \mathrm{K}_0(R/I) \to \mathrm{K}_1(I)$$

Unfortunately, this has many obstacles. First, we said that $\mathrm{K}_i(-)$ will be defined for a ring R, and an ideal I is not a ring, so we would need to generalize to K_i of ideals. Second, once we define $\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2$, it is not at all clear how to generalize the definition higher K-groups, even K_3.

It turns out that there is a way to overcome much of this - there are K-groups for ideals, and there is even an exact sequence involving $\mathrm{K}_0, \mathrm{K}_1, \mathrm{K}_2$ (see Theorem 5.4.4). Despite this, the obstacle of defining K_3 proves to be too much, as we note in Remark 5.4.4, there is a theorem of Swan which shows that there is no possible definition of a functor K_3 which will extend the exact sequence further.

Given this impossibility, why study algebraic K-theory at all? A better answer for this question would be to look at Rosenberg's book [13] on applications of K-theory to various other areas of mathematics. We won't worry so much about the applications, just building up some of the theory.

5.1 Definition of $\mathrm{K}_0(R)$ via projective modules

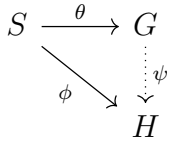
Given a ring R, a lot of the structure of R is captured by looking at the category of R-modules. (We assume rings have a unit and are associative, but do not always assume they are commutative.) The invariant $\mathrm{K}_0(R)$ drills down even a bit further - we consider only finitely generated R-modules, to avoid dealing with things that are "too big," and we restrict attention to projective modules, since they have so many excellent properties.

5.1.1 Grothendieck group completion

Let R be a ring, and consider the category of finitely generated projective modules. This category has a convenient binary operation given by direct sum, which has an identity (the trivial R-module). We might as well consider just isomorphism classes, too. So the isomorphism classes of finitely generated projective R-modules form a monoid, a set with a binary operation and identity.

As invariants go, monoids aren't ideal, since we don't have a lot of theory of monoids. It would be better if we had a group. Well, it turns out there's a way to just force a monoid to turn into a group. Roughly speaking, you can just throw in inverse elements and force group-ness on unsuspecting monoids. They never even see it coming.

Proposition 5.1.1 (Grothendieck group completion)**.** *Let S be a monoid. There is a unique group G and monoid homomorphism $\theta : S \to G$ with the following universal property: any monoid homomorphism $\phi : S \to H$ to a group H factors uniquely through G. That is, there is a unique group homomorphism $\psi : G \to H$ making the following diagram commute.*



Proof. This is not a thorough proof, merely a sketch. We write S multiplicatively with identity element 1. G is constructed in the way you would expect. Consider the set

$$S \sqcup \left\{ s^{-1} : s \in S \right\}$$

formed by adding formal inverses to S, and define $ss^{-1} = s^{-1}s = 1$. Then quotient out all relations that already exist in S, verify that the resulting monoid is in fact a group, and set

$$G = S \sqcup \left\{ s^{-1} : s \in S \right\} / \sim$$

The map $\theta : S \to G$ is the obvious one, by sending $s \in S$ to the class of s in G. The univeral property comes out of this construction without too much difficulty. □

Definition 5.1.2. Let S be a monoid. The group G from the previous proposition is the **Grothendieck group completion** of S.

Remark 5.1.3. While it seems plausible to guess that the special morphism $S \to G$ involved in the group completion is always an injective function, this is not the case. A counterexample is given in Proposition 5.1.6.

The next lemma gives a somewhat obvious but convenient criterion for describing group completions more concretely.

Lemma 5.1.4. *Let S be a monoid, and suppose there is a monoid homomorphism $\theta : S \to G$ where G is a group, and the image of S generates G. Then G is the Grothendieck group completion of S, and θ is the canonical homomorphism.*

Proof. We show that G has the universal property. If $\phi : S \to H$ is a monoid homomorphism to a group H, there is a group homomorphism $G \to H$ defined on generators $\theta(s)$ of G by

$$\phi(\theta(s)) = \phi(s)$$

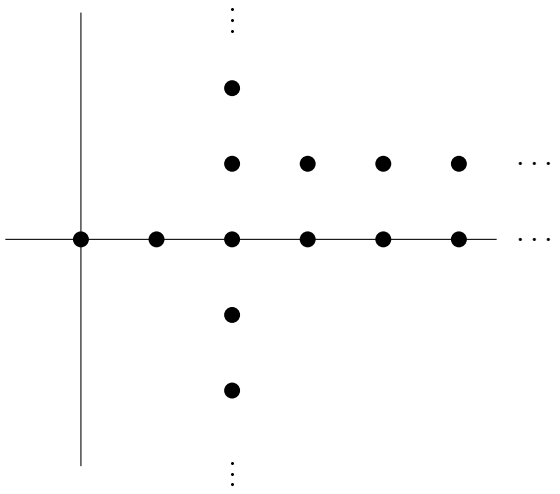
Clearly, this is also the only homomorphism possibly making the required triangle commute. □

Next we give an example of when the canonical map from a monoid S to its group completion G is not an injective function. If the reader is not interested, the example can be safely skipped. In that case, jump to the next section.

Definition 5.1.5. Let S be the set of points $a_{n,m}$ with $n \in \mathbb{Z}_{\geq 0}$ and

$$\begin{cases} m = 0 \text{ if } n = 0, 1 \\ m \in \mathbb{Z} \text{ if } n = 2 \\ m \in \{0, 1\} \text{ if } n \geq 3 \end{cases}$$

Graphically, we can depict S as the following set of points in the integer lattice. The horizontal axis is the n variable, and the vertical axis is the m variable.



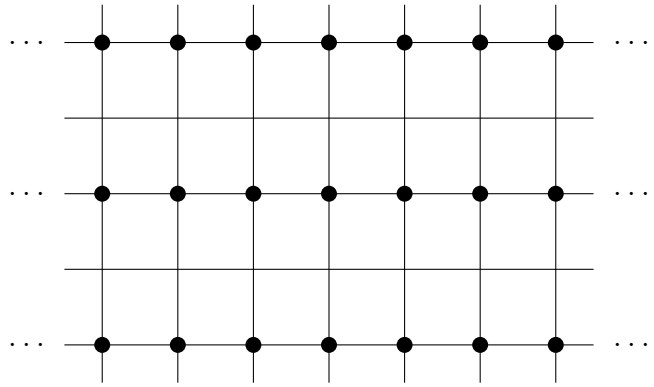
We give S an addition operation by

$$a_{n,m} + a_{n',m'} = a_{n+n',m+m'}$$

where $m+m'$ is reduced mod 2 if $n+n' \geq 3$. This makes S an abelian monoid with identity $a_{0,0}$.

Proposition 5.1.6 (Rosenberg [13] Exercise 1.1.7)**.** *Let S be the set defined above. The Grothendieck group completion of S is $G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the canonical homomorphism $S \to G$ is not injective.*

Proof. Let $N = \mathbb{Z} \times 2\mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}$ be the sublattice as depicted below.



Then define $\theta : S \to (\mathbb{Z} \times \mathbb{Z})/N \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by $a_{n,m} \mapsto (n, m \bmod 2)$. This is a monoid homomorphism, since

$$\theta(a_{n,m} + a_{n',m'}) = \theta(a_{n+n',m+m'}) = (n+n', m+m' \bmod 2) = (n, m \bmod 2) + (n', m' \bmod 2) = \theta(a_{n,m}) + \theta($$

Also, the image of S under θ includes $(1,0)$ and $(0,1)$, as seen below.

$$\theta(a_{1,0}) = (1,0) \qquad \theta(a_{2,3}) - \theta(a_{2,2}) = (2,3) - (2,2) = (0,1)$$

Thus $\theta(S)$ generates $(\mathbb{Z} \times \mathbb{Z})/N$, so by Lemma 5.1.4, $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the Grothendieck group of S and θ is the canonical homomorphism. Finally, it is clear that θ is not injective, because $\theta(a_{2,0}) = \theta(a_{2,2})$. □

5.1.2 Definition of K_0

We started our discussion of group completions by discussion the monoid of isomorphism classes of finitely generated projective R-modules under $\oplus$, so it's no surprise that we're going to form the group completion of that particular monoid.

Definition 5.1.7. Let R be a commutative ring with unity. The isomorphism classes of finitely generated projective modules over R form a monoid with respect to direct sum. $\mathrm{K}_0(R)$ is defined to be the Grothendieck group completion of this monoid.

Concretely, this means that elements of $\mathrm{K}_0(R)$ are isomorphism classes $[P]$ of projective R-modules, along with their formal inverses $-[P]$, and addition in $\mathrm{K}_0(R)$ is given on projective modules by

$$[P] + [Q] = [P \oplus Q]$$

Equivalently, we can describe $\mathrm{K}_0(R)$ as the free abelian group generated by isomorphism classes $[P]$ of projective R-modules, modulo the above relation.

Now we have half of a functor (the part on objects, $R \mapsto \mathrm{K}_0(R)$), so we need to describe how the functor K_0 acts on ring homomorphisms.

Definition 5.1.8. Let $f : R \to R'$ be a ring homomorphism. The **induced map** on K_0 is

$$f_\# : \mathrm{K}_0(R) \to \mathrm{K}_0(R') \qquad [P] \mapsto [R' \otimes_R P]$$

This tensor product makes sense becuase R' has an R-module structure via f. If P is finitely generated and projective (over R), then $R' \otimes_R P$ is finitely generated and projective (over R'), so this is a well defined map. Since the tensor product distributes over direct sums, this is a homomorphism of abelian groups. It is clear that $f_\#$ is functorial as well, that is,

$$(\mathrm{Id}_R)_\# = \mathrm{Id}_{K_0(R)} \qquad (f \circ g)_\# = f_\# \circ g_\#$$

This makes K_0 a covariant functor from the category of commutative rings with unity to the category of abelian groups.

Remark 5.1.9. Let R be a commutative ring. $\mathrm{K}_0(R)$ is already an abelian group under $\oplus$. We can also give it a multiplication operation via $\otimes$ (tensor over R).

$$[P] \otimes [Q] = [P \otimes Q]$$

There is some mild checking to verify this is well defined: one verifies that the tensor product of finitely generated modules is finitely generated, and that the tensor product of projective modules is projective. The multiplicative unit is then $[R]$, since

$$[P] \otimes [R] = [P \otimes R] = [P]$$

We don't usually think much about the ring structure on $\mathrm{K}_0(R)$, mostly because other K-groups do not have such obvious ring structures, so it's more holistic to consider them all as abelian groups.

5.1.3 Necessity of finite generation

It might be tempting to throw away the "finitely generated" part of defining $\mathrm{K}_0(R)$, but the following proposition shows that this leads to the whole theory being somewhat trivial. That is to say, without the finite generation hypothesis, K_0 would be less interesting.

Proposition 5.1.10 (Eilenberg Swindle)**.** *Let R be a ring, and let S be the set of isomorphism classes of countably generated projective R-modules, with addition given by $[P]+[Q] = [P \oplus Q]$. Let G be the group completion of S. Then G is trivial.*

Proof. It suffices to show that for any countably generated projective R-module P, the class $[P]$ is zero in G. Let P be a countably generated projective R-module. We denote the countably generated free R-module by R^∞. Then there is an R-module Q such that

$$P \oplus Q \cong R^\infty$$

Then

$$\begin{aligned} P \oplus R^\infty &\cong P \oplus R \oplus R \oplus \cdots \\ &\cong P \oplus (Q \oplus P) \oplus (Q \oplus P) \oplus \cdots \\ &\cong (P \oplus Q) \oplus (P \oplus Q) \oplus \cdots \\ &\cong R^\infty \end{aligned}$$

which induces the equality

$$[P] + [R^\infty] = [R^\infty] \implies [P] = 0$$

in G. □

5.1.4 K_0 of a PID

We give just a few examples of computation of K_0, and "computation" is a strong word for it.

Example 5.1.11. Let R be a PID (this includes fields). Then every projective module over R is free, hence the isomorphism classes of projective R-modules are determined by dimension. Dimension is additive with respect to direct sum, so we obtain an isomorphism

$$\dim : \mathrm{K}_0(R) \to \mathbb{Z} \qquad [P] = [R^n] = n[R] \mapsto \dim P = n$$

Example 5.1.12. Let R be a Dedekind domain (such as a ring of integers of a number field). Then

$$\mathrm{K}_0(R) \cong \mathrm{Cl}(R) \oplus \mathbb{Z}$$

where $\mathrm{Cl}(R)$ denotes the class group. We do not dedicate the space to prove it, but it can be found in chapter one of Milnor [10].

5.2 Definition of $\mathrm{K}_1(R)$ via infinite general linear group

Rather than dwell on K_0 for any longer, we move right along to defining K_1. Somewhat strangely, there is little overlap in setup - K_1 does not involve a group completion, or projective modules. Instead, the starting point is the group of invertible matrices over R, $\mathrm{GL}(n, R)$.

Definition 5.2.1. Let R be a ring. The **infinite general linear group** $\mathrm{GL}(R)$ is the direct limit of the chain of inclusions

$$\mathrm{GL}(1, R) \subset \mathrm{GL}(2, R) \subset \mathrm{GL}(3, R) \subset \cdots$$

where $\mathrm{GL}(n, R)$ embeds into $\mathrm{GL}(n + 1, R)$ by adding an extra column and row of zeroes, except for a 1 in the bottom right corner.

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

Thus $\mathrm{GL}(R)$ is the direct limit of all $\mathrm{GL}(n, R)$ where $A \in \mathrm{GL}(n, R)$ is identified with its images under the infinite chain of embeddings. (The direct limit is just the disjoint union, modulo the obvious identifications.) It is reasonable, though not entirely accurate, to think of $\mathrm{GL}(R)$ as "infinite matrices" which differ from the "infinite identity matrix" in only finitely many entries.

Definition 5.2.2. An element of $\mathrm{GL}(R)$ is an **elementary matrix** if it differs from the identity in exactly one off-diagonal entry. We denote the matrix with r in the ijth off diagonal entry by e_{ij}^r. The subgroup generated by all elementary matrices is $\mathrm{E}(R)$.

Remark 5.2.3. The following relations are not immediately obvious, but also not interesting to prove. Let i, j, k, ℓ be positive integers and $r, s \in R$.

$$e_{ij}^r e_{ij}^s = e_{ij}^{r+s}$$
$$\left[e_{ij}^r, e_{k\ell}^s\right] = \begin{cases} 1 & j \neq k, i \neq \ell \\ e_{i\ell}^{rs} & j = k, i \neq \ell \\ e_{kj}^{-sr} & j \neq k, i = \ell \end{cases}$$

Lemma 5.2.4 (Whitehead lemma)**.** $\mathrm{E}(R)$ *is equal to the commutator subgroup of* $\mathrm{GL}(R)$.

Proof. It is easy to show $\mathrm{E}(R) \subset [\mathrm{GL}(R), \mathrm{GL}(R)]$ by exhibiting each elementary matrix as a commutator of two matrices, which is immediate from the previous relations. The reverse inclusion is not quite as easy. Very roughly speaking, the proof is just Gaussian elimination. □

Definition 5.2.5. The **Whitehead group** $\mathrm{K}_1(R)$ is the quotient

$$\mathrm{GL}(R)/\,\mathrm{E}(R) = \mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)] = \mathrm{GL}(R)^{\mathrm{ab}}$$

In other words, $\mathrm{K}_1(R)$ is the cokernel of the inclusion $\mathrm{E}(R) \hookrightarrow \mathrm{GL}(R)$.

A ring homomorphism $f : R \to R'$ induces homomorphisms $\mathrm{GL}(n, R) \to \mathrm{GL}(n, R')$ for all n, and passing to the direct limit give a morphism $\mathrm{GL}(R) \to \mathrm{GL}(R')$. Passing to the abelianization, we obtain an induced map $f_* : \mathrm{K}_1(R) \to \mathrm{K}_1(R')$ making K_1 a covariant functor.

5.2.1 K_1 of a Euclidean domain

To give some example computations of K_1 for Euclidean and Dedekind domains, we first need a lemma.

Lemma 5.2.6 ($\mathrm{E} = \mathrm{SL}$ for Euclidean domain)**.** *Let R be a Euclidean domain. Then $\mathrm{E}(n, R) = \mathrm{SL}(n, R)$, and hence $\mathrm{E}(R) = \mathrm{SL}(R)$. If R is a Dedekind domain, then it is not necessarily true the $\mathrm{E}(n, R) = \mathrm{SL}(n, R)$, but $\mathrm{E}(R) = \mathrm{SL}(R)$ does hold.*

Proof. The proof for a Euclidean domain is, very roughly speaking, just the process of doing Gaussian elimination [1]. I have no idea why this is true for a Dedekind domain. □

Example 5.2.7. Let R be a Euclidean domain (this includes fields). By the previous lemma, $\mathrm{E}(R) = \mathrm{SL}(R)$, so

$$\mathrm{K}_1(R) = \mathrm{GL}(R)/\,\mathrm{SL}(R)$$

[1] "The special linear group over a field or a Euclidean domain is generated by transvections, and the stable special linear group over a Dedekind domain is generated by transvections." `https://en.wikipedia.org/wiki/Special_linear_group`

Considering the exact sequence

$$0 \longrightarrow \mathrm{SL}(R) \hookrightarrow \mathrm{GL}(R) \xrightarrow{\det} R^\times \longrightarrow 0$$

by the 1st isomorphism theorem,

$$\mathrm{K}_1(R) = \mathrm{GL}(R)/\mathrm{SL}(R) \cong R^\times$$

5.3 The functor K_2

While the connection between K_0 and K_1 remains mysterious at this point, the connection between K_1 and K_2 is more immediately obvious. Recall that K_1 was the cokernel of $\mathrm{E}(R) \to \mathrm{GL}(R)$. We will identify another group $\mathrm{St}(R)$ (the Steinberg group) which maps to $\mathrm{GL}(R)$ with image $\mathrm{E}(R)$, so we can realize $\mathrm{K}_1(R)$ also as the cokernel of $\mathrm{St}(R) \to \mathrm{GL}(R)$.

$$\mathrm{St}(R) \to \mathrm{GL}(R) \to \mathrm{K}_1(R) \to 0$$

Thinking categorically, one thing to consider next is the kernel of $\mathrm{St}(R) \to \mathrm{GL}(R)$. This is exactly our definition of $\mathrm{K}_2(R)$. First, though, we need to put in some work to properly define the Steinberg group $\mathrm{St}(R)$.

5.3.1 Definition of K_2 via the Steinberg group

Recall the various commutator relations that we wrote down for elementary matrices.

$$e_{ij}^r e_{ij}^s = e_{ij}^{r+s}$$

$$\left[e_{ij}^r, e_{k\ell}^s\right] = \begin{cases} 1 & j \neq k, i \neq \ell \\ e_{i\ell}^{rs} & j = k, i \neq \ell \\ e_{kj}^{-sr} & j \neq k, i = \ell \end{cases}$$

It is not so easy to tell whether these are all the relations in $\mathrm{E}(R)$, or if there are more. In particular, other relations may depend on the structure of the ring R. To avoid dealing with this to some degree, and also to make an attempt to answer the question of when these are sufficient relations, we abstract the relations into another group which we *define* to have just "these relations." That group is what we call the Steinberg group.

Definition 5.3.1. Let R be a ring and let $n \geq 3$. The **Steinberg group** $\mathrm{St}(n, R)$ is the group generated by symbols x_{ij}^r for $1 \leq i, j \leq n, i \neq j, r \in R$ subject to the following relations.

$$x_{ij}^r x_{ij}^s = x_{ij}^{r+s}$$

$$\left[x_{ij}^r x_{j\ell}^s\right] = x_{i\ell}^{rs} \qquad i \neq \ell$$

$$\left[x_{ij}^r, x_{k\ell}^s\right] = 1 \qquad j \neq k, i \neq \ell$$

The **stable Steinberg group** or just **Steinberg group**, denoted $\mathrm{St}(R)$ is the direct limit of all $\mathrm{St}(n, R)$ via the obvious inclusions $\mathrm{St}(n, R) \hookrightarrow \mathrm{St}(n+1, R)$.

Alternately, it is reasonable to think of $\mathrm{St}(R)$ as the group generated by x_{ij}^r for all $i, j \in \mathbb{Z}_{\geq 1}$ and $r \in R$, subject to the above relations.

Definition 5.3.2. The **canonical homomorphism** from the Steinberg group to the general linear group is

$$\phi : \mathrm{St}(n, R) \to \mathrm{GL}(n, R) \qquad x_{ij}^r \mapsto e_{ij}^r$$

Clearly the image is $\mathrm{E}(n, R)$. This is a homomorphism precislely because we only imposed relations on the x_{ij}^r which we already know to be true for e_{ij}^r. Passing to the direct limit, we obtain a homomorphism

$$\phi : \mathrm{St}(R) \to \mathrm{GL}(R)$$

with image $\mathrm{E}(R)$.

Definition 5.3.3. The kernel of the canonical homomorphism $\mathrm{St}(R) \to \mathrm{GL}(R)$ defined above is denoted $\mathrm{K}_2(R)$. Note that a homomorphism of rings $f : R \to R'$ induces a homomorphism on $\mathrm{St}(R)$ via

$$x_{ij}^r \mapsto x_{ij}^{f(r)}$$

hence induces a homomorphism on $\mathrm{K}_2(R)$, making K_2 a covariant functor. Also note that it fits into an exact sequence

$$1 \to \mathrm{K}_2(R) \to \mathrm{St}(R) \to \mathrm{GL}(R) \to \mathrm{K}_1(R) \to 1$$

Remark 5.3.4. In contrast with $\mathrm{K}_0, \mathrm{K}_1$, we cannot at this point give any examples of computations for K_2. Recall that for $\mathrm{K}_0, \mathrm{K}_1$ we really only tackled very special cases in our examples, where R was a Euclidean domain or Dedekind domain. These include the case of fields, at least. In the case of K_2, even the case when R is a field is not a reasonable example computation - it is a major theorem of Matsumoto, which we get to in a few sections.

5.4 Exact sequence involving K-groups

In this section, we give our only real link between the groups K_0 and $\mathrm{K}_1, \mathrm{K}_2$ via some exact sequences. However, the presentation is incredibly hand-wavy, so for any level of detail other sources should be consulted.

Remark 5.4.1. For a ring R, and an ideal I, there are sensible definitions of $\mathrm{K}_2\, I, \mathrm{K}_1\, I, \mathrm{K}_0\, I$. See Milnor [10] chapters 4 and 6.

Theorem 5.4.2. *Let R be a ring (not necessarily commutative) and I a two-sided ideal. There is an exact sequence*

$$\mathrm{K}_2\, I \to \mathrm{K}_2\, R \to \mathrm{K}_2\, R/I \to \mathrm{K}_1\, I \to \mathrm{K}_1\, R \to \mathrm{K}_1\, R/I \to \mathrm{K}_0\, I \to \mathrm{K}_0\, R \to \mathrm{K}_0\, R/I$$

Proof. See chapters 3,4,6 of Milnor [10]. □

Theorem 5.4.3 ("Mayer-Vietoris" sequence)**.** *Suppose we have a commutative square of rings (not necessarily commutative)*

$$\begin{array}{ccc} R & \xrightarrow{i_1} & R_1 \\ \downarrow{\scriptstyle i_2} & & \downarrow{\scriptstyle j_1} \\ R_2 & \xrightarrow{j_2} & R' \end{array}$$

satisfying

1. *R is the product of R_1, R_2 over R'. That is, for $r_1 \in R_1, r_2 \in R_2$, with $j_1(r_1) = j_2(r_2) \in R'$, there exists a unique $r \in R$ such that $i_1(r) = r_1, i_2(r) = r_2$.*

2. *At least one of j_1, j_2 is surjective.*

Then there is an exact sequence,

$$\mathrm{K}_1 R \to \mathrm{K}_1 R_1 \oplus K_1 R_2 \to \mathrm{K}_1 R' \to \mathrm{K}_0 R \to \mathrm{K}_0 R_1 \oplus \mathrm{K}_0 R_2 \to \mathrm{K}_0 R'$$

If the original commutative square also satisfies

3. *All maps i_1, i_2, j_1, j_2 are surjective.*

The the exact sequence can be extended to the left as follows.

$$\mathrm{K}_2 R \to \mathrm{K}_2 R_1 \oplus \mathrm{K}_2 R_2 \to \mathrm{K}_2 R' \to \mathrm{K}_1 R \to \cdots$$

Proof. See chapters 3,4,6 of Milnor [10]. □

Remark 5.4.4. Unfortunately, there is a result of Swan that there is no functor K_3 which will extend the previous two exact sequences further to the left. This may be taken as a sign that the definitions of K-groups for ideals given by Milnor "may not be too useful," to quote Milnor himself (Milnor [10] Remark 6.5).

5.5 Universal central extensions of groups

In an attempt to compute some K_2 groups, even for just a field, we begin with some theory of universal central extensions of groups. The eventual purpose of this is to identify $\mathrm{K}_2(R)$ with the group homology group $H_2(\mathrm{E}(R), \mathbb{Z})$, which is hopefully more computable, given our various tools for group homology.

We use $Z(G)$ or $\mathrm{center}(G)$ to denote the center of a group G. Our study of central extensions is motivated by the following result.

Theorem 5.5.1 (Milnor [10] 5.1)**.** $\mathrm{K}_2(R) = \mathrm{center}(\mathrm{St}(R))$.

Because of this, we have a short exact sequence of groups

$$1 \to \mathrm{K}_2(R) \to \mathrm{St}(R) \to E(R) \to 1$$

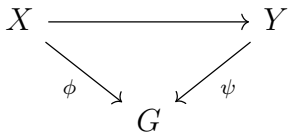
where (the image of) $\mathrm{K}_2(R)$ lies in the kernel of $\mathrm{St}(R) \to \mathrm{E}(R)$. We will study sequences of this type in more abstract generality, before returning to $\mathrm{K}_2(R)$ and $\mathrm{St}(R)$. Eventually, we will see that $\mathrm{St}(R)$ is not merely one example of such a situation, it is a very special type, called a universal central extension.

5.5.1 Definitions

Now we embark on a full study of central extensions, develop various criteria for when an extension is universal, and when a universal extension exists.

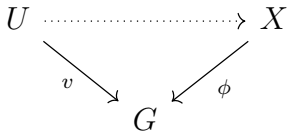
Definition 5.5.2. A **central extension** of a group G is a group X along with a surjective homomorphism $\phi : X \to G$ such that $\ker \phi \subset \text{center}(X)$. It is often denoted by (X, ϕ).

Definition 5.5.3. Let (X, ϕ) and (Y, ψ) be central extensions of G. A homomorphism $X \to Y$ **over G** is a homomorphism making the following triangle commute.



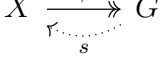
Thinking categorically, we could observe that central extensions of G form a category, with the morphisms being group homomorphisms over G. Then we could define a **universal central extension** as an initial object in this category. Alternatively, we give a more concrete definition below.

Definition 5.5.4. A **universal central extension** of a group G is a central extension (U, v) such that for any central extension (X, ϕ), there is a unique homomorphism $U \to X$ over G.



As a consequence of the universal property, if such (U, v) exists, it is unique up to isomorphism. As a consequence of the uniqueness of the homomorphism, any map $U \to U$ over G must be the identity.

Definition 5.5.5. A central extension (X, ϕ) is **split** if there is a section $s : G \to X$ so that $\phi s = \text{Id}_G$.



Note that if (X, ϕ) splits, then $X \cong G \times \ker \phi$ via

$$\begin{aligned} X \to G \times \ker \phi \qquad & x \mapsto \left(\phi x, xs\phi\left(x^{-1}\right)\right) \\ G \times \ker \phi \to X \qquad & (g, x) \mapsto s(g)x \end{aligned}$$

Definition 5.5.6. A group G is **perfect** if $G = [G, G]$.

Example 5.5.7. Let R be a commutative ring. The groups $\text{E}(n, R)$ and $\text{E}(R)$ are pefect, as a consequence of the basic commutator computations of elementary matrices. Similarly, the groups $\text{St}(n, R)$ and $\text{St}(R)$ are perfect, because of the "same" commutator relations in the Steinberg group.

5.5.2 Criterion for universality

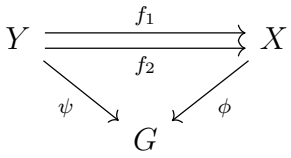
Our next goal is to prove the following criterion for a central extension to be universal.

Theorem 5.5.8 (Milnor [10] 5.3)**.** *A central extension U of G is universal if and only if U is perfect and every central extension of U splits.*

We'll build up to the proof with several lemmas.

Lemma 5.5.9 (Milnor [10] 5.4)**.** *Let (X, ϕ) and (Y, ψ) be central extensions of G. If Y is perfect, there exists at most one homomorphism from Y to X over G.*

Proof. Let $f_1, f_2 : Y \to X$ be homomorphisms over G.



For $y \in Y$, we have

$$f_1(y) = f_2(y)c$$

with $c \in \ker \phi$. (Concretely, $c = f_2(y)^{-1} f_1(y)$, but whatever.) Now for $y, z \in Y$, we have

$$f_1(yzy^{-1}z^{-1}) = \Big(f_2(y)c\Big)\Big(f_2(z)c\Big)\Big(f_2(y^{-1})c^{-1}\Big)\Big(f_2(z^{-1})c^{-1}\Big) = f_2(yzy^{-1}z^{-1})$$

Since Y is perfect, it is generated by commutators, and since f_1, f_2 agree on commutators, they are the same homomorphism. □

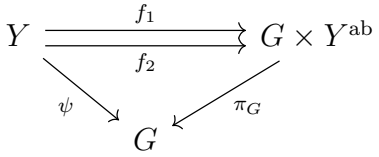
Lemma 5.5.10 (Milnor [10] 5.5)**.** *Every universal central extension is a perfect group.*

Proof. We'll prove the contrapositive, which is the following: If (Y, ψ) is a central extension of G with Y not perfect, then (Y, ψ) is not universal. In particular, we'll prove that the uniqueness property can fail, by constructing central extension (X, ϕ) (of G) so that there is more than one homomorphism from Y to X over G.

Let (Y, ψ) be a central extension of G, which is not perfect. Then $\pi_Y : Y \to Y^{\text{ab}} = Y/[Y, Y]$ is a nonzero homomorphism. Consider the central extension $\pi_G : G \times Y^{\text{ab}} \to G, (g, y) \mapsto g$. Define $f_1, f_2 : Y \to G \times Y^{ab}$ by $f_1 = \psi \times 1$ and $f_2 = \psi \times \pi_Y$.

$$f_1(y) = (\psi y, 1) \qquad f_2(y) = (\psi y, \pi_Y y)$$

These are two distinct homomorphisms $Y \to G \times Y^{\text{ab}}$ over G.



□

Lemma 5.5.11 (Milnor [10] 5.6)**.** *If (X, ϕ) is a central extension of a perfect group G. Let $X' = [X, X]$. Then $\phi|_{X'} : X' \to G$ is surjective, and X' is perfect. Thus, $(X', \phi|_{X'})$ is a perfect central extension of G.*

Proof. Since G is generated by commutators and $\phi : X \to G$ is surjective, it is immediate that $\phi : X' \to G$ is surjective. Now we just need to show that X' is perfect.

We claim that every element $x \in X$ can be written as $x = x'c$ with $x' \in X', c \in \text{center}(X)$. Let $x \in X$. By surjectivity of $\phi|_{X'}$, there is $x' \in X'$ with $\phi(x) = \phi(x')$. Then let $c = (x')^{-1}x \in \ker\phi \subset \text{center}(X)$, so we can write $x = x'c$ with $x' \in X', c \in \text{center}(X)$. Now, a generator $[x, y]$ of X' can be written as

$$[x, y] = [x'c, y'd] = [x', y']$$

with $x', y' \in X', c, d \in \text{center}(X)$. Thus X' is generated by its own commutators, so X' is perfect. □

Lemma 5.5.12 (roughly Milnor [10] page 45)**.** *Let (U, v) be a central extension of a group G, with U perfect. Then if (X, ϕ) is a central extension of U, the composition $v\phi : X \to G$ is a central extension of G.*

Proof. It suffices to show $\ker v\phi \subset Z(X)$. Let $x \in \ker(v\phi)$. Then $\phi x \in \ker v \subset \text{center}(U)$. Thus the map

$$\sigma_x : X \to X \qquad y \mapsto xyx^{-1}$$

is a homomorphism over U.

$$\phi\sigma_x(y) = \phi(xyx^{-1}) = (\phi x)(\phi y)(\phi x)^{-1} = (\phi y)(\phi x)(\phi x)^{-1} = \phi y$$

$$\begin{array}{ccc} X & \xrightarrow{\sigma_x} & X \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\phi} & \\ & U & \end{array}$$

Let $X' = [X, X]$ and consider $\sigma_x|_{X'}$. Since U is perfect, by Lemma 5.5.11, X' is perfect. Then by Lemma 5.5.9, there is a unique homomorphism $X' \to X'$ over U. Since the identity is such a map, by uniquess we have $\sigma_x|_{X'} = \text{Id}_{X'}$.

$$\begin{array}{ccc} X' & \xrightarrow{\sigma_x=\text{Id}} & X' \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\phi} & \\ & U & \end{array}$$

That is to say, $x \in \ker v\phi$ commutes with elements of X'. By a similar argument as before, we can write any element $y \in X$ as a product $y'c$ with $y' \in X'$ and $c \in \text{center}(X)$. Thus x commutes with any element of X, hence $x \in \text{center}(X)$.

$$x(y'c) = (y'x)c = (y'c)x$$

Thus $(X, v\phi)$ is a central extension of G. □

Lemma 5.5.13 (Milnor [10] page 45)**.** *Let (U, v) be a universal central extension of a group G. Then every central extension of U splits.*

Proof. By Lemma 5.5.10, U is perfect, so by Lemma 5.5.12 the $(X, v\phi)$ is a central extension of G. Now by universality of U, there is a unique homomorphism $s : U \to X$ over G. Then $\phi s : U \to U$ is a homomorphism over G, so by uniqueness $\phi s = \mathrm{Id}_U$.

$$\begin{array}{ccccc} U & \xrightarrow{s} & X & \xrightarrow{\phi} & U \\ & {\scriptstyle v}\searrow & \downarrow{\scriptstyle v\phi} & \swarrow{\scriptstyle v} & \\ & & G & & \end{array}$$

Thus s is a section of (X, ϕ), so it is split. □

Now we combine all of our lemmas together, and do a bit more work to get the final criterion for universality.

Theorem 5.5.14 (Milnor [10] 5.3)**.** *A central extension U of G is universal if and only if U is perfect and every central extension of U splits.*

Proof. Suppose (U, v) is a universal central extension of a group G. By Lemma 5.5.10, U is perfect, and by Lemma 5.5.13, every central extension of U splits. This completes one direction of the proof. All that remains to show is that if (U, v) is a central extension with U perfect and every central extension of U splits, then (U, v) is universal.

Let (U, v) be a central extension with U perfect, and suppose that every central extension of U splits. Let (X, ϕ) be a central extension of G. Form the pullback

$$U \times_G X = \{(u, x) \in U \times X : v(u) = \phi(x)\}$$

$$\begin{array}{ccc} U \times_G X & \xrightarrow{\pi_X} & X \\ \downarrow{\scriptstyle \pi_U} & & \downarrow{\scriptstyle \phi} \\ U & \xrightarrow{v} & G \end{array}$$

The $(U \times_G X, \pi_U)$ is a central extension of U, since

$$\begin{aligned} (u, x) \in \ker \pi_U &\implies u = 1 \\ &\implies v(u) = \phi(x) = 1 \\ &\implies x \in \ker \phi \subset \mathrm{center}(X) \\ &\implies (x, u) \in \mathrm{center}(U \times_G X) \end{aligned}$$

By hypothesis, every central extension of U splits. so there is a section $s : U \to U \times_G X$, so $s(u) = (u, hu)$ for some homomorphism $h : U \to X$. This h is the required homomorphism $U \to X$ over G.

$$\phi h(u) = \phi \pi_X(u, hu) = v\pi_U(u, hu) = v(u)$$

$$\begin{array}{ccc} U & \xrightarrow{\quad h \quad} & X \\ & {\scriptstyle v}\searrow \quad \swarrow{\scriptstyle \phi} & \\ & G & \end{array}$$

Since U is perfect, by Lemma 5.5.9, h is unique. □

Using group homology, we can give an alternate form of the previous criterion, which is sometimes easier to check.

Proposition 5.5.15 (Group homology criterion for universal central extension)**.** *Let G be a perfect group. A central extension E of G is universal if and only if $H_1(E,\mathbb{Z}) = H_2(E,\mathbb{Z}) = 0$.* [2]

Proof. By Theorem 5.5.14,

$$E \text{ is universal} \iff E \text{ is perfect and every central extension of } E \text{ splits}$$

By Corollary 3.6.9,

$$E \text{ is perfect} \iff H_1(E,\mathbb{Z}) = 0$$

By Corollaries 3.5.5 and 3.6.11,

$$\begin{aligned} \text{Every central extension of } E \text{ splits} &\iff H^2(E,A) = 0 \text{ for every trivial } E\text{-module } A \\ &\iff E^{\text{ab}} \text{ is free abelian and } H_2(E,\mathbb{Z}) = 0 \end{aligned}$$

From this it is clear that if E is the universal central extension, then $H_1(E,\mathbb{Z}) = H_2(E,\mathbb{Z}) = 0$. For the converse, if $H_1(E,\mathbb{Z}) = H_2(E,\mathbb{Z}) = 0$, then $E^{\text{ab}} = H_1(E,\mathbb{Z}) = 0$ is somewhat vacuously free abelian, hence by our equivalences E is universal. □

5.5.3 Criterion for existence of universal central extension

Now that we have a criterion for when an extension is universal, we can use it to say when exactly a group G has a universal central extension.

Perhaps this is too obvious to note, but there is no reason to expect that every group G has a universal central extension. First of all if G does, then G is a quotient of a perfect group, so G is perfect. It turns out that this one obvious necessary condition is also sufficient.

We begin with a few simple group-theoretic lemmas.

Lemma 5.5.16 (Commutator of normal subgroups is normal)**.** *Let G be a group, with H, K normal subgroups. Then $[H,K]$ is normal in G.*

Proof. It suffices to show that for $g \in G$, conjugating a generator of $[H,K]$ gives an element of $[H,K]$.

$$g[h,k]g^{-1} = ghkh^{-1}k^{-1}g^{-1} = (ghg^{-1})(gkg^{-1})(ghg^{-1})(gkg^{-1})$$

Since H, K are normal, $ghg^{-1} \in H$, etc. Thus this final product is a generator of $[H,K]$. □

Lemma 5.5.17 (Taking commutators commutes with taking quotients)**.** *Let G be a group with N a normal subgroup. Then $[G/N, G/N] = [G,G]/N$ (equality as subsets of G/N).*

Proof. The generators of $[G/N, G/N]$ are elements $[xN, yN]$ with $x, y \in G$. Generators of $[G,G]/N$ are $[x,y]N$. But these two types of generators are the same, because of how multiplication in G/N is defined. □

[2] $\mathbb{Z}$ is viewed as a trivial E-module.

With these two lemmas in hand, we can prove that our one necessary condition (being perfect) is also sufficient (to have a universal central extension).

Theorem 5.5.18 (Milnor [10] 5.7)**.** *A group G has a universal central extension if and only if G is perfect.*

Proof. One direction is immediate from our previous work, as we now describe. Suppose G has a universal central extension (U, v). We know U is perfect by Theorem 5.5.14, and $G \cong U/\ker v$ is a quotient of a perfect group, so G is perfect.

Conversely, suppose G is perfect. Choose a surjective group homomorphism ψ from a free group F onto G.

$$1 \longrightarrow \ker\psi \hookrightarrow F \xrightarrow{\psi} G \longrightarrow 1$$

Let $N = [\ker\psi, F]$. By Lemma 5.5.16, N is normal in F. Also, $N \subset \ker\psi$, since if $a \in \ker\psi, b \in F$, then

$$\psi[a,b] = (\psi a)(\psi b)(\psi a)^{-1}(\psi b)^{-1} = (\psi b)(\psi b)^{-1} = 1$$

Thus we have a surjection

$$\phi : F/N \to F/\ker\psi \cong G$$

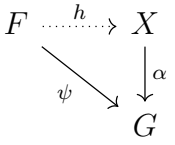
The kernel of ϕ is central. (Why? Let $\overline{x} \in \ker\phi$. Then it has a representative $x \in \ker\psi$. Then for $\overline{y} \in F/N$, we have

$$[\overline{x}, \overline{y}] = xyx^{-1}y^{-1}N = N$$

since $x \in \ker\psi$.) Then by Lemma 5.5.11, the commutator subgroup

$$(F/N)' = [F/N, F/N] = [F,F]/N$$

is a perfect central extension of G. The last equality is from Lemma 5.5.17. Finally, we show that the perfect central extension $[F,F]/N \to G$ is universal, by showing the universal property directly. Let (X, α) be a central extension of G. Since F is free, there exists a homomorphism $h : F \to X$ over G.



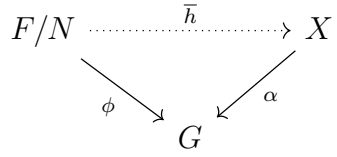
We claim that $h(N) = 1$. Take a generator of N, $[k, f]$ with $k \in \ker\psi, f \in F$. Then

$$1 = \psi(k) = \alpha h(k) \implies h(k) \in \ker\alpha \subset \text{center}(X)$$

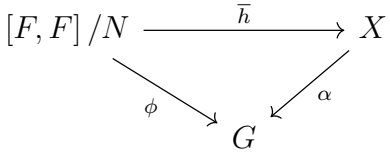
Thus

$$h[k,f] = [h(k), h(f)] = 1$$

Since $h(N) = 1$, h induces a homomorphism $\overline{h} : F/N \to X$ over G.



Then we restrict to $[F, F]/N$.



Thus the required homomorphism exists. It is unique by Lemma 5.5.9. □

5.5.4 Application - $\mathrm{K}_2(R) \cong H_2(\mathrm{E}(R), \mathbb{Z})$

Now we get to reap the benefits of our work with central extensions and extract information about K_2 from it.

Theorem 5.5.19 (Milnor [10] 5.1 or Rosenberg [13] 4.2.7)**.** $\mathrm{St}(R)$ *is the universal central extension of* $\mathrm{E}(R)$*.*

Proof. We already observed that $\mathrm{St}(n, R)$ is perfect, and similarly $\mathrm{St}(R)$ is perfect, as a consequence of the defining relations. Using our criterion, the theorem is true if we show the following.

1. $\ker \phi$, also know as $\mathrm{K}_2(R)$, is a central subgroup of $\mathrm{St}(R)$, so that $\mathrm{St}(R)$ is a central extension of $\mathrm{E}(R)$. We already mentioned this without proof as Theorem 5.5.1.

2. Every central extension of $\mathrm{St}(R)$ splits.

Both of these are doable, but take a few pages of proof. The proofs are not that interesting, though. It's mostly just playing with group relations. □

Next is the key result linking universal central extensions to group homology. As an immediate corollary, we will obtain an identification of $\mathrm{K}_2(R)$ with the homology group $H_2(E(R), \mathbb{Z})$.

Theorem 5.5.20 (Rosenberg [13] 4.1.19)**.** *Let G be a perfect group, and (E, ϕ) be the universal central extension with $N = \ker \phi$. Then $N \cong H_2(G, \mathbb{Z})$. Furthermore, under the isomorphisms*

$$\mathrm{Ext}(G, N) \cong H^2(G, N) \cong \mathrm{Hom}_{\mathbb{Z}}(H_2(G, \mathbb{Z}), N)$$

the class of the extension (E, ϕ) corresponds to an isomorphism $H_2(G, \mathbb{Z}) \xrightarrow{\cong} N$.

Proof. Let G, E, ϕ, N be as in the statement of the theorem, and let A be an abelian group, viewed as trivial module over E and G and N. Consider the inflation-restriction sequence (Proposition 3.9.20).

$$H^1(E,A) \xrightarrow{\text{Res}} H^1(N,A)^{E/N} \xrightarrow{\tau} H^2(E/N, A^N) \xrightarrow{\text{Inf}} H^2(E,A)$$

We simplify each term, from left to right.
(Term 1) Since E is perfect, $E^{\text{ab}} = 0$, and because A is a trivial E-module, by Proposition 3.2.7,

$$H^1(E,A) \cong \text{Hom}_{\mathbb{Z}}(E^{\text{ab}}, A) = 0$$

(Term 2) By the first isomorphism theorem, $E/N \cong G$, which acts trivially only $H^1(N,A)$, and since A is a trivial N-module, using Proposition 3.2.7 again,

$$H^1(N,A)^{E/N} = H^1(N,A) \cong \text{Hom}_{\mathbb{Z}}(N,A)$$

(Term 3) A is a trivial N-module so $A^N = A$, so $H^2(E/N, A^N) \cong H^2(G,A)$. Then since the SES of the universal coefficient theorem (3.6.10) is split,

$$H^2(G,A) \cong \text{Ext}^1_{\mathbb{Z}}(H_1(G,\mathbb{Z}),A) \oplus \text{Hom}_{\mathbb{Z}}(H_2(G,\mathbb{Z}),A)$$

Since G is perfect and $G^{\text{ab}} = 0$, since $H_1(G,\mathbb{Z}) \cong \text{Hom}_{\mathbb{Z}}(G^{\text{ab}}, A)$ (Proposition 3.2.7 again) is zero, so the Ext^1 term vanishes, and

$$H^2(E/N, A^N) \cong H^2(G,A) \cong \text{Hom}_{\mathbb{Z}}(H_2(G,\mathbb{Z},A))$$

(Term 4) Since E is universal, every central extension of E splits by Theorem 5.5.14, so by Corollary 3.5.5, $H^2(E,A) = 0$. After all these substitutions, the exact sequence becomes

$$0 \longrightarrow \text{Hom}_{\mathbb{Z}}(N,A) \xrightarrow{\cong} \text{Hom}_{\mathbb{Z}}(H_2(G,\mathbb{Z}),A) \longrightarrow 0$$

Since A was an arbitrary abelian group, these isomorphism together with the Yoneda lemma imply $N \cong H_2(G,\mathbb{Z})$.

To prove the second claim of the theorem, that the extension E corresponds to an isomorphism $H_2(G,\mathbb{Z}) \to N$, requires tracing the construction of the transgression map τ of the inflation-restriction sequence, see Theorems 4.1.19, 4.1.20 of Rosenberg [13] for details on this. □

Corollary 5.5.21 (Rosenberg [13] 4.2.10)**.** *Let R be a commutative ring with unity. Then*

$$\text{K}_2(R) \cong H_2(\text{E}(R), \mathbb{Z})$$

Proof. By Theorem 5.5.19, $\text{St}(R)$ is the universal central extension of $\text{E}(R)$, and by definition, $\text{K}_2(R)$ is the kernel.

$$1 \to \text{K}_2(R) \hookrightarrow \text{St}(R) \xrightarrow{\phi} \text{E}(R) \to 1$$

Thus by Theorem 5.5.20,

$$\text{K}_2(R) \cong H_2(\text{E}(R), \mathbb{Z})$$

□

Having accomplished all that we set out to do in identifying $\mathrm{K}_2(R)$ with $H_2(\mathrm{E}(R), \mathbb{Z})$, we now ask, what does this give us? Can we say anything about the homology group which we did not know about $\mathrm{K}_2(R)$? Not at this point, unfortunately. Even if R is a field, $\mathrm{E}(R)$ may still be a complicated group, and computing H_2 groups, even with coefficients in $\mathbb{Z}$, is not trivial. But it is a good start.

5.6 K_2 of a field

We have been rather down on the possibility of computing K_2 of a field using simple tools, but this does actually turn out to be mostly doable, though the process of getting there is not especially pretty. Following Milnor [10] (who is presenting work of Matsumoto), we embark on a process of computing K_2 of a field, involving a lot of work with Steinberg group relations and defining some objects called Steinberg symbols.

The outcome of all of this is eventually Matsumoto's theorem, which describes K_2 of a field in terms of generators and relations. This presentation is useful enough to compute K_2 explicitly in at least one case - for a finite field, all of the generators vanish, so K_2 of a finite field is the trivial group.

5.6.1 Generation of $\mathrm{K}_2 F$ by symbols

This section mostly follows the presentation in Chapter 9 of Milnor [10]. The important results are Corollary 5.6.14, Theorem 5.6.17, and Theorem 5.6.18, everything else is technical and involves machinery/notation which can mostly be discarded after obtaining the results. Consequently, all of the intermediate proofs (which just involve algebraic manipulation) are omitted. This is not to say the proofs are easy or short, but they are mostly tedious.

In this section with work with arbitrary associative rings with unity, which we denote by Λ, not necessarily commutative. We will work in $\mathrm{St}(n, \Lambda)$ with $n \geq 3$. Recall that $\mathrm{St}(n, \Lambda)$ is generated by elements x_{ij}^{λ} for $1 \leq i, j \leq n, i \neq j, \lambda \in \Lambda$. We denote the canonical homomorphism $\mathrm{St}(n, \Lambda) \to \mathrm{GL}(n, \Lambda), x_{ij}^{\lambda} \mapsto e_{ij}^{\lambda}$ by ϕ.

Definition 5.6.1. For a unit $u \in \Lambda^{\times}$, define

$$w_{ij}(u) = x_{ij}^{u} x_{ji}^{-u^{-1}} x_{ij}^{u} \qquad h_{ij}(u) = w_{ij}(u) w_{ij}(-1)$$

These are defined in this way so that the images of $w_{ij}(u)$ and $h_{ij}(u)$ in $\mathrm{GL}(n, \Lambda)$ have the following somewhat simple forms.

$$\phi\big(w_{ij}(u)\big) = e_{ij}^{u} e_{ji}^{-u^{-1}} e_{ij}^{u} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & \dots & u & & \\ & & \vdots & \ddots & \vdots & & \\ & & -u^{-1} & \dots & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

where unmarked entries along the diagonal are 1, and all other unmarked entries are zero. The u occurs in the ijth entry, and the $-u^{-1}$ occurs in the jith entry. Similarly,

$$\phi\big(h_{ij}(u)\big) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & u & & & & \\ & & & \ddots & & & \\ & & & & -u^{-1} & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

where the u occurs in the iith entry, and the $-u^{-1}$ occurs in the jjth entry.

Lemma 5.6.2 (Properties of $w_{ij}(u)$, $h_{ij}(u)$, Milnor [10] 9.5, 9.6, 9.10)**.** *Let $u, v \in \Lambda^\times$.*

- $w_{ij}(u)w_{ij}(-u) = 1$
- $h_{ij}(1) = 1$
- $w_{ij}(u) = w_{ji}(-u^{-1})$
- $[h_{12}(u), h_{13}(v)] = h_{13}(uv)h_{13}(u)^{-1}h_{13}(v)^{-1}$
- *All $h_{ij}(u)$ can be written as a product of $h_{1k}(v)$ for various k, v. Furthermore, they satisfy relations*

$$h_{ij}(u)h_{ji}(u) = 1 \qquad h_{ij}(u)^{-1}h_{jk}(u)^{-1}h_{ki}(u)^{-1} = 1$$

Definition 5.6.3. $W \subset \mathrm{St}(n, \Lambda)$ is the subgroup generated by all $w_{ij}(u)$ for $1 \leq i, j \leq n$, $i \neq j, u \in \Lambda^\times$.

Definition 5.6.4. A matrix in $\mathrm{GL}(n, \Lambda)$ is a **monomial matrix** if it can be written as a product PD where P is a permutation matrix and D is a diagonal matrix. (Recall: A permutation matrix has one 1 in each row and column, and zeroes elsewhere.)

Lemma 5.6.5 (Milnor [10] 9.1)**.** *If Λ is commutative, then the image of $\phi|_W : W \to \mathrm{GL}(n, \Lambda)$ is exactly the set of all monomial matrices with determinant one.*

Lemma 5.6.6 (Milnor [10] 9.2)**.** *Let $w \in W$. The conjugation map*

$$\mathrm{St}(n, \Lambda) \to \mathrm{St}(n, \Lambda) \qquad x \mapsto wxw^{-1}$$

takes every generator x_{ij}^λ to another generator. (See Corollary 5.6.10 for more precise statement.)

Definition 5.6.7. Let $\phi : \mathrm{St}(n, \Lambda) \to \mathrm{GL}(n, \Lambda)$ be the canonical homomorphism. We define $C_n = \ker(\phi|_W)$.

Corollary 5.6.8 (Milnor [10] 9.3)**.** *C_n is contained in the center of $\mathrm{St}(n, \Lambda)$.*

Proof. Immediate consequence of Lemma 5.6.6. □

Definition 5.6.9. For a permutation $\pi \in S_n$ and $i, j \in \{1, \ldots, n\}$, we use the shorthand $\pi(ij) = \pi(i), \pi(j)$. For example, instead of $h_{\pi(i),\pi(j)}(u)$ we write $h_{\pi(ij)}(u)$.

Corollary 5.6.10 (Milnor [10] 9.4)**.** *Let $w \in W$. We may uniquely express $\phi(w)$ as a product PD, with P a permutation matrix and $D = \operatorname{diag}(v_1, \ldots, v_n)$ a diagonal matrix. Let $\pi \in S_n$ be the permutation corresponding to P. Then*

$$\begin{aligned} w x_{ij}^{\lambda} w^{-1} &= x_{\pi(ij)}^{v_i \lambda v_j^{-1}} \\ w w_{ij}(u) w^{-1} &= x_{\pi(ij)}^{v_i u v_j^{-1}} \\ w h_{ij}(u) w^{-1} &= h_{\pi(ij)}(v_i u v_j^{-1}) h_{\pi(ij)}(v_i v_j^{-1})^{-1} \end{aligned}$$

Definition 5.6.11. Let Λ be a commutative ring. The **symbol** map is

$$\{,\} : \Lambda^\times \times \Lambda^\times \to \mathrm{K}_2 \Lambda \qquad \{u, v\} = [h_{ij}(u), h_{ik}(v)] = h_{ik}(uv) h_{ik}(u)^{-1} h_{ik}(v)^{-1}$$

for $i \neq j, i \neq k, j \neq k$. Note that this does not depend on the choice of indices i, j, k due to the last two properties of Lemma 5.6.2. Also note that this agrees with the definition of symbols in Chapter 8 of Milnor [10], because $\phi(h_{12}(u)) = D_u$ and $\phi(h_{13}(v) = D'_v$ (see Definition 5.6.1).

Lemma 5.6.12 (Milnor [10] 9.7)**.** *Let Λ be a commutative ring. Then symbol defined above is skew symmetric and bimultiplicative. Furthermore, the image is contained in $C_n = \ker(\phi|_W)$.*

Just for clarification, we return to not assuming Λ is commutative.

Lemma 5.6.13 (Milnor [10] 9.8)**.** *For any unit $u \in \Lambda^\times$, $\{u, -u\} = 1$. If $u, 1-u \in \Lambda^\times$, then $\{u, 1-u\} = 1$.*

Corollary 5.6.14 (Symbols vanish in a finite field, Milnor [10] 9.9)**.** *If Λ is a finite field, or if $\Lambda = \mathbb{Z}/p^n\mathbb{Z}$ for a prime p with p an odd prime, then $\{u, v\} = 1$ for all u, v.*

Lemma 5.6.15 (Milnor [10] 9.14 and 9.15)**.** *Let $T \subset \mathrm{St}(n, \Lambda)$ be the subgroup generated by all x_{ij}^{λ} with $i < j$.*

1. *Every element of T can be written as a product*

$$\prod_{i<j} x_{ij}^{\lambda(ij)}$$

with the factors arranged in lexicographic order. (This is a straightforward consequence of Steinberg relations.)

2. *As a consequence of (1), ϕ maps T isomorphically onto the group of upper triangular unipotent subgroup of $\mathrm{GL}(n, \Lambda)$. ("Unipotent" means 1's along the diagonal.)*

3. *If Λ is a division ring, then $\mathrm{St}(n, \Lambda) = TWT$. (Obviously $TWT \subset \mathrm{St}(n, \Lambda)$, so the content of this assertion is just the reverse inclusion.)*

Recall that $C_n = \ker(\phi|_W) \subset \mathrm{St}(n, \Lambda)$. We can also write this as $W \cap \ker \phi$.

Theorem 5.6.16 (Milnor [10] 9.11)**.** *Let Λ be a commutative ring. Then C_n is generated by symbols $\{u, v\}$.*

Theorem 5.6.17 (Milnor [10] 9.12)**.** *If Λ is a division ring, then $\ker \phi \subset W$, so $\ker \phi = C_n$. Thus $\mathrm{St}(n, \Lambda)$ is a central extension of $\mathrm{E}(n, \Lambda)$ for $n \geq 3$.*

Theorem 5.6.18 ($\mathrm{K}_2 F$ is generated by symbols, Milnor [10] 9.13)**.** *If Λ is a field, then $\mathrm{K}_2 \Lambda$ is generated by symbols $\{u, v\}$. In particular, if Λ is a finite field, then $\mathrm{K}_2 \Lambda$ is trivial (by 5.6.14).*

Proof. Immediate consequence of Theorems 5.6.17 and 5.6.16. □

The next proposition gives some more details on why K_2 vanishes for a finite field.

Proposition 5.6.19. *Let $\mathbb{F}_q$ be the finite field with q elements.*

1. *If q is odd, there exists $u \in \mathbb{F}_q^\times$ such that u and $1 - u$ are both not squares.*
2. *If α is a generator of $\mathbb{F}_q^\times$, then $\{\alpha, \alpha\}$ is trivial.*
3. *For any $u, v \in \mathbb{F}_q^\times$, $\{u, v\}$ is trivial.*
4. *$K_2(\mathbb{F}_q)$ is trivial.*

Proof. (1) Note that $\mathbb{F}_q^\times$ is cyclic of order $q - 1$. Let α be a generator. Since $q - 1$ is even, half of the elements of $\mathbb{F}_q^\times$ are squares $(1, \alpha^2, \alpha^4, \ldots, \alpha^{q-3})$ and half are not squares $(\alpha, \alpha^3, \ldots, \alpha^{q-2})$. Consider the bijection

$$\mathbb{F}_q \to \mathbb{F}_q \qquad u \mapsto 1 - u$$

This maps 0 to 1 and 1 to 0, so we have a bijection

$$\mathbb{F}_q \setminus \{0, 1\} \to \mathbb{F}_q \setminus \{0, 1\} \qquad u \mapsto 1 - u$$

Suppose there is no u such that u and $1 - u$ are both not squares. Then under this bijection, all of the $\frac{q-1}{2}$ non-squares get mapped to squares. But one of the squares in $\mathbb{F}_q^\times$ is 1, so there are only $\frac{q-1}{2} - 1$ squares in $\mathbb{F}_q \setminus \{0, 1\}$, so this is impossible. Thus there does exist $u \in \mathbb{F}_p^\times$ such that $u, 1 - u$ are both not squares.

(2) Let α be a generator of $\mathbb{F}_q^\times$. Note that since the symbol is anti-commutative,

$$\{\alpha, \alpha\}^2 = 1$$

Also note that

$$\{\alpha, \alpha\}^{q-1} = \left\{\alpha^{q-1}, \alpha\right\} = \{1, \alpha\} = 1$$

If q is even (so $q - 1$) is odd, this says that $\{\alpha, \alpha\}$ to an odd and even power are trivial, so it must be trivial. If q is odd, by (1) we can choose $u \in \mathbb{F}_q^\times$ such that $u, 1 - u$ are both not squares, so $u = \alpha^i, 1 - u = \alpha^j$ with i, j odd. Then

$$1 = \{u, 1 - u\} = \left\{\alpha^i, \alpha^j\right\} = \{\alpha, \alpha\}^{ij}$$

so once again $\{\alpha, \alpha\}$ to an odd power (namely ij) is trivial. Since it also squares to 1, it is trivial.

(3) Let $u, v \in \mathbb{F}_q^\times$. Then write them as powers of a generator $u = \alpha^i, v = \alpha^j$. Then by the symbol relations,

$$\{uv\} = \left\{\alpha^i, \alpha^j\right\} = \{\alpha, \alpha\}^{ij}$$

which is trivial by (2).

(4) This is immediate from (3) and the fact that symbols generate $K_2(K)$ for any field K. □

5.6.2 Matsumoto's theorem

Finally we give a precise statement of Matsumoto's theorem, which gives a presentation of $\mathrm{K}_2 F$ for a field F. We do not prove it here.

Theorem 5.6.20 (Matsumoto's theorem)**.** *Let F be a field. The abelian group $\mathrm{K}_2 F$ has a presentation with generators $\{x, y\}$ for $x, y \in F^\times$ and relations*

$$\begin{aligned} \{x, 1-x\} &= 1 && \text{for } x \neq 0, 1 \\ \{x_1 x_2, y\} &= \{x_1, y\}\{x_2, y\} \\ \{x, y_1 y_2\} &= \{x, y_1\}\{x, y_2\} \end{aligned}$$

Remark 5.6.21 (Milnor [10] 11.2)**.** By 5.6.16, the kernel C_n of $\mathrm{St}(n, F) \to \mathrm{SL}(n, F)$ is generated by the symbols $\{u, v\}$, which satisfy the relations of 5.6.20. Thus by 5.6.20, there is a canonical surjection $\mathrm{K}_2 F \to C_n$, defined by sending a generator $\{u, v\}$ to itself.

Since $\mathrm{K}_2 \Lambda$ is the direct limit over n of the C_n, the universal property of the direct limit gives a map $C_n \to \mathrm{K}_2 \Lambda$, and by uniqueness considerations, these maps must be inverses. Thus $C_3, C_4, C_5, \ldots$ are all canonically isomorphic to each other and to the direct limit $\mathrm{K}_2 \Lambda$.

5.6.3 Steinberg symbols

Since the symbol map $\{,\}$ was so crucial in describing K_2 of a field, we make some abstract definitions generalizing a map with the same properties, and some properties such maps always have.

Definition 5.6.22. Let F be a field and A an abelian group, written multiplicatively. A **Steinberg symbol** on F with values in A is a bimultiplicative map $c : F^\times \times F^\times \to A$ satisfying $c(x, 1-x) = 1$.

Corollary 5.6.23 (Milnor [10] 11.3)**.** *If c is a Steinberg symbol on F with values in A, there is a unique homomorphism $\mathrm{K}_2 F \to A$ so that $\{x, y\} \mapsto c(x, y)$ for all $x, y \in F^\times$.*

Proof. This is just the case $n = 2$ of Remark 5.7.7. □

Lemma 5.6.24 (Properties of Steinberg symbols)**.** *Let $c : F^\times \times F^\times \to A$ be a Steinberg symbol.*

$c(xy,z) = c(x,z)c(y,z)$	bimultiplicative, by definition
$c(x,yz) = c(x,y)c(x,z)$	bimultiplicative by definition
$c(x,1-x) = 1$	by definition
$c(x,1) = c(1,x) = 1$	consequence of bimultiplicative
$c\left(x,y^{-1}\right) = c(x,y)^{-1} = c\left(x^{-1},y\right)$	consequence of bimultiplicative
$c\left(x^{-1},y^{-1}\right) = c(x,y)$	consequence of bimultiplicative
$c(x,-x) = 1$	see Milnor[*10*] page 95
$c(x,y) = c(y,x)^{-1}$	see Milnor[*10*] page 95
$x+y=1 \implies c(x,y)=1$	because $c(x,1-x)=1$
$c(x,-1)^2 = 1$	consequence of bimultiplicative

5.6.4 Tate's computation of $\mathrm{K}_2\,\mathbb{Q}$

At this point, we have Matsumoto's presentation of $\mathrm{K}_2(F)$, and we can use it to explicitly determine $\mathrm{K}_2(F)$ in the case where F is finite. This presentation is also sufficient to explicitly describe $\mathrm{K}_2(\mathbb{Q})$, though it takes more work, and we omit many of the details.

Definition 5.6.25. A **discrete valuation** v on a field K is a group homomorphism $v : K^\times \to \mathbb{Z}$, satisfying

$$v(x+y) \geq \min\Big(v(x), v(y)\Big)$$

It is often convenient to extend v to $K \to \mathbb{Z} \cup \{\infty\}$ by setting $v(0) = \infty$. The associated discrete valuation ring is

$$\mathcal{O}_K = \big\{x \in K^\times : v(x) \geq 0\big\} \cup \{0\} = \{x \in K : v(x) \geq 0\}$$

which has unique maximal ideal

$$\mathfrak{m} = \big\{x \in K^\times : v(x) > 0\big\} \cup \{0\} = \{x \in K : v(x) > 0\}$$

The quotient $\mathcal{O}_K/\mathfrak{m}$ is the **residue class field** of K.

Definition 5.6.26. Let v be a discrete valuation on a field K, with residue class field $k = \mathcal{O}_K/\mathfrak{m}$. The associated **tame symbol** is $d_v : K^\times \times K^\times \to k^\times$ is

$$d_v(x,y) = (-1)^{v(x)v(y)}\frac{x^{v(y)}}{y^{v(x)}}$$

Note that d_v is a Steinberg symbol (Milnor [10] 11.5).

Definition 5.6.27. For a prime $p \in \mathbb{Z}$ with $p \geq 3$, let v_p be the p-adic valuation on $\mathbb{Q}$. To economize on notation, we denote $d_{v_p}(x,y)$ by $(x,y)_p$. Note that $(x,y)_p$ takes values in $(\mathbb{Z}/p\mathbb{Z})^\times$ (for $p \geq 3$).

In the case $p = 2$, we define $(x, y)_2$ as follows. Any nonzero rational can be written uniquely in the form $(-1)^i 2^j 5^k u$ where $k = 0, 1$ and u is a quotient of integers congruent to 1 modulo 8. Then define

$$\left((-1)^i 2^j 5^k u, (-1)^I 2^J 5^K u'\right)_2 = (-1)^{iI+jK+kJ}$$

This is in fact a well defined Steinberg symbol. Note that $(x, y)_2$ takes values in $\{\pm 1\}$.

Definition 5.6.28. We denote the target of $(x, y)_p$ by A_p, so we have $A_2 = \{\pm 1\}$, and for $p \geq 3$, $A_p = (\mathbb{Z}/p\mathbb{Z})^\times$.

Theorem 5.6.29 (Milnor [10] 11.6, due to Tate)**.** *The map*

$$\mathrm{K}_2 \mathbb{Q} \to A_2 \oplus A_3 \oplus A_5 \oplus \dots \qquad \{x, y\} \mapsto (x, y)_2 \oplus (x, y)_3 \oplus (x, y)_5 \oplus \dots$$

is an isomorphism of abelian groups.

For an alternate description of the previous theorem, see Rosenberg Theorem 4.4.9 [13].

5.7 Milnor K-theory

In this section we discuss Milnor's attempt to define higher K-groups for fields by generalizing the presentation given by Matsumoto in the calculation of $K_2 F$. The higher Milnor K-groups are NOT isomorphic to the higher K-groups defined by Quillen, but much simpler to define and work with. Also, there is a homomorphism from Milnor's $\mathrm{K}_n F$ to Quillen's $\mathrm{K}_n F$, which is an isomorphism for $n = 0, 1, 2$. [3]

The presentation follows section 1.2 of Fesenko `https://www.maths.nottingham.ac.uk/plp/pmzibf/book/ch9n.pdf`.

Definition 5.7.1. Let F be a field, and for $n \in \mathbb{Z}_{\geq 1}$ consider the n-fold tensor product

$$T^n = F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times$$

We write T^n multiplicatively (even though tensor products are typically written additively), so that

$$(\alpha_1 \otimes \cdots \otimes \alpha_i \otimes \cdots \otimes \alpha_n)(\alpha_1 \otimes \cdots \otimes \beta_i \otimes \cdots \otimes \alpha_n) = \alpha_1 \otimes \cdots \otimes \alpha_i \beta_i \otimes \cdots \otimes \alpha_n$$

[4] Let $I_n \subset T^n$ be the subgroup generated by elements

$$\alpha_1 \otimes \cdots \otimes \alpha_n$$

with $\alpha_i + \alpha_j = 1$ for some $i \neq j$. Then **nth Milnor K-group** of F is the quotient $\mathrm{K}_n^M(F) = T^n / I_n$. We also set $\mathrm{K}_0^M F = \mathbb{Z}$. (This makes sense since $\mathrm{K}_0 F \cong \mathbb{Z}$, see example 5.1.11).

[3] `https://en.wikipedia.org/wiki/Milnor_K-theory`

[4] If we write T^n additively instead, this relation looks like

$$(\alpha_1 \otimes \cdots \otimes \alpha_i \otimes \cdots \otimes \alpha_n) + (\alpha_1 \otimes \cdots \otimes \beta_i \otimes \cdots \otimes \alpha_n) = \alpha_1 \otimes \cdots \otimes (\alpha_i + \beta_i) \otimes \cdots \otimes \alpha_n$$

Definition 5.7.2. The image of $\alpha_1 \otimes \cdots \otimes \alpha_n \in \mathrm{K}_n^M F$ is a **symbol** and written $\{\alpha_1, \ldots, \alpha_n\}$. By definition, the symbols generated $\mathrm{K}_n^M F$, which is the generalization of our known fact that symbols $\{x, y\}$ generate $\mathrm{K}_2 F$ (Theorem 5.6.18). By definition, the symbols satisfy the relations [5]

$$\begin{aligned} \{\alpha_1, \ldots, \alpha_n\} &= 1 \qquad \text{if } \alpha_i + \alpha_j = 1 \text{ for some } i \neq j \\ \{\ldots, \alpha\beta, \ldots\} &= \{\ldots, \alpha, \ldots\}\{\ldots, \beta, \ldots\} \end{aligned}$$

Remark 5.7.3. By Matsumoto's theorem, $\mathrm{K}_2^M F \cong \mathrm{K}_2 F$, since Matsumoto showed that $\mathrm{K}_2 F$ is generated by elements $\{x, y\}$ for $x, y \in F^\times$ with the same relations. Also note that $\mathrm{K}_1^M F \cong \mathrm{K}_1 F$, since in this case $T^n = \mathbb{F}^\times, I_n = 0$ so $\mathrm{K}_1^M F \cong F^\times$, and by example 5.2.7, $\mathrm{K}_1 F \cong F^\times$ also.

Lemma 5.7.4. *Symbols satsify the relations*

$$\begin{aligned} \{\alpha_1^m, \alpha_2, \ldots, \alpha_n\} &= \{\alpha_1, \ldots, \alpha_n\}^m \qquad \text{for all } m \in \mathbb{Z} \\ \{\alpha_1, \ldots, \alpha_n\} &= 1 \qquad \text{if } \alpha_i = 1 \text{ for some } i \end{aligned}$$

Proof. The first is an immediate consequence of multiplicativity. The second is a consequence of the first, as

$$\begin{aligned} \{\ldots, 1, \ldots\} &= \{\ldots, xx^{-1}, \ldots, \} = \{\ldots, x, \ldots\}\{\ldots, x^{-1}, \ldots\} \\ &= \{\ldots, x, \ldots\}\{\ldots, x, \ldots\}^{-1} = 1 \end{aligned}$$

□

Definition 5.7.5. For $n, m \in \mathbb{Z}_{\geq 1}$, the usual "concatenation" map

$$T^n \otimes_{\mathbb{Z}} T^m \to T^{n+m} \qquad (\alpha_1 \otimes \cdots \alpha_n) \otimes (\alpha_{n+1} \otimes \cdots \otimes \alpha_m) \mapsto \alpha_1 \otimes \cdots \otimes \alpha_m$$

induces a map [6]

$$\mathrm{K}_n^M F \otimes_{\mathbb{Z}} \mathrm{K}_m^M F \to \mathrm{K}_{n+m}^M F \qquad \{\alpha_1, \cdots, \alpha_n\} \otimes \{\alpha_{n+1}, \cdots, \alpha_m\} \mapsto \{\alpha_1, \cdots, \alpha_m\}$$

Also in the case $n = 0$ or $m = 0$ we have the usual $\mathbb{Z}$-actions on $\mathrm{K}_n^M F$ or $\mathrm{K}_m^M F$ respectively, so taking this all together, we have made a graded ring

$$\mathrm{K}^M F = \bigoplus_{n \geq 0} \mathrm{K}_n^M F$$

called the **Milnor ring** of the field F.

[5] If we write these relations additively, they look like

$$\begin{aligned} \{\alpha_1, \ldots, \alpha_n\} &= 0 \qquad \text{if } \alpha_i + \alpha_j = 1 \text{ for some } i \neq j \\ \{\ldots, \alpha\beta, \ldots, \} &= \{\ldots, \alpha, \ldots\} + \{\ldots, \beta, \ldots\} \end{aligned}$$

[6] There is some checking here that various things satisfy needed relations, but this is not especially interesting to work out.

Definition 5.7.6. Let F be a field and A an abelian group, written multiplicatively. A **generalized Steinberg symbol** on F, also called a **Steinberg cocycle** or **n-symbolic map** is a map

$$c : \prod_{i=1}^{n} F^\times \to A$$

such that

$$\begin{aligned} c(\ldots, xy, \ldots) &= c(\ldots, x, \ldots) \cdot c(\ldots, y, \ldots) \\ c(x_1, \ldots, x_n) &= 1 \qquad\qquad \text{if } x_i + x_j = 1 \text{ for some } i \neq j \end{aligned}$$

The first property is called **(multi)-multiplicativity** and the second property is called the **Steinberg property**. Alternately, we may bake in the multiplicativity property by requiring that c be a map

$$c : (F^\times)^{\otimes n} \to A$$

in which case c just needs to satisfy the Steinberg property. We will also call such a map an n-symbolic map.

Remark 5.7.7. Let c be an n-symbolic map on a field F. By multiplicativity, c induces a map on $T^n = \bigotimes_{i=1}^n F^\times$, and by the Steinberg property, it vanishes on I_n, so c induces

$$\mathrm{K}_n^M F \to A \qquad \{x_1, \ldots, x_n\} \mapsto c(x_1, \ldots, x_n)$$

Since the symbols generate $\mathrm{K}_n^M F$, this extends uniquely to a map on all of $\mathrm{K}_n^M F$.

5.7.1 K_2 of an algebraically closed field

We continue to follow Fesenko's notes `https://www.maths.nottingham.ac.uk/plp/pmzibf/book/ch9n.pdf` to show that if F is an algebraically closed field, then $\mathrm{K}_2 F$ is divisible.

Definition 5.7.8. Let A be an abelian group written additively, and let $n \in \mathbb{Z}$, and consider the multiplication-by-n-map $n : A \to A, a \mapsto na$. If A is written multiplicatively, it is more appropriate to call this the nth-power-map and write it $n : A \to A, a \mapsto a^n$.

A is **n-divisible** if $n : A \to A$ is surjective. A is **uniquely n-divisible** if $n : A \to A$ is an isomorphism. A is **divisible** if it is n-divisible for all $n \in \mathbb{Z}_{\geq 1}$. A is **uniquely divisible** if it is uniquely n-divisible for all $n \in \mathbb{Z}_{\geq 1}$.

Proposition 5.7.9. *Let F be a field and $m \in \mathbb{Z}_{\geq 1}$ such that $F^\times = F^{\times m}$, and also suppose that either* $\operatorname{char} F = m$ *or the group of mth roots of unity $\mu_m \subset F^{\mathrm{sep}}$ is contained in F. Then $\mathrm{K}_n^M F$ is uniquely m-divisible.*

Proof. Define

$$f_m : \prod_{i=1}^{n} F^\times \to \mathrm{K}_n^M F \qquad (\alpha_1, \ldots, \alpha_n) \mapsto \{\beta_1, \alpha_2, \ldots, \alpha_n\}$$

where $\beta_1 \in F^\times$ satisfies $\beta_1^m = \alpha_1$. To verify that this is well defined, suppose $\gamma_1 \in F^\times$ is also an mth root of α_1, $\gamma_1^m = \alpha_1$. Then

$$\left(\beta_1\gamma_1^{-1}\right)^m = \beta_1^m\gamma_1^{-m} = \alpha_1\alpha_1^{-1} = 1$$

so $\beta_1\gamma_1^{-1} = \zeta$ is an mth root of unity. Now choose $\beta_2 \in F^\times$ so that $\alpha_2 = \beta_2^m$. Then using Lemma 5.7.4 a few times,

$$\begin{aligned}
\{\beta_1, \alpha_2, \ldots, \alpha_n\} &= \{\gamma_1\zeta, \alpha_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \alpha_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \beta_2^m, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta, \beta_2, \ldots, \alpha_n\}^m \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}\{\zeta^m = 1, \beta_2, \ldots, \alpha_n\} \\
&= \{\gamma_1, \alpha_2, \ldots, \alpha_n\}
\end{aligned}$$

Thus f_m is well defined. Now we claim that f_m is an n-symbolic map. It is clear that f_m is multiplicative with respect to the arguments $\alpha_2, \ldots, \alpha_n$. It is also multiplicative with respect to the 1st argument, since if $\beta_1^m = \alpha_1, (\beta_1')^m = \alpha_1'$, then $(\beta_1\beta_1')^m = \alpha_1\alpha_1'$ and so

$$\begin{aligned}
f_m(\alpha_1\alpha_1', \alpha_2, \ldots, \alpha_n) &= \{\beta_1\beta_1', \ldots, \alpha_n\} \\
&= \{\beta_1, \ldots, \alpha_n\}\{\beta_1', \ldots, \alpha_n\} \\
&= f_m(\alpha_1, \ldots, \alpha_n) f_m(\alpha_1', \ldots, \alpha_n)
\end{aligned}$$

If $\alpha_i + \alpha_j = 1$ for some $i \neq j$, and $i, j \neq 1$, then it is clear from the definition of f that $f_m(\alpha_1, \ldots, \alpha_n) = 1$. If $\alpha_1 + \alpha_j = 1$ for some $j \neq 1$, choose β_1 so that $\beta_1^m = \alpha_1$, and then we need to consider the cases (1) $\operatorname{char} F = m$ and (2) $\mu_m \subset F$ separately. In case (1) where $\operatorname{char} F = m$, we get

$$\alpha_j = 1 - \alpha_1 = 1 - \beta_1^m = (1 - \beta_1)^m$$

hence

$$f_m(\alpha_1, \ldots, \alpha_j, \ldots) = \{\beta_1, \ldots, (1-\beta_1)^m, \ldots\} = \{\beta_1, \ldots, 1-\beta_1, \ldots\}^m = 1$$

since $\beta_1 + (1 - \beta_1) = 1$. So in case (1), f_m has the Steinberg property. In case (2), let $\zeta \in F$ be a primitive mth root of unity. Then

$$\alpha_j = 1 - \alpha_1 = 1 - \beta_1^m = \prod_{k=1}^{m}(1 - \zeta^k\beta_1)$$

Note that

$$1 = \left\{\zeta^k\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} = \left\{\zeta^k, \ldots, 1 - \zeta^k\beta_1, \ldots\right\}\left\{\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} \tag{5.7.1}$$

$$\implies \left\{\beta_1, \ldots, 1 - \zeta^k\beta_1, \ldots\right\} = \left\{\zeta^k, \ldots, 1 - \zeta^k\beta_1, \ldots\right\}^{-1} \tag{5.7.2}$$

Then using equation 5.7.2

$$f_m(\alpha_1,\ldots,\alpha_j,\ldots) = \left\{\beta_1,\ldots,\prod_k(1-\zeta^k\beta_1),\ldots\right\}$$
$$= \prod_k \left\{\beta_1,\ldots,1-\zeta^k\beta_1,\ldots\right\} = \prod_k \left\{\zeta^k,\ldots,1-\zeta^k\beta_1,\ldots\right\}^{-1}$$

Now choose δ_k so that $\delta_k^m = 1-\zeta^k\beta_1$. Then we continue our equalities.

$$f_m(\alpha_1,\ldots,\alpha_j,\ldots) = \prod_k \left\{\zeta^k,\ldots,\delta_k^m,\ldots\right\}^{-1} = \prod_k \left\{\zeta^k,\ldots,\delta_k,\ldots,\right\}^{-m}$$
$$= \prod_k \left\{(\zeta^k)^m,\ldots,\delta_k,\ldots\right\}^{-1} = \prod_k \left\{1,\ldots,\delta_k,\ldots,\right\}^{-1} = \prod_k 1 = 1$$

So in case (2), f_m has the Steinberg property. Hence in either case, f_m is an n-symbolic map, and induces the group homomorphism

$$\widetilde{f}_m : \mathrm{K}_n^M F \to \mathrm{K}_n^M F \qquad \{\alpha_1,\ldots,\alpha_n\} \mapsto \{\beta_1,\ldots,\alpha_n\}$$

where $\beta_1^m = \alpha_1$, which is inverse to m-power-map, since

$$(\widetilde{f}_m \circ m)\{\alpha_1,\ldots,\alpha_n\} = \widetilde{f}_m\{\alpha_1,\ldots,\alpha_n\}^m = \widetilde{f}_m\{\alpha_1^m,\ldots,\alpha_n\} = \{\alpha_1,\ldots,\alpha_n\}$$

Thus $\mathrm{K}_n^M F$ is uniquely m-divisible. □

Corollary 5.7.10. *Let F be an algebraically closed field. Then $\mathrm{K}_n^M F$ is uniquely divisible.*

Proof. Since F is algebraically closed, it contains all mth roots of unity for all $m \geq 1$. Hence by Proposition 5.7.9, is uniquely m-divisible for all $m \geq 1$, so by definition of uniquely divisible 5.7.8, it is uniquely divisible. □

Having done the above, we now give a slightly different method of showing that K_2^M of an algebraically closed field is divisible. We give a laundry list of lemmas which build up to this. In the end, the proof ends up relying on basically the same trick as the Fesenko proof, but it's still interesting. These ideas are from exercise 7.1 of Gille & Szamuely [4].

Proposition 5.7.11. *Let K be an algebraically closed field. Then $\mathrm{K}_2^M(K)$ is uniquely divisible.*

Proof. Let $n \in \mathbb{Z}$, $n \neq 0$, and consider the following diagram with exact rows.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & R & \longrightarrow & K^\times \otimes_{\mathbb{Z}} K^\times & \xrightarrow{\{,\}} & K_2^M(K) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \downarrow{\scriptstyle n} & & \\
0 & \longrightarrow & R & \longrightarrow & K^\times \otimes_{\mathbb{Z}} K^\times & \xrightarrow{\{,\}} & K_2^M(K) & \longrightarrow & 0
\end{array}$$

where R is the submodule generated by elements $u \otimes (1-u)$. By Proposition 1.4.14, $K^\times \otimes \mathrm{K}^\times$ is uniquely divisible, so the middle map is an isomorphism. By the snake lemma, there is an exact sequence

$$\ker n \to \ker n \to \ker n \to \operatorname{coker} n \to \operatorname{coker} n \to \operatorname{coker} n$$

which since the middle map is an isomorphism becomes

$$0 \to \ker n \xrightarrow{\cong} \operatorname{coker} n \to 0$$

Since $\mathrm{K}_2^M(K)$ is a quotient of a divisible group, it is divisible, so it suffices to prove that it is torsion free, which is to say, that the kernel of n is trivial. By our isomorphism, this is equivalent to showing that $n : R \to R$ has trivial cokernel, namely, is surjective. Since R is generated by elements $u \otimes (1-u)$ for $u \in K^\times$, it suffices to show that $u^{1/n} \otimes (1-u) \in R$, or equivalently by exactness, that $\left\{u^{1/n}, 1-u\right\} = 1$ in $\mathrm{K}_2^M(K)$.

This is where we are essentially back to the argument of Fesenko. Let $\beta \in K^\times, \beta^n = u$, and let $\zeta \in K^\times$ be a primitive nth root of unity. Then

$$1 - u = \prod_{i=1}^{n} (1 - \zeta^i \beta)$$

Now

$$\{\beta, 1-u\} = \left\{\beta, \prod (1-\zeta^i\beta)\right\} = \prod^{n} \left\{\beta, 1-\zeta^i\beta\right\} = \prod \left\{\zeta^i, 1-\zeta^i\beta\right\}^{-1}$$

Now choose $\alpha_i \in K^\times$ so that $\alpha_i^n = 1 - \zeta^i\beta$. Then

$$1 = \prod \left\{\zeta^i, \alpha_i^n\right\}^{-1} = \prod \left\{\zeta^i, \alpha_i\right\}^{-n} = \prod \left\{\zeta^{in}, \alpha_i\right\}^{-1} = \prod \{1, \alpha_i\} = 1$$

□

5.8 Merkurjev-Suslin theorem

The Merkurjev-Suslin theorem is the bow that ties together almost everything developed in these notes. Depending on how the statement is formulated, it involves group cohomology, Brauer groups, algebraic K-theory (in particular, K_2 which is the same as K_2^M). It relates the languages of central simple algebras (in particular, cyclic algebras) with the language of cup products from group cohomology, and makes use of the isomorphisms of Kummer theory.

Though it is not the most general version of Merkurjev-Suslin, the easiest way to conceptualize the theorem is that it tells you rather explicitly about a set of generators for the Brauer group of a field. It says that the m-torsion subgroup of $\mathrm{Br}(K)$ is generated by "cyclic algebras," whatever those are. Since $\mathrm{Br}(K)$ is a torsion group, it is the union of all m-torsion subgroups, so this gives a complete set of generators for $\mathrm{Br}(K)$.

In a more general version, Merkurjev-Suslin gives an isomorphism between the m-torsion of $\mathrm{Br}(K)$, and the quotient $\mathrm{K}_2^M(K)/m\,\mathrm{K}_2^M$, and tells you how elements correspond under this isomorphism. A symbol $\{a,b\}$ in K_2^M corresponds to a cyclic algebra $(a,b)_\omega$ in $\mathrm{Br}(K)$.

Before we can state the Merkurjev-Suslin theorem, we need to describe the Galois symbol map. In its most general statement (in these notes), the Mekurjev-Suslin theorem says that the Galois symbol map induces a particular isomorphism. Defining the symbol map involves Kummer theory, cup products, and some lemmas about K_2^M.

5.8.1 Statement of Merkurjev-Suslin theorem in terms of cyclic algebras

In this section, we assume K is a field containing a primitive mth root of unity. The results still hold in the general case, but they are simpler to state in this case, and the description of cyclic algebras is much simpler in this case.

Definition 5.8.1. Let K be a field containing a primitive mth root of unity ω. For $a,b \in K^\times$, the **cyclic algebra** $(a,b)_\omega$ is given by the presentation

$$\langle x,y \mid x^m = a, y^m = b, xy = \omega yx\rangle$$

Note that $\dim_K(a,b)_\omega = m^2$, with a K-basis given by products x^iy^j for $0 \le i,j \le m-1$.

Theorem 5.8.2 (Merkerjev-Suslin, Theorem 2.5.7 on page 41 of Gille & Szamuely [4])**.** *Let K be a field containing a primitive mth root of unity ω. The a central simple K-algebra A whose class has order dividing m in $\mathrm{Br}(K)$ is Brauer equivalent to a tensor product of cyclic algebras.*

$$[A] = (a_1,b_1)_\omega \otimes_K \cdots \otimes_K (a_i,b_i)_\omega$$

That is, the m-torsion subgroup ${}_m\mathrm{Br}(K) \subset \mathrm{Br}(K)$ is generated by cyclic algebras.

Remark 5.8.3. Every field has a primitive square root of unity (namely -1), so the case $m=2$ says that the 2-torsion of $\mathrm{Br}(K)$ for any field K is generated by quaternion algebras. (This is pointed out in Theorem 1.5.8 of Gille & Szamuely [4].)

5.8.2 Construction of Galois symbol

We outline the process of constructing the Galois symbol map $h^n_{K,m} : K^M_n(K) \to H^n(G_K, \mu_m^{\otimes n}$, assuming $\mathrm{char}\, K$ is coprime to m. This will allow us to make a state a more general version of Merkurjev-Suslin.

Remark 5.8.4. Let K be a field and let m be a positive integer such that m is coprime to the characteristic of K, so that the group of mth roots of unity μ_m lives in a separable closure K^{sep}. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K. Recall from Kummer theory that in this situation, there is an isomorphism

$$K^\times/K^{\times m} \cong H^1(G_K, \mu_m)$$

We may also view this as a surjection $K^\times \to H^1(G_K, \mu_m)$ with kernel $K^{\times m}$.

$$0 \to K^{\times m} \hookrightarrow K^\times \to H^1(G_K, \mu_m) \to 0$$

The isomorphism may be described explicitly in terms of elements as follows. For $a \in K^\times$, the class of $a \in K^\times / K^{\times m}$ corresponds to the Kummer cocycle $\chi_a \in H^1(G_K, \mu_m)$, where

$$\chi_a : G_K \to \mu_m \qquad \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

where α is any mth root of a. For details behind this, such as why χ_a is well defined, or why it is a cocycle, see Proposition 4.3.6 of Gille & Szamuley [4] or Proposition 2.5.8 of Sharifi [15].

Definition 5.8.5. Let R be a ring and M be an R-module. We use the notation $M^{\otimes n}$ for the n-fold tensor product $M \otimes_R \cdots \otimes_R M$ with n factors. (In what follows, we will always have $R = \mathbb{Z}$, but this notation makes sense more generally.)

Definition 5.8.6. Let $K, m, K^{\text{sep}}, \mu_m, G_K$ be as above. For $n \in \mathbb{Z}_{\geq 2}$, Consider the cup product (all tensor products over $\mathbb{Z}$)

$$H^1(G_K, \mu_m)^{\otimes n} \xrightarrow{\cup} H^n(G_K, \mu_m^{\otimes n})$$

Combining this with the surjections $K^\times \to H^1(G_K, \mu_m)$, we obtain a homomorphism

$$\partial^n : (K^\times)^{\otimes n} \to H^n(G_K, \mu_m^{\otimes n})$$

Remark 5.8.7. Recall the general fact that for two positive integers a, b,

$$\mathbb{Z}/a\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/\gcd(a,b)\mathbb{Z}$$

Iterating this, we obtain

$$\mu_m^{\otimes n} = \mu_m \otimes \cdots \otimes \mu_m \cong \mathbb{Z}/m\mathbb{Z} \otimes \cdots \otimes \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \cong \mu_m$$

So for the target of ∂^n we have $H^n(G_K, \mu_m^{\otimes n}) \cong H^n(G_K, \mu_m)$. Despite this, we still often write the tensor product.

Proposition 5.8.8. *Let ∂^n be the map defined above. If $a_1, \ldots, a_n \in K^\times$ such that $a_i + a_j = 1$ for some pair $i \neq j$, then $\partial^n(a_1 \otimes \cdots \otimes a_n) = 0$.*

Proof. Lemma 4.6.2 and Proposition 4.6.1 in Gille & Szamuley [4]. □

Definition 5.8.9. Let K, ∂^n, etc. be as above. Recall that the nth Milnor K-group $K_n^M(K)$ is the quotient of $(K^\times)^{\otimes n}$ by the ideal generated by elements $a_1 \otimes \cdots \otimes a_n$ for which some pair i, j we have $a_i + a_j = 1$. By definition, ∂^n vanishes on this ideal, and induces a homomorphism

$$h^n_{K,m} : K_n^M(K) \to H^n(G_K, \mu_m^{\otimes n})$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker & \longrightarrow & (K^\times)^{\otimes n} & \xrightarrow{\{\ldots\}} & K_n^M(K) & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \partial^n} & \swarrow{\scriptstyle h^n_{K,m}} & & & \\ & & & & H^2(G_K, \mu_m^{\otimes n}) & & & & \end{array}$$

The class of $a_1 \otimes \cdots \otimes a_n \in (K^\times)^{\otimes n}$ in the quotient $K_n^M(K)$ is denoted by $\{a_1, \ldots, a_n\}$ and is called a **symbol**. The map $h^n_{K,m}$ is the **Galois symbol** map.

5.8.3 Statement of Merkurjev-Suslin theorem in terms of Galois symbol

Now we state the Merkurjev-Suslin theorem (without proof) in general for any field K, in terms of the Galois symbol $h^2_{K,m} : K_2^M(K) \to H^2(G_K, \mu_m^{\otimes 2})$.

Theorem 5.8.10 (Merkurjev-Suslin theorem, Theorem 4.6.6 on page 132 of Gille & Szamuely [4])**.** *Let K be a field and m a positive integer which is invertible in K. For $n = 2$, the Galois symbol map is a surjection*

$$h^2_{K,m} : K_2^M(K) \twoheadrightarrow H^2(G_K, \mu_m^{\otimes 2})$$

with kernel $mK_2(M)$, so it induces an isomorphism

$$K_2^M(K)/m \cong H^2(G_K, \mu_m^{\otimes 2})$$

Remark 5.8.11. The previous theorem is a special case of the much more general Voevodsky-Rost theorem (published 2000), formerly known as the Bloch-Kato conjecture. It says that $h^n_{K,m}$ is an isomorphism for all $n \geq 0$, not just $n = 2$. Note that the case $n = 0$ is trivial, and $n = 1$ is just the isomorphism

$$K_1(K)/m = K^\times/K^{\times m} \cong H^1(G_K, \mu_m)$$

of Kummer theory. The case $n = 2$ (above) was proven by Merkurjev-Suslin in 1982.

Remark 5.8.12. Let K be a field and let m be a positive integer which is coprime to the characteristic of K. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group. From remark 5.8.7, we have an isomorphism

$$H^2(G_K, \mu_m^{\otimes 2}) \cong H^2(G_K, \mu_m)$$

From Kummer theory, we have an isomorphism

$$H^2(G_K, \mu_m) \cong {}_m \mathrm{Br}(K)$$

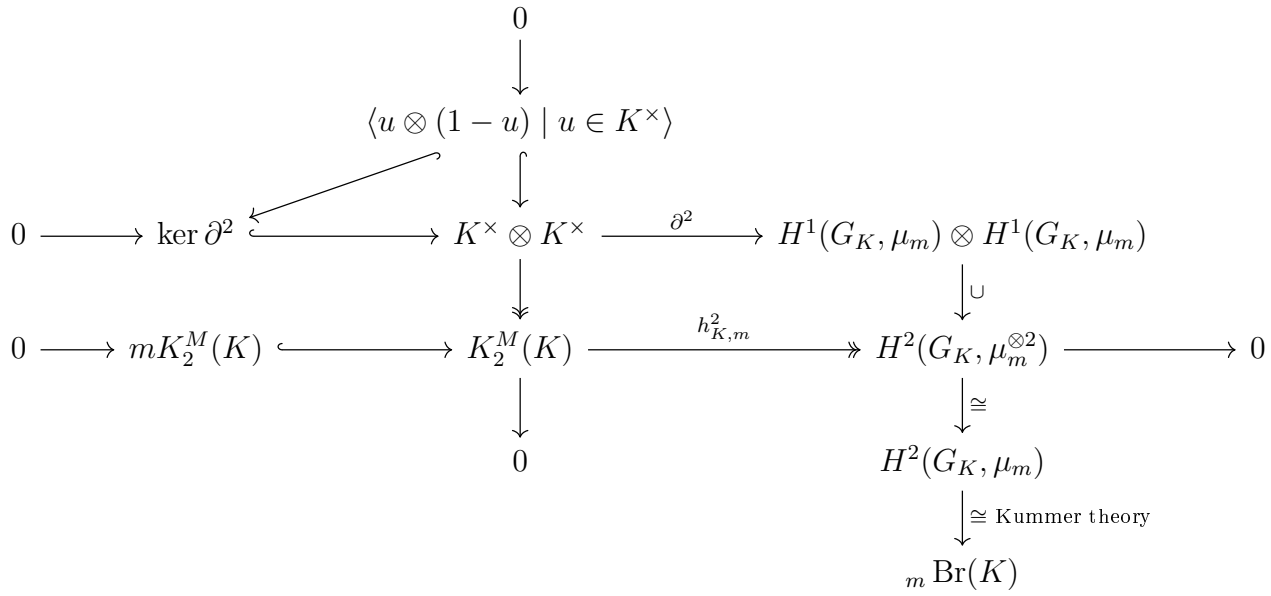
Combining these with the isomorphism of the Merkurjev-Suslin theorem, we obtain

$$K_2^M(K)/m \cong {}_m \mathrm{Br}(K)$$

Remark 5.8.13. Here is a large diagram attempting to summarize the various objects and maps involved in the above statements. The map δ is one of the isomorphisms from Kummer theory, coming from the connecting homomorphism of a LES.

The vertical sequence involving $K_2^M(K)$ is exact by definition of $K_2^M(K)$. The first horizontal row is exact by definition of kernel. The inclusion of $\langle u \otimes (1-u) \rangle$ into $\ker \partial^2$ is the content of Proposition 5.8.8. Exactness of the second horizontal row is the content of

the Merkurjev-Suslin theorem.



5.8.4 Connection between the two versions

Since we stated two theorems which are not immediately obviously the same thing and used the same name for them, we should justify why these are reasonably thought of as "the same" theorem. The reason is that the first version, in terms of cyclic algebras, is a corollary of the second version in terms of the Galois symbol, once we set up a few lemmas.

Definition 5.8.14. Let L/K be a cyclic Galois extension of order m, and fix an isomorphism $\chi : \mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$. Let $b \in K^\times$, and let $\sigma = \chi^{-1}(1)$. The **cyclic algebra** (χ, b) is the algebra with the following presentation. It is generated as an L-algebra by L and an element y, satisfying

$$y^m = b \qquad \sigma(\lambda) = y^{-1}\lambda y, \ \ \forall \lambda \in L$$

Remark 5.8.15. If K contains a primitive mth root of unity ω, then there is an isomorphism $(\chi, b) \cong (a, b)_\omega$ [7] which justifies the double use of the term "cyclic algebra." See Corollary 2.5.5 of Gille & Szamuely [4].

Proposition 5.8.16. *Let K be a field, fix separable closure K^{sep}, and let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Let L/K be a cyclic Galois extension of degree m contained in K^{sep}, and let $G = \mathrm{Gal}(L/K)$. Fix an isomorphism*

$$\chi : G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

Then define

$$\widetilde{\chi} : G_K \to \mathbb{Z}/m\mathbb{Z} \qquad \sigma \mapsto \chi(\sigma|_L)$$

Let $\delta : H^1(G_K, \mathbb{Z}/m\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$ be the coboundary map of the LES associated to

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$$

[7] There are details about what a anc χ should be to make this work, but we omit these.

Then consider the cup product map

$$H^2(G_K, \mathbb{Z}) \otimes H^0(G_K, K^{\text{sep}\,\times}) \xrightarrow{\cup} H^2(G_K, K^{\text{sep}\,\times})$$

Fix $b \in K^\times$. Under the isomorphism

$$H^2(G_K, K^{\text{sep}\,\times}) \cong \text{Br}(K)$$

the element $\delta(\widetilde{\chi}) \cup b$ correpends to the Brauer class of the cyclic algebra (χ, b).

Proof. Proposition 4.7.3 of Gille & Szamuley [4]. □

Proposition 5.8.17. *Let K be a field and let m be a positive integer which is coprime to the characteristic of K, and suppose K contains a primitive mth root of unity ω. Let $a, b \in K^\times$. Under the isomorphism*

$$K_2^M(K)/m \cong {}_m\,\text{Br}(K)$$

of remark 5.8.12, the element $\{a, b\}$ corresponds to the Brauer class of the cyclic algebra $(a, b)_\omega$. That is, $h^n_{K,m}\{a, b\}$ is Brauer equivalent to $(a, b)_\omega$.

Proof. Proposition 4.7.1 of Gille & Szamuely [4]. □

Remark 5.8.18. The tensor product $K^\times \otimes K^\times$ is generated by simple tensors $a \otimes b$, so the quotient $K_2^M(K)$ is generated by the images of these, that is, $K_2^M(K)$ is generated by symbols $\{a, b\}$. Thus the previous proposition says that ${}_m\,\text{Br}(K)$ is generated by cyclic algebras $(a, b)_\omega$. That is to say, the Galois symbol version of Merkurjev-Suslin 5.8.10 implies the cyclic algebra version of Merkurjev-Suslin 5.8.2.

Chapter 6

Local fields

This whole chapter is more of an appendix, and primarily serves as a reference for sections 4.6.7 and 4.6.8. Despite this, it is a very incomplete reference.

6.1 Valuations and absolute values

The primordial example of an absolute value is the usual absolute value on $\mathbb{R}$ or $\mathbb{Q}$, which has the well known extension to complex norm on $\mathbb{C}$. Unfortunately, we will largely ignore this absolute value, because it is not as "algebraic" as the absolute values we consider.

Definition 6.1.1. Let K be a field. An **absolute value** on K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ which satisfies

$$|x| = 0 \iff x = 0$$

and is a group homomorphism $K^\times \to \mathbb{R}_{\geq 0}$, that is, for $x, y \in K$,

$$|xy| = |x||y|$$

and satisfies the triangle inequality

$$|x + y| \leq |x| + |y|$$

If the absolute value also satisfies the stronger **nonarchimedean triangle inequality**

$$|x + y| \leq \max(|x|, |y|)$$

then we call the absolute value **nonarchimedean**. Note that the usual absolute value on $\mathbb{R}$ is not nonarchimedean (so we call it archimedean).

Example 6.1.2. Let $p \in \mathbb{Z}$ be a prime. The **p-adic absolute value** on $\mathbb{Q}$ is given by

$$|x|_p = |p^n x'|_p = p^{-n}$$

where x' is uniquely determined by factoring out all powers of p from x. Another way to describe this valuation is by

$$|q|_p = \begin{cases} 1 & q \neq p \\ \frac{1}{p} & q = p \end{cases}$$

where q in $\mathbb{Z}$ is a prime or -1. Using the multiplicative property, this determines $|\cdot|_p$ on all of $\mathbb{Q}$. Note that the p-adic absolute value is nonarchimedean (requires some basic number theoretic arguments to prove).

Remark 6.1.3. Let K be a field with an absolute value $|\cdot|$. This induces a distance function on K via

$$d(x, y) = |x - y|$$

which gives K a metric topology. Whenever a field K has an absolute value, we think of it having the induced metric topology.

Theorem 6.1.4 (Gouvea [5] 2.2.2)**.** *Let K be a field with absolute value $|\cdot| : K \to \mathbb{R}_{\geq 0}$, and let*

$$A = \{1n : n \in \mathbb{Z}\} \subset K$$

be the image of $\mathbb{Z}$ in K. The absolute value is nonarchimedean if and only $|a| \leq 1$ for all $a \in A$.

Proof. If the absolute value is nonarchimedean, then for $a \in A$ we have

$$|a| = |1 + \cdots + 1| \leq \max(|1|, \ldots, |1|) = 1$$

which proves the forward direction. For the converse, let $x, y \in K$; we need to show $|x+y| \leq \max(|x|, |y|)$. If $y = 0$, this is obvious since $|0| = 0$. If $y \neq 0$, then this is equivalent to

$$\left|\frac{x}{y} + 1\right| \leq \max\left(\left|\frac{x}{y}\right|, 1\right)$$

Thus if the inequality holds for $y = 1$, it holds in general. That is, we just need to show $|x + 1| \leq \max(|x|, 1)$. Let $m \in \mathbb{Z}_{\geq 1}$. Then

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x|^k \leq \sum_{k=0}^{m} |x|^k \leq (m+1)\max(1, |x|^m)$$

Taking mth roots, we obtain

$$|x + 1| \leq (m+1)^{1/m} \max(1, |x|)$$

for every $m \in \mathbb{Z}_{\geq 1}$. Since

$$\lim_{m\to\infty} (m+1)^{1/m} = 1$$

the previous inequality holding for all $m \in \mathbb{Z}_{\geq 1}$ implies

$$|x + 1| \leq \max(1, |x|)$$

which is what we needed to show. □

Theorem 6.1.5 (Ostrowski's theorem)**.** *Up to equivalence, the only nontrivial absolute values on $\mathbb{Q}$ are $|\cdot|_\infty$ and $|\cdot|_p$ for primes $p \in \mathbb{Z}$. (Conversely, these are all distinct for $p_1 \neq p_2$.)*

Proof. This is not a trivial result, but also does not involve heavy mathematical machinery. See Milne [8] chapter 7 for a proof. □

Proposition 6.1.6 (Exercises 68, 69 of Gouvea [5]). .

1. *Let p, q be distinct primes. The p-adic and q-adic absolute values are not equivalent.*
2. *An archimedean absolute value on a field K is not equvialent to a nonarchimedean absolute value. In particular, $|\cdot|_p$ is not equivalent to $|\cdot|_\infty$ for any p.*

Proof. (1) They are equivalent if and only if there exists $c \in \mathbb{R}_{>0}$ such that $|x|_p^c = |x|_q^c$ for all $x \in \mathbb{Q}$. For any $c \in \mathbb{R}_{>0}$,

$$|p|_q^c = 1 \qquad |q|_q^c = \frac{1}{q^c} \neq 1$$

(2) If an archimedean absolute value $|\cdot|_a$ is equivalent to a nonarchimedean absolute value $|\cdot|_b$, then $|x|_a = |x|_b^c$ for some $c \in \mathbb{R}_{>0}$, so

$$|x+y|_a = |x+y|_b^c \leq \max\left(|x|_b, |y|_b\right)^c = \max\left(|x|_a^c, |y|_b^c\right) = \max(|x|_a, |y|_a)$$

so $|\cdot|_a$ has the nonarchimedean triangle inequality, which is impossible by definition. □

An alternative way to look at nonarchimedean absolute values is by looking at valuations. Later we'll show that these are entirely equivalent perspectives.

Definition 6.1.7. Let K be a field. A **valuation** on K is a group homomorphism $v : K^\times \to \mathbb{R}$, satisfying

$$v(x+y) \geq \min(v(x), v(y))$$

for all $x, y \in K^\times$. It is sometimes convenient to extend a valuation v to all of K by setting $v(0) = \infty$, but this shouldn't be taken too literally.

A valuation v is **discrete** if the image $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$. Note that a discrete subgroup of $(\mathbb{R}, +)$ is necessarily isomorphic to $\mathbb{Z}$, so often we **normalize** a discrete valuation so that the image is precisely $\mathbb{Z}$, which we can always do just by introducing a scaling factor.

Lemma 6.1.8. *Let K be a field and $v : K^\times \to \mathbb{Z}$ a discrete valuation. Then*

1. *If $a \in K^\times$ is a root of unity, then $v(x) = 0$.*
2. *If $a, b \in K^\times$ and $v(b) < v(a)$, then $v(a+b) = v(b)$.*
3. *If $a_1, \ldots, a_n \in K^\times$ satsify $a_1 + \cdots + a_n = 0$, then the minimal value of $v(a_i)$ is attained for at least two indices.*

Proof. (1) If $a^n = 1$ then $nv(a) = v(a^n) = v(1) = 0$ so $v(a) = 0$.
(2) Let a, b be such that $v(b) < v(a)$. Then

$$v(a+b) \geq \min(v(a), v(b)) = v(b)$$

and

$$v(b) = v(b + a - a) \geq \min(v(a + b), v(-a)) = \min(v(a + b), v(a))$$

If this min was $v(a)$ we would have a contradiction since $v(b) < v(a)$, so $v(b) \geq v(a + b)$. Since we have inequality both ways, $v(a + b) = v(b)$.
(3) Suppose $a_1 + \cdots + a_n = 0$ and choose i so that $v(a_i)$ is minimal. Then solve for a_i.

$$a_i = -(a_1 + \cdots + \widehat{a}_i + \cdots + a_n)$$

Taking valuations,

$$v(a_i) = v(-1) + v(a_1 + \cdots + \widehat{a}_i + \cdots + a_n) = v(a_1 + \cdots + \widehat{a}_i + \cdots + a_n) \geq \min_{j \neq i} v(a_j)$$

Thus there is another value j such that $v(a_j) \leq v(a_i)$. But by choice of i, $v(a_i) \leq v(a_j)$, so they are equal. □

6.1.1 Correspondence between valuations and absolute values

Proposition 6.1.9. *Let K be a field and fix $b \in K^\times$. There is a bijective correspondence*

$$\{\text{discrete valuations on } K\} \longleftrightarrow \{\text{nonarchimedean discrete absolute values on } K\}$$
$$v \longmapsto |x| = b^{-v(x)}$$

Also, this correspondence preserves the usual equivalence on both sides.

Proof. Omitted. □

Remark 6.1.10. We spell out the correspondence above in more detail with the following table.

Nonarchimedean discrete absolute value	Discrete valuation
$\lvert\cdot\rvert : K^\times \to \mathbb{R}_{>0}$	$v : K^\times \to \mathbb{Z}$
$\lvert\cdot\rvert : K \to \mathbb{R}_{\geq 0}$	$v : K \to \mathbb{Z} \cup \{\infty\}$
$\lvert x\rvert = 0 \iff x = 0$	$v(0) = \infty \iff x = 0$
$\lvert xy\rvert = \lvert x\rvert\lvert y\rvert$	$v(xy) = v(x) + v(y)$
$\lvert x + y\rvert \leq \max(\lvert x\rvert, \lvert y\rvert)$	$v(x + y) \geq \min(v(x), v(y))$
$\lvert x\rvert = b^{-v(x)}$	v
$\lvert\cdot\rvert$	$v(x) = -\log_b(x)$ where $\lvert K^\times\rvert = \{b^n : n \in \mathbb{Z}\}$

In practice, there is often a usual choice for b for a given valuation. For example, the p-adic absolute value and p-adic valuation on $\mathbb{Q}$ are traditionally related by the choice of $b = p$.

6.1.2 Completions

Definition 6.1.11. Let K be a field with an absolute value $|\cdot|$. A **Cauchy sequence** with respect to the absolute value is a sequence (a_n) with $a_n \in K$ such that for every $\epsilon > 0$, there exists $N > 0$ such that for $i, j \geq N$,

$$|a_i - a_j| < \epsilon$$

This generalizes the usual notion of Cauchy sequences in $\mathbb{Q}$ or $\mathbb{R}$, just by replacing the usual absolute value with any absolute value function.

Definition 6.1.12. Let K be a field with an absolute value $|\cdot|$. K is **complete** with respect to $|\cdot|$ if every Cauchy sequence in K has a limit in K.

Lemma 6.1.13 (Gouvea [5] 3.2.3)**.** *The field $\mathbb{Q}$ is not complete with respect to any of its nontrivial absolute values.*

Theorem 6.1.14. *Let K be a field with an absolute value $|\cdot|$. There exists a unique up to isomorphism field $\widehat{K}$ which is an extension of K, with an absolute value on $\widehat{K}$ extending the absolute value on K, such that $\widehat{K}$ is complete with respect to the absolute value.*

Proof. This is just a sketch. Consider the set of Cauchy sequences in K. They can be added, subtracted, and multiplied point-wise. Consider two sequences to be equivalent if their difference approaches zero. Then set $\widehat{K}$ to be the set of equivalence classes of such sequences. Note that nonzero classes in $\widehat{K}$ can now be divided point-wise, since a nonzero Cauchy sequence is eventually bounded away from zero. K embeds into $\widehat{K}$ by taking an element x to the constant sequence $(x, x, x \ldots)$. The abolute value on K can be extended to $\widehat{K}$ by setting

$$|(a_n)| = \lim_{n\to\infty} |a_n|$$

We leave it as an exercise to verify that this makes sense and extends the absolute value. The trickiest part is to verify that $\widehat{K}$ is complete with respect to this absolute value, which requires some careful working through definitions, but nothing too difficult. □

If we take $K = \mathbb{Q}$ with the usual archimedean absolute value, then we get $\widehat{K} = \mathbb{R}$.

Definition 6.1.15. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is denoted $\mathbb{Q}_p$. Note that if p, q are distinct primes, then $\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic[1], but this will take some work to show (see Proposition 6.2.17).

6.1.3 Extending complete absolute values

Proposition 6.1.16. *Let K be a complete nonarchimedean discretely valued field, and let L/K be a finite extension, with $n = [L : K]$. Then there is a unique absolute value on L extending the absolute value on K, such that L is complete with respect to the absolue value. Explicitly,*

$$|x|_L = \left|N_K^L(x)\right|_K^{1/n}$$

Furthermore, the valuation ring $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

[1] Obviously they are not isomoprhic as valued fields since they have distinct residue fields, but even more, they are not isomorphic just as abstract fields.

Remark 6.1.17. By the above, if L/K is Galois and $\alpha, \alpha' \in L$ are Galois conjugates, then $|\alpha|_L = |\alpha'|_L$, since α, α' have the same norm.

Remark 6.1.18. Let K be a complete valued field as in the previous theorem. Since the algebraic closure of K is the union over all finite extensions of K, using the previous theorem, we can extend the absolute value on K uniquely to the algebraic closure. (This can also be done for the separable closure if that is desirable.) However, this does not tell us that the algebraic closure is complete with respect to the extended value, and usually it is not. We now have processes

$$K \rightsquigarrow \widehat{K} \qquad K \rightsquigarrow K^{\text{alg}}$$

both with unique extensions of the absolute value. So we can do things like

$$K \rightsquigarrow \widehat{K} \rightsquigarrow \widehat{K}^{\text{alg}} \rightsquigarrow \widehat{\widehat{K}^{\text{alg}}} \rightsquigarrow \widehat{\widehat{K}^{\text{alg}}}^{\text{alg}} \rightsquigarrow \cdots$$

which in principle may never terminate, since after taking the completion, we may not have an algebraically closed field, and after taking the algebraic closure, we may not have a complete field.

For example, the algebraic closure of $\mathbb{Q}_p$ is not complete with respect to to the extended absolute value (assertion without proof here, not obvious). However, it is a theorem (citation?) that if you form the completion of $\mathbb{Q}_p^{\text{alg}}$ with respect to its absolute value that the resulting field is algebraically closed in addition to being complete. That is, starting with $\mathbb{Q}$ with p-adic absolute value, the above process terminates after

$$\mathbb{Q} \rightsquigarrow \mathbb{Q}_p \rightsquigarrow \mathbb{Q}_p^{\text{alg}} \rightsquigarrow \widehat{\mathbb{Q}_p^{\text{alg}}}$$

since this completion is algebraically closed, taking the algebraic closure does nothing.

6.1.4 Hensel's lemma

Proposition 6.1.19 (Hensel's lemma, version 1)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$, and residue field $k = \mathcal{O}_K/\mathfrak{m}$. Let $f \in \mathcal{O}_K[x]$, and suppose there exist $g_1, h_1 \in \mathcal{O}_K[x]$ with g_1 monic and $\gcd(g_1, h_1) = 1$ such that*

$$\overline{f} = \overline{g_1 h_1} \in k[x] \qquad (\text{equivalently } f \equiv g_1 h_1 \bmod \mathfrak{m})$$

Then there exist $g, h \in \mathcal{O}_K[x]$ such that g is monic, $\overline{g} = \overline{g}_1, \overline{h} = \overline{h}_1$, and $f = gh$. That is, factorizations of polynomials over k lift to factorizations over $\mathcal{O}_K$, provided there are no common factors and one is monic.

Remark 6.1.20. This is hardly worth stating, but the "converse" of Hensel's lemma is obvious. If f factors in in $\mathcal{O}_K[x]$, then applying the quotient map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{m}$ to the coefficients gives a factorization in $k[x]$.

Remark 6.1.21. In particular, we care about the case $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, \mathfrak{m} = p\mathbb{Z}_p, k = \mathbb{F}_p$. In this case, Hensel's lemma says that if a polynomial $f(x) \in \mathbb{Z}_p[x]$ has a factorization $\bmod p$ into relatively prime factors, then that factorization comes from a factorization in $\mathbb{Z}_p$.

In particular, $\mathbb{Z} \subset \mathbb{Z}_p$, and this is where Hensel's lemma is often applied, at least in examples. Suppose we want to know if some polynomial equation $f(x) = 0$ with $f \in \mathbb{Z}[x]$ has a solution in $\mathbb{Q}_p$ or $\mathbb{Z}_p$. If we find a factorization of $\overline{f}$ with a monic, non-repeated linear factor $(x - a)$ where $a \in \mathbb{F}_p$, then that factorization lifts to a factorization of f in $\mathbb{Z}_p[x]$ so there is a lift of $\alpha \in \mathbb{Z}_p$ so that $\overline{\alpha} = a$ and $f(\alpha) = 0$. The next corollary says this more precisely.

Corollary 6.1.22 (Hensel's lemma, version 1, for $\mathbb{Q}_p$)**.** *Let $f(x) \in \mathbb{Z}_p[x]$. If $\overline{f}(x) \in \mathbb{F}_p[x]$ has a simple root a, that is, there exists $a \in \mathbb{F}_p$ such that $\overline{f}(a) = 0$ and $\overline{f'}(a) \neq 0$, then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\overline{\alpha} = a$.*

We also need another version of Hensel's lemma at one point later.

Proposition 6.1.23 (Hensel's lemma, version 2)**.** *Let K be a complete nonarchimedean discretely valued field, with associated local ring $(\mathcal{O}_K, \mathfrak{m})$. Let $f(x) \in \mathcal{O}_K[x]$ be monic. Suppose $a \in \mathcal{O}_K$ such that*

$$f'(a) \neq 0 \qquad |f(a)| < |f'(a)|^2$$

Then there exists a unique $\alpha \in \mathcal{O}_K$ such that $f(\alpha) = 0$ and

$$|a - \alpha| \leq \left| \frac{f(a)}{f'(a)} \right|$$

Proposition 6.1.24. *Let p be a prime.*

1. *If $p \geq 3$, then: $u \in \mathbb{Z}_p^\times$ is a square $\iff$ $\overline{u} \in \mathbb{F}_p^\times$ is a square.*
2. *If $p = 2$, then: $u \in \mathbb{Z}_2^\times$ is a square $\iff$ $u \equiv 1 \bmod 8$.*

Proof. ($1 \implies$) If $u = \alpha^2 \in \mathbb{Z}_p$ then $\overline{u} = \overline{\alpha}^2 \in \mathbb{F}_p^\times$. ($1 \impliedby$) Suppose $\overline{u} = a^2 \in \mathbb{F}_p$. Consider $f(x) = x^2 - u \in \mathbb{Z}_p[x]$. Then

$$\overline{f}(x) = x^2 - \overline{u} = x^2 - a^2 = (x - a)(x + a)$$

Note that $\overline{f'}(a) = 2a \neq 0$ since $p \geq 3$, so we can apply Corollary 6.1.22 to conclude that there is a root $\alpha \in \mathbb{Z}_p$ of f, so $u = \alpha^2$. (2) Omitted. □

6.2 $\mathbb{Q}_p$ and $\mathbb{Z}_p$

Definition 6.2.1. Let $a, b \in \mathbb{Q}_p$. We say a, b are **congruent mod** p^n if

$$|a - b|_p \leq p^{-n}$$

This extends the usual notion of congruence mod p^n from $\mathbb{Z}$.

Proposition 6.2.2 (Gouvea [5] 3.3.4)**.** *The ring $\mathbb{Z}_p$ is a local ring with principal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\}$. Furthermore,*

1. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$

2. *The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. In particular, for $x \in \mathbb{Z}_p$, and $n \geq 1$, there exists $\alpha \in \mathbb{Z}, 0 \leq \alpha \leq p^n - 1$ such that $|x - \alpha| \leq p^{-n}$, and such α is unique.*

3. *For any $x \in \mathbb{Z}_p$, there exists a Cauchy sequence α_n converging to x, such that $\alpha_n \in \mathbb{Z}, 0 \leq \alpha_n \leq p^n - 1$, and for every n we have $\alpha_n \equiv \alpha_{n-1} \bmod p^{n-1}$. Furthermore, the sequence (α_n) with these properties is unique.*

Proposition 6.2.3 (Hensel's lemma for $\mathbb{Q}_p$)**.** *Let $f(x) \in \mathbb{Z}_p[x]$. Suppose $a \in \mathbb{Z}_p$ such that*

$$f(a) \equiv 0 \bmod p \qquad f'(a) \not\equiv 0 \bmod p$$

Then there exists a unique $b \in \mathbb{Z}_p$ such that

$$f(b) = 0 \qquad a \equiv b \bmod p$$

Remark 6.2.4. A p-adic integer $x \in \mathbb{Z}_p$ has a unique expansion

$$x = \sum_{k=0}^{\infty} a_k p^k = a_0 + a_1 p + a_2 p^2 + \cdots$$

where $0 \leq a_i \leq p - 1$. It is a unit (is in $\mathbb{Z}_p^\times$) if and only if $a_0 \neq 0$.

Lemma 6.2.5. *The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. That is, if $x \in \mathbb{Z}_p$ and $n \geq 1$, there exists $\alpha \in \mathbb{Z}$ with $0 \leq \alpha \leq p^n - 1$ such that $|x - \alpha|_p \leq p^{-n}$.*

Proof. Using the expansion of above, write $x = a_0 + a_1 p + a_2 p^2 + \cdots$, then set $\alpha = a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$. Then it is clear that $0 \leq \alpha \leq p^n - 1$ and using the nonarchimedean triangle inequality we get

$$|x - \alpha|_p = |a_n p^n + a_{n+1} p^{n+1} + \cdots|_p \leq \max_{i \geq n} |a_i p^i| = |p^n| = p^{-n}$$

□

6.2.1 p-adic units $\mathbb{Z}_p^\times$

Remark 6.2.6. From the previous unique description via expansions, it is clear that the following sequence is exact.

$$0 \to p^n \mathbb{Z}_p \hookrightarrow \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z} \to 0$$

where the right map is the "truncation" map

$$a_0 + a_1 p + a_2 p^2 + \cdots \mapsto a_0 + a_1 p + \cdots + a_{n-1} p^{n-1}$$

Thus from the first isomorphism theorem we obtain

$$\mathbb{Z}_p / p^n \mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

More generally, for $m \leq n$ we have a truncation map $p^m\mathbb{Z}_p \to \mathbb{Z}/p^{n-m}\mathbb{Z}$ with kernel $p^n\mathbb{Z}_p$ fitting into an exact sequence

$$0 \to p^n\mathbb{Z}_p \to p^m\mathbb{Z}_p \to \mathbb{Z}/p^{n-m}\mathbb{Z} \to 0$$

inducing an isomorphism

$$p^m\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^{n-m}\mathbb{Z}$$

The first version was just the case $m = 0$.

Definition 6.2.7. Let $U_0 = \mathbb{Z}_p^\times$ and for $n \geq 1$, set

$$U_n = 1 + p^n\mathbb{Z}_p = \left\{1 + a_n p^n + a_{n+1}p^{n+1} + \cdots \in \mathbb{Z}_p^\times\right\}$$

Note that U_n is a subgroup of $\mathbb{Z}_p^\times$, and that there is a filtration

$$\mathbb{Z}_p^\times \supset 1 + p\mathbb{Z}_p \supset 1 + p^2\mathbb{Z}_p \supset \cdots \qquad U_0 \supset U_1 \supset U_2 \supset \cdots$$

Lemma 6.2.8. *There are exact sequences*

$$1 \longrightarrow 1 + p\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times \xrightarrow{\text{mod } p} (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow 1$$

$$1 \longrightarrow 1 + p^n\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times \xrightarrow{\text{mod } p^n} (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow 1$$

$$1 \longrightarrow 1 + p^{n+1}\mathbb{Z}_p \hookrightarrow 1 + p^n\mathbb{Z}_p \xrightarrow{1+p^n x \mapsto x \text{ mod } p} \mathbb{Z}/p\mathbb{Z} \longrightarrow 1$$

[2] *for $n \geq 1$ which induce isomorphisms*

$$U_0/U_1 \cong (\mathbb{Z}/p\mathbb{Z})^\times \qquad U_0/U_n \cong (\mathbb{Z}/p^n\mathbb{Z})^\times \qquad U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$$

Proof. Exactness is obvious by inspection, and the isomorphisms are immediate from the first isomorphism theorem. □

Definition 6.2.9. For $x \in \mathbb{Q}_p$, the **p-adic exponential** function is

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

and the **p-adic logarithm** is

$$\log(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$$

Note that at this point, these are both formal power series, but the next lemma determines their respective domains of convergence.

[2] The first sequence is redudant, as it is a special case of the second, but we include it anyway.

Lemma 6.2.10. *Let $f(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{Q}_p[[x]]$. Define*

$$r_f = \left(\limsup |a_n|_p^{1/n}\right)^{-1}$$

Then $f(x)$ converges for $|x|_p < r_f$ and diverges for $|x|_p > r_f$.

Proof. Proposition 4.3.1 of Gouvea [5]. Gouvea also gives a criterion for convergence on the "boundary" $|x|_p = r_f$ which is not included here. □

Lemma 6.2.11. *The p-adic logarithm and exponential have the following properties.*

1. *For $f(x) = \log(1+x)$, $r_f = 1$, so the domain of $\log(1+x)$ is $p\mathbb{Z}_p$ and the domain of $\log(x)$ is $1 + p\mathbb{Z}_p$.*
2. *For $f(x) = \exp(x)$, $r_f = p^{-1/(p-1)}$, so the domain of $\exp(x)$ is*

$$\begin{cases} p\mathbb{Z}_p & p \geq 3 \\ 4\mathbb{Z}_2 & p = 2 \end{cases}$$

3. *Whenever there is convergence, the following identities hold.*

$$\begin{aligned} \log(ab) &= \log a + \log b \\ \exp(a+b) &= (\exp a)(\exp b) \\ \exp\log a &= a \\ \log\exp a &= a \end{aligned}$$

Proof. Section 4.5 of Gouvea [5]. In particular, Lemma 4.5.1, Proposition 4.5.3, Lemma 4.5.5, Proposition 4.5.7, Proposition 4.5.8 □

Proposition 6.2.12. *If $p \geq 3$, then we have isomorphisms*

$$\mathbb{Z}_p \cong p\mathbb{Z}_p \underset{\log}{\overset{\exp}{\underset{\cong}{\rightleftarrows}}} 1 + p\mathbb{Z}_p = U_1$$

In the case $p = 2$ we have isomorphisms

$$\mathbb{Z}_2 \cong 4\mathbb{Z}_2 \underset{\log}{\overset{\exp}{\underset{\cong}{\rightleftarrows}}} 1 + 4\mathbb{Z}_2 = U_2$$

Proof. The isomorphisms given by exp and log follow from the previous lemma 6.2.11. The isomorphism $\mathbb{Z}_p \cong p\mathbb{Z}_p$ is given by $x \mapsto px$, and similarly $\mathbb{Z}_2 \cong 4\mathbb{Z}_2$ via $x \mapsto 4x$. See Proposition 4.5.9 of Gouvea [5] for more on this. □

Remark 6.2.13. Let p be odd. Under the isomorphism $\log : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$, the subgroup $U_n = 1 + p^n\mathbb{Z}_p \subset 1 + p\mathbb{Z}_p$ on the left side has image $p^n\mathbb{Z}_p$ on the right side, so the p-adic logarithm gives an isomorphism

$$U_n = 1 + p^n\mathbb{Z}_p \cong p^n\mathbb{Z}_p$$

Proposition 6.2.14 (Structure of $\mathbb{Z}_p^\times$)**.**

$$\mathbb{Z}_p^\times \cong \begin{cases} U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times & p \geq 3 \\ U_2 \times (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}_2 \times \{\pm 1\} & p = 2 \end{cases}$$

Proof. In light of the isomorphisms from Proposition 6.2.12, the first and second exact sequences of Lemma 6.2.8 give exact sequences below.

$$0 \longrightarrow \mathbb{Z}_p \cong U_1 \hookrightarrow \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow 0 \qquad p \geq 3$$

$$0 \longrightarrow \mathbb{Z}_2 \cong U_2 \hookrightarrow \mathbb{Z}_2^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \cong \{\pm 1\} \longrightarrow 0$$

We claim that these are split exact. For the $p = 2$ sequence, simply use the embedding

$$\{\pm 1\} \hookrightarrow \mathbb{Z}^\times \hookrightarrow \mathbb{Z}_2^\times$$

Splitting of the other sequence is more involved, so we omit some details. Basically, it suffices to find $(p-1)$st roots of unity in $\mathbb{Z}_p^\times$, since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$.

Consider $f(x) = x^{p-1} - 1 \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$. Over $\mathbb{F}_p$, this splits completely into $p-1$ distinct linear factors, and the derivative is $\overline{f'}(x) = (p-1)x^{p-2} \neq 0$, so by Hensel's lemma, all of the simple roots lift to roots in $\mathbb{Z}_p$. Thus $\mathbb{Z}_p$ contains all $(p-1)$st roots of unity.

See Corollary 4.5.10 of Gouvea [5] for some more details. Once the sequences split, we obtain exactly the claimed isomorphisms. □

Corollary 6.2.15 (Structure of $\mathbb{Q}_p^\times$)**.**

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times \cong \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times (\mathbb{Z}/p\mathbb{Z})^\times & p \geq 3 \\ \mathbb{Z} \times \mathbb{Z}_2 \times (\mathbb{Z}/4\mathbb{Z})^\times & p = 2 \end{cases}$$

Proof. Any element of $\mathbb{Q}_p^\times$ can be written uniquely as $p^n u$ where $u \in \mathbb{Z}_p^\times$, so we get an isomorphism

$$\mathbb{Q}_p^\times \to \mathbb{Z} \times \mathbb{Z}_p^\times \qquad p^n u \mapsto (n, u)$$

The rest is immediate from the structure of $\mathbb{Z}_p^\times$. □

6.2.2 Completions of $\mathbb{Q}$ are non-isomorphic

Remark 6.2.16. From the structure of $\mathbb{Q}_p^\times$ given in Corollary 6.2.15, and the fact that $\mathbb{Z}$ and $\mathbb{Z}_p$ are torsion-free, the torsion subgroup of $\mathbb{Q}_2$ is $(\mathbb{Z}/4\mathbb{Z})^\times$ and for $p \geq 3$ the torsion subgroup of $\mathbb{Q}_p^\times$ is $(\mathbb{Z}/p\mathbb{Z})^\times$. That is to say, the only roots of unity in $\mathbb{Q}_2$ are ± 1, and for $p \geq 3$ the only roots of unity in $\mathbb{Q}_p^\times$ are $(p-1)$st roots of unity.

Proposition 6.2.17. *The fields $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \ldots$ are all pairwise non-isomorphic (as abstract fields).*

Proof. According to the following table comparing the torsion subgroup of the multiplicative group, none of $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3$ is isomorphic to $\mathbb{Q}_5, \mathbb{Q}_5, \ldots$ and none of $\mathbb{Q}_5, \mathbb{Q}_7, \ldots$ are isomorphic to each other.

K	Torsion in $K^\times$
$\mathbb{R}$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_2$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_3$	$\mathbb{Z}/2\mathbb{Z} \cong \{\pm 1\}$
$\mathbb{Q}_p$, $p \geq 5$	$\mathbb{Z}/(p-1)\mathbb{Z}$

So it remains to check that $\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_3$ are pairwise non-isomorphic. For this, we consider the invariant $K^\times/K^{\times 2}$.

K	$K^\times/K^{\times 2}$	$\lvert K^\times/K^{\times 2}\rvert$
$\mathbb{R}$	$\mathbb{R}/\mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z}$	2
$\mathbb{Q}_2$	$(\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z})/2 \cong (\mathbb{Z}/2\mathbb{Z})^3$	8
$\mathbb{Q}_3$	$(\mathbb{Z} \times \mathbb{Z}_3 \times \mathbb{Z}/2\mathbb{Z})/2 \cong (\mathbb{Z}/2\mathbb{Z})^2$	4

Note that $\mathbb{Z}_3/2 = 0$ because 2 is a unit in $\mathbb{Z}_3$. Since these are all distinct, none of these are isomorphic either. □

Remark 6.2.18. Let p be an odd prime. One interesting consequence of $|\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}| = 4$ is that $\mathbb{Q}_p$ has exactly three quadratic field extensions (in a fixed algebraic closure), because any quadratice field extension is formed by adjoining a square root of a non-square.

6.2.3 The group of units $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic

Proposition 6.2.19. *Let p be an odd[3] prime and $n \in \mathbb{Z}_{\geq 1}$. The group of units $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic.*

Proof. By Lemma 6.2.8,

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong \mathbb{Z}_p^\times/U_n = \mathbb{Z}_p^\times/(1 + p^n\mathbb{Z}_p)$$

Using Proposition 6.2.14,

$$\mathbb{Z}_p^\times \cong U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times$$

Since $U_n \subset U_1$, in the quotient $\mathbb{Z}_p^\times/U_n \cong (U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times)/U_n$ the U_n lives entirely in the U_1 component, so

$$\mathbb{Z}_p^\times/U_n \cong (U_1 \times (\mathbb{Z}/p\mathbb{Z})^\times)/U_n \cong (U_1/U_n) \times (\mathbb{Z}/p\mathbb{Z})^\times$$

By Remark 6.2.13, $U_n \cong p^n\mathbb{Z}_p$, so

$$U_1/U_n = \frac{1 + p\mathbb{Z}_p}{1 + p^n\mathbb{Z}_p} \cong \frac{p\mathbb{Z}_p}{p^n\mathbb{Z}_p} \cong \mathbb{Z}/p^{n-1}\mathbb{Z}$$

The final isomorphism comes from Remark 6.2.6. Putting this together, we obtain

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong U_1/U_n \times (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times$$

Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, the product on the right is a product of cyclic groups of relatively prime orders, so it is cyclic. □

[3] This does fail for $p = 2$ for at least some values of n. As a counterexample, $(\mathbb{Z}/8\mathbb{Z})^\times$ is order four, but not cyclic, since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$.

6.3 Ramification

Definition 6.3.1. Let K be a complete nonarchimedean discretely valued field, and L/K a finite extension. Let k_K be the associated residue field of K and k_L the associated residue field of L. Note that $\mathcal{O}_K \subset \mathcal{O}_L$ and $\mathfrak{m}_K \subset \mathfrak{m}_L$, hence

$$k_K \hookrightarrow k_L$$

The **residual degree** is

$$f(L|K) = f_K^L = [k_K : k_L]$$

Definition 6.3.2. Let K be a complete nonarchimedean discretely valued field, and L/K a finite extension with $d = [L : K]$. Let $v_K : K^\times \to \mathbb{Z}$ be a normalized discrete valuation. Let $v_L : L^\times \to \mathbb{R}$ be the extension of v_K, and the we know that

$$\operatorname{im} v_L \subset \frac{1}{d}\mathbb{Z}$$

so v_L is also discrete. The **ramification degree** is

$$e(L|K) = e_K^L = e_{L/K} = [v_L(L^\times) : v_K(K^\times)]$$

That is, if π_K is a uniformizer for K and π_L is a uniformizer for L, then

$$(\pi_K) = \left(\pi_L^{e(L|K)}\right)$$

as ideals of $\mathcal{O}_L$.

Definition 6.3.3. Let $L, K, e_{L/K}, f_{L/K}$ be as above. If $e_{L/K} = 1$, then L/K is **unramified**. if $f_{L/K} = 1$, then L/K is **totally ramified**.

Proposition 6.3.4. *Let K be a complete nonarchimedean discretely valued field, and let L/K be a finite separable extension, with extended absolute value, such that the valuation on L is also discrete. Then $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L : K]$.*

Proposition 6.3.5. *Let K be a complete nonarchimedean discretely valued field, and L/K a finite extension, with extended absolute value. Assume that the residue fields k_K, k_L are perfect. Then*

$$[L : K] = e_{L/K} f_{L/K}$$

Proof. Let $d = [L : K]$. By Proposition 6.3.4, $\mathcal{O}_L \cong \mathcal{O}_K^d$ as an $\mathcal{O}_K$-module. Let π_K, π_L be uniformizers, that is,

$$(\pi_K) = \pi_K \mathcal{O}_K = \mathfrak{m}_K \qquad (\pi_L) = \pi_L \mathcal{O}_L = \mathfrak{m}_L$$

Then

$$\mathcal{O}_L/\pi_K\mathcal{O}_L \cong \mathcal{O}_K^d/\pi_k\mathcal{O}_K^d \cong (\mathcal{O}_K/\pi_K\mathcal{O}_K)^d \cong (k_K)^d$$

Recall that by definition of $e = e_{L/K}$, $(\pi_K) = (\pi_L^e)$. Consider the filtration

$$\begin{array}{ccccccccc} \mathcal{O}_L & \supset & \pi_L\mathcal{O}_L & \supset & \pi_L^2\mathcal{O}_L & \supset & \cdots & \supset & \pi_L^e\mathcal{O}_L = \pi_k\mathcal{O}_L \\ & & (\pi_L) & & (\pi_L^2) & & & & (\pi_L^e) = (\pi_k) \end{array}$$

Recall that by definition of $f = f_{L/K}$, we have $k_L \cong k_K^f$. At each step of the filtration, we have

$$\pi_L^i\mathcal{O}_K/\pi_L^{i+1}\mathcal{O}_L \cong \mathcal{O}_L/\pi_L\mathcal{O}_L \cong k_L \cong k_K^f$$

Since there are e steps in the filtration, and each step has successive quotient k_k^f, in total we have

$$\mathcal{O}_L/\pi_K\mathcal{O}_L \cong \left(k_K^f\right)^e = k_K^{ef}$$

Since this quotient is also k_K^d, we get $d = ef$ as desired. □

Proposition 6.3.6. *The indices e, f are "multiplicative in towers." More precisely, let K be a complete nonarchimedean discretely valued field, and let $K \subset L \subset M$ be a tower of finite extensions. Then*

$$e_K^M = e_L^M e_K^L \qquad f_K^M = f_L^M f_K^L$$

Proof. For f, this just follows from the tower law for field extensions.

$$f_K^M = [k_M : k_K] = [k_M : k_L][k_L : k_K] = f_L^M f_M^L$$

The result for e could probably be proved directly, but it also follows using the tower law for f, the tower law for $K \subset L \subset M$, and the previous result $[L : K] = e_K^L f_K^L$.

$$e_K^M = \frac{[M : K]}{f_K^M} = \frac{[M : L][L : K]}{f_L^M f_K^L} = \left(\frac{[M : L]}{f_L^M}\right)\left(\frac{[L : K]}{f_K^L}\right) = e_L^M e_K^L$$

□

Example 6.3.7. Let $K = \mathbb{Q}_5$ and $L = \mathbb{Q}_5(\sqrt{2})$, so $[L : K] = 2$. Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Note that

$$N_K^L(\sqrt{2}) = \sqrt{2}(-\sqrt{2}) = 2$$

so

$$|\sqrt{2}|_L = |2|_K^{1/2} = 1$$

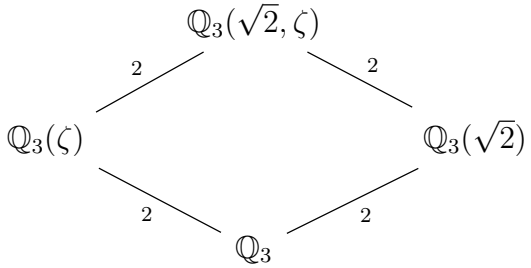
so $\sqrt{2} \in \mathcal{O}_L$. Thus there is an element of the residue field $k_L = \mathcal{O}_L/\mathfrak{m}_L$ which is a root of $x^2 - 2$. Since $x^2 - 2$ is irreducible over $k_K \cong \mathbb{F}_5$, the extension k_L/k_K has degree greater than 1, that is, $f > 1$. Since $ef = 2$, this forces $f = 2, e = 1$. Hence $\mathbb{Q}_5(\sqrt{2})$ is totally unramified over $\mathbb{Q}_5$.

Example 6.3.8. Let $K = \mathbb{Q}_5$ and $L = \mathbb{Q}_5(\sqrt{5})$, so $[L : K] = 2$. Normalize the discrete valuation on K so that $v_K(K^\times) = \mathbb{Z}$ and $v_L(L^\times) = \frac{1}{e}\mathbb{Z}$. Then

$$1 = v_L(5) = 2v_L(\sqrt{5}) \implies v_L(\sqrt{5}) = \frac{1}{2}$$

Thus $e \geq 2$, so $f = 1, e = 2$, and $\sqrt{5}$ is a uniformizer.

Example 6.3.9. Let $K = \mathbb{Q}_3$ and $L = \mathbb{Q}_3(\sqrt{2}, \zeta)$ where ζ is a primitive 3rd root of unity. Note that $[L : K] = 4$.



Note that ζ is a root of $x^2 + x + 1$ over $\mathbb{Q}_3$. By a similar argument as in Example 6.3.7,

$$e_{\mathbb{Q}_3}^{\mathbb{Q}_3(\sqrt{2})} = 1 \qquad f_{\mathbb{Q}_3}^{\mathbb{Q}_3(\sqrt{2})} = 2$$

Regarding $\mathbb{Q}_3(\zeta)$, we observe that

$$\begin{aligned} x^2 + x + 1 = (x - \zeta)(x - \zeta^2) &\implies 3 = (\zeta - 1)(\zeta^2 - 1) \\ &\implies v_{\mathbb{Q}_3(\zeta)}(3) = 1 = v_L(\zeta - 1) + v_L(\zeta^2 - 1) \end{aligned}$$

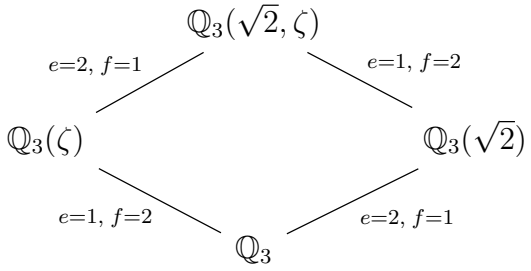
Since $\zeta - 1, \zeta^2 - 1$ are Galois conjugates, they have equal valuation. Hence

$$v_L(\zeta - 1) = \frac{1}{2}$$

so

$$e^{\mathbb{Q}_3(\zeta)}\mathbb{Q}_3 = 2 \qquad f_{\mathbb{Q}_3}^{\mathbb{Q}_3(\zeta)} = 1$$

Returning to our original diagram, we can write in the ramification and residual degrees we computed. Since all the extensions are degree 2, we can also deduce ramification and residual degrees for the upper extensions and the total extension L/K by multiplicativity in towers.



By multiplicativity in towers,

$$e_K^L = f_K^L = 2$$

6.4 Galois-type correspondence for unramified extensions

Proposition 6.4.1. *Let K be a complete nonarchimedean discretely valued field, with perfect residue field k_K. For a finite unramified extension L/K, by the primitive element theorem we can write L as $L = K(\alpha)$ for some $\alpha \in L$. Define*

$$k_L = k_K(\overline{\alpha})$$

This gives an inclusion-preserving bijection

$$\Psi : \{\text{finite unramified extensions of } K\} \to \{\text{finite extensions of } k_K\}$$
$$L = K(\alpha) \mapsto k_L = k_K(\overline{\alpha})$$

Furthermore, if L/K and L'/K are finite unramified extensions, there is an isomorphism

$$\mathrm{Hom}_K(L, L') \to \mathrm{Hom}_{k_K}(k_L, k_{L'})$$
$$\phi \mapsto \phi|_{\mathcal{O}_L} \bmod \mathfrak{m}_K$$

That is, the bijection Ψ is actually an equivalence of categories.

Proof. Theorem 7.50 of Milne [7]. □

Proposition 6.4.2. *Let K be as above, and let L/K be a finite unramified extension. Then*

$$\mathrm{Aut}(L/K) \cong \mathrm{Aut}(k_L/k_K)$$

Thus L/K is Galois if and only if k_L/k_K is Galois and in this case,

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K)$$

Proof. A finite extension L/K is Galois if and only if K is the fixed field of $\mathrm{Aut}(L/K)$. By the equivalence of categories above, $\mathrm{Aut}(L/K) \cong \mathrm{Aut}(k_L/k_k)$, and K is the fixed field of $\mathrm{Aut}(L/K)$ if and only k_K is the fixed field of $\mathrm{Aut}(k_L/k_K)$. □

Example 6.4.3. Let p be a prime, and let K be a complete local field with residue field $k_K = \mathbb{F}_p$. [4] Since $\mathbb{F}_p$ has a unique finite extension of degree n for each $n \in \mathbb{Z}_{\geq 1}$, K has a unique unramified extension L_n of degree n for each $n \in \mathbb{Z}_{\geq 1}$. Concretely in the case $K = \mathbb{Q}_p$, we have

$$L_n = \mathbb{Q}_p(\mu_{p^n-1})$$

where μ_{p^n-1} is the group of $p^n - 1$ roots of unity. To point out the blatantly obvious, L_n corresponds to the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$, and

$$\mathrm{Gal}(L_n/K) \cong \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

Proposition 6.4.4. *Let K be a complete nonarchimedean discretely valued field, with perfect residue field k_K, and let L/K be a finite separable extension. There exists a unique subextension K^{un} such that L/K^{un} is totally ramified and K^{un}/K is unramified.*

$$\begin{array}{c} L \\ \Big| f=1 \text{ totally ramified} \\ K^{\mathrm{un}} \\ \Big| e=1 \text{ unramified} \\ K \end{array}$$

[4] For concreteness, take $K = \mathbb{Q}_p$ or $K = \mathbb{F}_{p^n}((t))$, the field of formal power series. Actually, there is a classification theorem to say that all such nonarchimedean fields are a finite extension of one of these two types.

*K^{un} is called the **maximal unramified extension of** K **in** L. If L/K is infinite, we may still find a maximal unramified extension K^{un}/L, in the sense that for any unramified extesion E/K, $E \subset K$, although we can no longer guarantee that L/K^{un} is totally ramified in this case.*

Proof. First, assume L/K is finite. Since k_L/k_K is a finite extension, by the Proposition 6.4.1, there exists a unique unramified extension K^{un}/K such that $k_L \cong k_{K^{\mathrm{un}}}$. By multiplicativity in towers, $f^L_{K^{\mathrm{un}}} = 1$.

Now suppose L/K is infinite. Then we construct K^{un} as the compositum of all finite unramified extensions E/K, noting that the compositum of unramified extensions is unramified. Then by construction, K^{un} contains all unramified extensions of K. □

Example 6.4.5. Let $K = \mathbb{Q}_3, L = \mathbb{Q}_3(\sqrt{2}, \zeta)$ where ζ is a primitive 3rd root of unity. We considered this example previously in Example 6.3.9, and saw that $\mathbb{Q}_3(\sqrt{2})$ is the maximal unramified subextension.

Definition 6.4.6. Let K be a complete nonarchimedean local field with perfect residue field k_K [5], and fix a separable closure K^{sep}. Then by Proposition 6.4.4, there is a maximal unramified extesion $K^{\mathrm{un}} \subset K^{\mathrm{sep}}$, called the **maximal unramified extension of** K. By construction an intermediate extesion $K \subset E \subset K^{\mathrm{sep}}$ is unramified if and only if $E \subset K^{\mathrm{un}}$.

6.5 Assorted exercises from Gouvea [5]

Proposition 6.5.1 (Exercise 113 of Gouvea [5])**.** *Let p be a prime and m an integer such that $\gcd(m, p) = 1$. Then $\gcd(m, p-1) > 1$ if and only if there exists $\alpha \in \mathbb{Z}$ such that $\alpha^m \equiv 1 \bmod p$ and $\alpha \not\equiv 1 \bmod p$. Furthermore, for any such α, the least integer m such that $\alpha^m \equiv 1 \bmod p$ is a divisor of $p-1$.*

Proof. ($\implies$) Note that $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ so if $d = \gcd(m, p-1) > 1$, then $\mathbb{F}_p^\times$ has a subgroup of order d. Let $\alpha \in \mathbb{Z}$ be a representative of the generator of the subgroup of order d, so that $\alpha^d \equiv 1 \bmod p$. Then

$$\alpha^m \equiv (\alpha^d)^{m/d} \equiv 1^{m/d} \equiv 1 \bmod p$$

and $\alpha \not\equiv 1 \bmod p$ since α generates a nontrivial subgroup.

($\impliedby$) Suppose α exists. Then α generates a nontrivial proper subgroup of $\mathbb{F}_p^\times$ of order dividing m, so that order divies m and $p-1$, hence $\gcd(m, p-1) > 1$.

Regarding the "furthermore" statement, the least m such that $\alpha^m \equiv 1 \bmod p$ is the order of the subgroup of $\mathbb{F}_p^\times$ generated by α so it divides the order of $\mathbb{F}_p^\times$ which is $p-1$. □

Proposition 6.5.2 (Exercise 126 of Gouvea [5])**.** *Let p be an odd prime and $n \in \{0, 1, \ldots, p-2\}$. Then*

$$\sum_{x \in \mathbb{F}_p} x^n = 0$$

[5] Is this necessary? Milne [8] includes it in Corollary 7.52, so I've kept it.

Proof. For $n = 0$ this is clear, assuming we take $0^0 = 1$. For $n \neq 0$, we can rewrite the sum as a sum over $\mathbb{F}_p^\times$, and it becomes a geometric series. Let α be a generator of $\mathbb{F}_p^\times$, so that $\alpha^{p-1} = 1$.

$$\sum_{x \in \mathbb{F}_p^\times} x^n = \sum_{k=1}^{p-1} (\alpha^k)^n = \sum_{k=1}^{p-1} (\alpha^n)^k = \alpha^n \left(\frac{1 - (\alpha^n)^{p-1}}{1 - \alpha^n} \right) = \alpha^n \left(\frac{0}{1 - \alpha^n} \right) = 0$$

□

Proposition 6.5.3 (Exercise 161 of Gouvea [5])**.** *If p is an odd prime, then $\log_p(x) = 0$ if and only if $x = 1$. If $p = 2$, then $\log_p(x) = 0$ if and only if $x = \pm 1$.*

Proof. Let p be an odd prime. First, it is clear that $\log_p(1)$. Conversely, for $y \in \mathbb{Z}_p$,

$$\log_p(1 + py) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{p^n}{n} y^n$$

(This converges for $y \in \mathbb{Z}_p$.) By Strassman's theorem, this has at most N zeroes where $N = 1$ because

$$|a_1| \frac{1}{p} > |a_2|, |a_3|, \ldots$$

using the fact that $p > 2$. So 1 is the only zero of $\log_p$. Now consider the case $p = 2$. It is clear that $\log_2(1) = 0$. Also

$$2 \log_2(-1) = \log_2((-1)^2) = \log_2(1) = 0 \implies \log_2(-1) = 0$$

Consider the "same" power series as above

$$\log_2(1 + 2y) = \frac{2}{1} y - \frac{2^2}{2} y^2 + \frac{2^3}{3} y^3 - \cdots$$

Applying Strassman's theorem again, we get $N = 2$ so there are at most 2 zeroes of this, so ± 1 are all of the zeroes. □

6.6 A concrete failure of the Hasse principle

The Hasse principle asserts that "global" information is related to "local" information, in the sense that existence of solutions in $\mathbb{Q}$ to some equation are related to existence of solutions in all local field completions of $\mathbb{Q}$, namely $\mathbb{Q}_p$ for all p and $\mathbb{R}$. This is exactly true in the case of quadratic forms - the Hass-Minkowsi theorem says that a quadratic form has a solution in $\mathbb{Q}$ if and only if there is a solution in every $\mathbb{Q}_p$ and a solution in $\mathbb{R}$. However, it fails for higher degree forms, as given by the following example.

Lemma 6.6.1. *Let p be an odd prime, and let a, b be quadratic non-residues mod p. Then ab is a quadratic residue mod p.*

Proof. If a, b are both non-residues, they both represent the same nontrivial class in $\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$ (this isomorphism uses the fact that $p-1$ is even). Then ab represents the trivial class, that is, $ab \in \mathbb{F}_p^{\times 2}$. □

Proposition 6.6.2. *The equation*

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0$$

has a root in $\mathbb{Q}_p$ for all primes p and in $\mathbb{R}$, but no root in $\mathbb{Q}$.

Proof. It is clear that there is no root in $\mathbb{Q}$, since $2, 17$, and 34 are not squares, and it is clear that there are roots in $\mathbb{R}$. Since $17 \equiv 1 \bmod 8$, by Proposition 6.1.24, there is a root of $x^2 - 17$ in $\mathbb{Q}_2$.

Now let p be an odd prime. It suffices to show that at least one of $2, 17, 34$ is a square in $\mathbb{Q}_p$. By Proposition 6.1.24, if $u \in \mathbb{Q}_p^\times$ is a quadratic residue mod p, then it is a square in $\mathbb{Q}_p$. If either 2 or 17 is a quadratic residue mod p, we are done. If both are non-residues, then by Lemma 6.6.1, then $34 = (2)(17)$ is a quadratic residue, so it is a square in $\mathbb{Q}_p$. □

Remark 6.6.3. The proof of the previous proposition actually yields an infinite family of equations for which the Hasse principle fails. For any prime of the form $p = 8k + 1$, and the proof above shows that

$$(x^2 - 2)(x^2 - p)(x^2 - 2p) = 0$$

has a solution in every $\mathbb{Q}_p$ and in $\mathbb{R}$ but no solutions in $\mathbb{Q}$.

Bibliography

[1] J.W.S. Cassels and A. Frohlich. Algebraic number theory, 1967.

[2] David Cox. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, 1989.

[3] David S. Dummit and Richard M. Foote. Abstract algebra, third edition, 2004.

[4] Philippe Gille and Tamás Szamuely. Central simple algebras and group cohomology, 2006.

[5] Fernando Q. Gouvea. P-adic numbers, 1997.

[6] Serge Lang. Algebra.

[7] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.

[8] James S. Milne. Fields and galois theory (v4.60), 2018. Available at www.jmilne.org/math/.

[9] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[10] J. Milnor. Introduction to algebraic k-theory, 1972.

[11] R.S. Pierce. Associative algebras, 1982.

[12] Igor Rapinchuk. The brauer group of a field. Available at https://drive.google.com/file/d/0B0CCc00SqXL4dTBIbU8xa0Vjb2c/edit.

[13] Jonathan Rosenberg. Algebraic k-theory and its applications, 1994.

[14] J.P. Serre. Local fields, 1979.

[15] Romyar Sharifi. Group and galois cohomology. Available at http://math.ucla.edu/ sharifi/groupcoh.pdf.

[16] Charles A. Weibel. An introduction to homological algebra, 1994.