Algebraic Number Theory, a Computational Approach

William Stein

August 20, 2020

Chapter 1

Galois Cohomology

Let G be a group and suppose G acts on an abelian group A (defined below). In this chapter we will study abelian groups attached to the action of G on A. These are called *cohomology groups* and denoted by $H^n(G, A)$. The theory of these groups is referred to as *group cohomology*. In the later sections G will represent the Galois group of a field extension. This is called *Galois cohomology*. Studying Galois cohomology helps us understand the structure of Galois groups such as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.1 Group Rings and Modules

In this section we define group modules, which are analogous to modules over a ring. For a review of the theory of modules over a ring see [DF04, Ch. 10].

Definition 1.1.1. Let G be any group. The *group ring* $\mathbb{Z}[G]$ of G is the free abelian group (equivalently the free $\mathbb{Z}$-module) on the elements of G equipped with multiplication given by the group structure on G. Note that $\mathbb{Z}[G]$ is a commutative ring if and only if G is abelian.

Example 1.1.2. For example, the group ring of the cyclic group $C_n = \langle a \rangle$ of order n is the free $\mathbb{Z}$-module on $1, a, \ldots, a^{n-1}$, and the multiplication is induced by $a^i a^j = a^{i+j} = a^{i+j \pmod n}$ extended linearly. For example, in $\mathbb{Z}[C_3]$ we have

$$(1 + 2a)(1 - a^2) = 1 - a^2 + 2a - 2a^3 = 1 + 2a - a^2 - 2 = -1 + 2a - a^2.$$

Since $a^3 = 1$ you might think that $\mathbb{Z}[C_3]$ is isomorphic to the ring $\mathbb{Z}[\zeta_3]$ of integers of $\mathbb{Q}(\zeta_3)$, but you would be wrong, since the ring of integers is isomorphic to $\mathbb{Z}^2$ as an abelian group, but $\mathbb{Z}[C_3]$ is isomorphic to $\mathbb{Z}^3$ as abelian group. Note that $\mathbb{Q}(\zeta_3)$ is a quadratic extension of $\mathbb{Q}$.

Exercise 1.1.3. Is $\mathbb{Z}[\zeta_3]$ isomorphic to the group ring of some group?

Hint: Note that the rank of the group ring as a $\mathbb{Z}$-module is equal to the size of the group. If $\mathbb{Z}[\zeta_3]$ was a group ring then it would have to be isomorphic to $\mathbb{Z}[C_2]$.

Exercise 1.1.4.

(a) Write down any two elements of $\mathbb{Z}[\mathbb{Z}]$ and multiply them. This is not hard, but is good practice with the concept of a group ring.

(b) Show $\mathbb{Z}[\mathbb{Z}]$ is isomorphic to $\mathbb{Z}\left[x, \frac{1}{x}\right]$.

Definition 1.1.5. Let G be a finite group. A *G-module* is an abelian group A equipped with a left action of G, i.e., a group homomorphism $G \to \operatorname{Aut}(A)$, where $\operatorname{Aut}(A)$ denotes the group of group isomorphisms $A \to A$ with the operation of function composition.

Exercise 1.1.6. Fix an abelian group A. Show the following are equivalent sets of data. Specifically, given any one of the following objects, there is a natural way to construct another.

(a) A group homomorphism $G \to \operatorname{Aut}(A)$.

(b) A map $\rho : G \times A \to A$ such that for all $g, h \in G$ and $a, b \in A$,

  (i) $\rho(g, a + b) = \rho(g, a) + \rho(g, b)$

  (ii) $\rho(e, a) = a$ where e is the identity in G.

  (iii) $\rho(gh, a) = \rho(g, \rho(h, a))$

(c) A ring homomorphism $\mathbb{Z}[G] \to \operatorname{End}(A)$.

(d) A map $\rho : \mathbb{Z}[G] \times A \to A$ with the same properties listed in (b).

Remark 1.1.7. In Exercise 1.1.6, part (a) is our definition of a G-module and parts (c) and (d) are the data of a $\mathbb{Z}[G]$-module. This shows that a G-module in the above sense is the same as a $\mathbb{Z}[G]$-module in the usual module sense.

Example 1.1.8. If G is any finite group and A any abelian group then we can always make A into a G-module by giving it the trivial action. In particular, $\mathbb{Z}$ with the trivial action is a module over any group G, as is $\mathbb{Z}/m\mathbb{Z}$ for any positive integer m. Another example is $G = (\mathbb{Z}/n\mathbb{Z})^*$, which acts via multiplication on $A = \mathbb{Z}/n\mathbb{Z}$.

Remark 1.1.9. The construction $\mathbb{Z}[G]$ from G is natural, in the sense that it defines a functor between categories. Moreover, $\mathbb{Z}[G]$ is the most natural way to construct a ring from a group in the sense that the group ring functor is a left adjoint to the forgetful functor from rings to groups. These types of functors are sometimes called "free" functors. If you are interested in free objects, see if you can come up with a natural way to add structure to other objects. Could you make a set into a group? How about a vector space?

1.2 Group Cohomology

Let G be a finite group and A a G-module. For each integer $n \geq 0$ there is an abelian group $H^n(G, A)$ called the *nth cohomology group of G acting on A*. The general definition is somewhat complicated, but the definition for $n \leq 1$ is fairly concrete. For example, the 0*th cohomology group*

$$H^0(G, A) = \{x \in A : \sigma x = x \text{ for all } \sigma \in G\} = G^A$$

is the subgroup of elements of A that are fixed by every element of G.

The *first cohomology group*

$$H^1(G, A) = C^1(G, A)/B^1(G, A)$$

is the group C^1 of 1-*cocycles* modulo the group B^1 of 1-*coboundaries*, where

$$C^1(G, A) = \{f : G \to A \text{ such that } f(\sigma\tau) = f(\sigma) + \sigma f(\tau)\}$$

where the maps $f : G \to A$ range over all set-theoretic maps. If we let $f_a : G \to A$ denote the set-theoretic map $f_a(\sigma) = \sigma(a) - a$, then

$$B^1(G, A) = \{f_a : a \in A\}.$$

There are also explicit, and increasingly complicated, definitions of $H^n(G, A)$ for each $n \geq 2$ in terms of *crossed homomorphisms*, which are certain maps $G \times \cdots \times G \to A$ modulo a subgroup. We will not need these maps, but for more information about them see [Cp86, Ch. IV.2].

Exercise 1.2.1. Suppose G acts trivially on A. Show that $B^1(G, A) = 0$ and $C^1(G, A) \cong \mathrm{Hom}(G, A)$. In particular, this shows $H^1(G, A) \cong \mathrm{Hom}(G, A)$. Deduce that if $A = \mathbb{Z}$ then $H^1(G, \mathbb{Z}) = 0$. Here $\mathrm{Hom}(G, A)$ represents the set of group homomorphisms from G to A. It comes with a natural group structure given by $(f_1 + f_2)(a) = f_1(a) + f_2(a)$.

[*Hint*: For any $\sigma \in G$ we have $f_a(\sigma) = \sigma(a) - a = a - a = 0$. Also for any finite group G, show that $\mathrm{Hom}(G, \mathbb{Z}) = 0$.]

Example 1.2.2. The groups $H^n(G, \mathbb{Z})$ and $H^n(G, \mathbb{Z}/p\mathbb{Z})$ (where p is a prime) are computable in Sage. For example we can compute $H^{10}(A_5, \mathbb{Z})$ and $H^7(A_5, \mathbb{Z}/5\mathbb{Z})$ where A_5 is the alternating group of order 120 and $\mathbb{Z}/5\mathbb{Z}$ is given the trivial A_5-module structure.

```
G = AlternatingGroup(5); G
```

```
Alternating group of order 5!/2 as a permutation group
```

```
G.cohomology(10)
```

```
Multiplicative Abelian group isomorphic to C2 x C2
```

```
G.cohomology(7,5)
```

```
Multiplicative Abelian group isomorphic to C5
```

1.2.1 The Main Theorem

Definition 1.2.3. If X is any abelian group, then $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ is a G-module, see Exercise 1.2.4. We call a module constructed in this way *coinduced*.

Exercise 1.2.4. Let X be any abelian group. Show that $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ is a G-module with the action induced by $(g \cdot f)(h) = f(hg)$ for all $g \in G$, $f \in \mathrm{Hom}(\mathbb{Z}[G], X)$, and $h \in \mathbb{Z}[G]$.

The following theorem gives three properties of group cohomology, which uniquely determine group cohomology.

Theorem 1.2.5. *Suppose G is a finite group. Then*

1. *We have $H^0(G, A) = A^G$.*
2. *If A is a coinduced G-module, then $H^n(G, A) = 0$ for all $n \geq 1$.*
3. *If $0 \to A \to B \to C \to 0$ is any exact sequence of G-modules, then there is a long exact sequence*

$$
\begin{tikzcd}
0 \arrow[r] & H^0(G,A) \arrow[r] & H^0(G,B) \arrow[r] & H^0(G,C) \arrow[dll] & \\
& H^1(G,A) \arrow[r] & H^1(G,B) \arrow[r] & H^1(G,C) \arrow[dl] & \\
& & \cdots \arrow[dl] & & \\
& H^n(G,A) \arrow[r] & H^n(G,B) \arrow[r] & H^n(G,C) \arrow[dll] & \\
& H^{n+1}(G,A) \arrow[r] & H^{n+1}(G,B) \arrow[r] & H^{n+1}(G,C) \arrow[r] & \cdots
\end{tikzcd}
$$

Moreover, the functor $H^n(G,-)$ is uniquely determined by these three properties.

We will not prove this theorem. For proofs see [Cp86, Atiyah-Wall] and [Ser79, Ch. 7]. The properties of the theorem uniquely determine group cohomology, so one should in theory be able to use them to deduce anything that can be deduced about cohomology groups. Indeed, in practice one frequently proves results about higher cohomology groups $H^n(G,A)$ by writing down appropriate exact sequences, using explicit knowledge of H^0, and chasing diagrams.

Remark 1.2.6. Alternatively, we could view the defining properties of the theorem as the definition of group cohomology, and could state a theorem that asserts that group cohomology exists.

Remark 1.2.7. For those familiar with commutative and homological algebra, we have

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

where $\mathbb{Z}$ is the trivial G-module.

Remark 1.2.8. One can interpret $H^2(G,A)$ as the group of equivalence classes of extensions of G by A, where an extension is an exact sequence

$$0 \to A \to M \to G \to 1$$

such that the induced conjugation action of G on A is the given action of G on A. (Note that G acts by conjugation, as A is a normal subgroup since it is the kernel of a homomorphism.)

1.2.2 Example Application of the Theorem

For example, let's see what we get from the exact sequence

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

where m is a positive integer, and $\mathbb{Z}$ has the structure of trivial G module. By definition we have $H^0(G,\mathbb{Z}) = \mathbb{Z}$ and $H^0(G,\mathbb{Z}/m\mathbb{Z}) = \mathbb{Z}/m\mathbb{Z}$. The long exact sequence begins

$$\begin{array}{l} 0 \longrightarrow \mathbb{Z} \xrightarrow{\quad m \quad} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \\ \longrightarrow H^1(G,\mathbb{Z}) \xrightarrow{[m]} H^1(G,\mathbb{Z}) \longrightarrow H^1(G,\mathbb{Z}/m\mathbb{Z}) \\ \longrightarrow H^2(G,\mathbb{Z}) \xrightarrow{[m]} H^2(G,\mathbb{Z}) \longrightarrow H^2(G,\mathbb{Z}/m\mathbb{Z}) \longrightarrow \cdots \end{array}$$

From the first few terms of the sequence and the fact that $\mathbb{Z}$ surjects onto $\mathbb{Z}/m\mathbb{Z}$, we see that $[m] : H^1(G,\mathbb{Z}) \to H^1(G,\mathbb{Z})$ is injective. This is consistent with Exercise 1.2.1 above that showed $H^1(G,\mathbb{Z}) = 0$. Using this vanishing and the right side of the exact sequence we obtain an isomorphism

$$H^1(G,\mathbb{Z}/m\mathbb{Z}) \cong H^2(G,\mathbb{Z})[m]$$

where $H^2(G,\mathbb{Z})[m]$ is the kernel of the map $[m] : H^2(G,\mathbb{Z}) \to H^2(G,\mathbb{Z})$. By Exercise 1.2.1, when a group acts trivially the H^1 is Hom, so

$$H^2(G,\mathbb{Z})[m] \cong \mathrm{Hom}(G,\mathbb{Z}/m\mathbb{Z}). \tag{1.1}$$

One can prove that for any $n > 0$ and any module A that the group $H^n(G,A)$ has exponent dividing $\#G$ (see Remark 1.3.5 and Exercise 1.3.6). Thus (1.1) allows us to understand $H^2(G,\mathbb{Z})$, and this comprehension arose naturally from the properties in Theorem 1.2.5 that determine the cohomology groups H^n.

1.3 Inflation and Restriction

Suppose H is a subgroup of a finite group G and A is a G-module.

For each $n \geq 0$, there is a natural map

$$\mathrm{res}_H : H^n(G,A) \to H^n(H,A)$$

called *restriction*. Elements of $H^n(G, A)$ can be viewed as classes of n-cocycles, which are certain maps $G \times \cdots \times G \to A$. From this perspective res_H takes a map to its restriction $H \times \cdots \times H \to A$. This is equivalent to precomposing with the natural inclusion $H \times \cdots \times H \to G \times \cdots \times G$.

If H is a normal subgroup of G, there is also an *inflation* map

$$\inf_H : H^n(G/H, A^H) \to H^n(G, A),$$

given by taking a cocycle $f : G/H \times \cdots \times G/H \to A^H$ and precomposing with the quotient map $G \to G/H$ to obtain a cocycle for G.

Exercise 1.3.1. Let $G = \mathbb{Z}/12\mathbb{Z}$, H the subgroup generated by 6, and $A = \mathbb{Z}/5\mathbb{Z}$. How many ways can G act on A? Pick a nontrivial action and compute A^H. How does G/H act on A^H?

The following proposition will be useful when proving the weak Mordell-Weil theorem (see Theorem **??**).

Proposition 1.3.2. *Suppose H is a normal subgroup of G. Then there is an exact sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\inf_H} H^1(G, A) \xrightarrow{\mathrm{res}_H} H^1(H, A).$$

Proof. Our proof follows [Ser79, pg. 117] closely.

We see that $\mathrm{res} \circ \inf = 0$ since on cocycles the composition is defined by precomposing with $H \to G \to G/H$, which gives the trivial map. It remains to prove that $\inf_H$ is injective and that the image of $\inf_H$ contains the kernel of res_H.

1. *(That $\inf_H$ is injective):* Suppose $f : G/H \to A^H$ is a cocycle whose image in $H^1(G, A)$ is equivalent to 0 modulo coboundaries. Then there is an $a \in A$ such that $f(\sigma) = \sigma a - a$, where we identify f with the map $G \to A$ that is constant on the cosets of H. But f depends only on the coset of σ modulo H, so $\sigma a - a = \sigma\tau a - a$ for all $\tau \in H$, i.e., $\tau a = a$ (as we see by adding a to both sides and multiplying by σ^{-1}). Thus $a \in A^H$, so f is equivalent to 0 in $H^1(G/H, A^H)$.

2. *(The image of $\inf_H$ contains the kernel of res_H):* Suppose $f : G \to A$ is a cocycle whose restriction to H is a coboundary, i.e., there is $a \in A$ such that $f(\tau) = \tau a - a$ for all $\tau \in H$. Subtracting the coboundary $g(\sigma) = \sigma a - a$ for $\sigma \in G$ from f, we may assume $f(\tau) = 0$ for all $\tau \in H$. Examing the equation $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ with $\tau \in H$

shows that f is constant on the cosets of H. Again using this formula, but with $\sigma \in H$ and $\tau \in G$, we see that

$$f(\tau) = f(\sigma\tau) = f(\sigma) + \sigma f(\tau) = \sigma f(\tau),$$

so the image of f is contained in A^H. Thus f defines a cocycle $G/H \to A^H$, i.e., is in the image of $\inf_H$.

□

Example 1.3.3. The sequence of Proposition 1.3.2 need not be surjective on the right. For example, suppose $H = A_3 \subset S_3$, and let S_3 act trivially on the group $\mathbb{Z}/3\mathbb{Z}$. Using the Hom interpretation of H^1, we see that $H^1(S_3/A_3, \mathbb{Z}/3\mathbb{Z}) = H^1(S_3, \mathbb{Z}/3\mathbb{Z}) = 0$, but $H^1(A_3, \mathbb{Z}/3\mathbb{Z})$ has order 3. We can compute this example in Sage as follows.

```
S3 = SymmetricGroup(3); S3
```

```
Symmetric group of order 3! as a permutation group
```

```
S3.cohomology(1,3)
```

```
Trivial Abelian group
```

```
A3 = AlternatingGroup(3); A3
```

```
Alternating group of order 3!/2 as a permutation group
```

```
A3.cohomology(1,3)
```

```
Multiplicative Abelian group isomorphic to C3
```

Remark 1.3.4. One generalization of Proposition 1.3.2 is to a more complicated exact sequence involving the "transgression map" tr:

$$0 \to H^1(G/H, A^H) \xrightarrow{\inf_H} H^1(G, A) \xrightarrow{\mathrm{res}_H} H^1(H, A)^{G/H} \xrightarrow{\mathrm{tr}} H^2(G/H, A^H) \to H^2(G, A).$$

Another generalization of Proposition 1.3.2 is that if $H^m(H, A) = 0$ for $1 \le m < n$, then there is an exact sequence

$$0 \to H^n(G/H, A^H) \xrightarrow{\inf_H} H^n(G, A) \xrightarrow{\mathrm{res}_H} H^n(H, A).$$

For more information see [Ser79, Ch. VII.6].

Remark 1.3.5. If H is a not-necessarily-normal subgroup of G, there are also maps

$$\mathrm{cores}_H : H^n(H, A) \to H^n(G, A)$$

for each n. For $n = 0$ this is the trace map $a \mapsto \sum_{\sigma \in G/H} \sigma a$, but the definition for $n \geq 1$ is more involved. One has $\mathrm{cores}_H \circ \mathrm{res}_H = [\#(G/H)]$.

Exercise 1.3.6. Suppose G is a finite group and A is a finite G-module. Prove that for any n, the group $H^n(G, A)$ is a torsion abelian group of exponent dividing the order $\#A$ of A.

1.4 Galois Cohomology

Suppose L/K is a finite Galois extension of fields (recall that Galois here means is normal and separable), and A is a $\mathrm{Gal}(L/K)$-module. Put

$$H^n(L/K, A) = H^n(\mathrm{Gal}(L/K), A).$$

Following Section **??**, we can put a topology on $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ by taking as a basis of the origin, subgroups of the form $\mathrm{Gal}(K^{\mathrm{sep}}/L)$ where L/K is a finite Galois extension.

Exercise 1.4.1. Let H be a subgroup of $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Show that H is open if and only if H is closed and has finite index in G.

[*Hint*: If H is open then it contains a basis element N. By definition of the basis described above, N is finite index in G. What does this say about the index of H in G? What about the complement of H?]

Definition 1.4.2. Let A be a $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. We say that A is a *continuous* $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module if the map $\mathrm{Gal}(K^{\mathrm{sep}}/K) \times A \to A$ (see Exercise 1.1.6) is continuous when A has the discrete topology.

Exercise 1.4.3. Let $G = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and A be a G-module. Show that A is a continuous G-module if and only if the subgroup $G_a = \{\sigma \in G : \sigma(a) = a\}$ is open for every $a \in A$.

Now let A be a continuous $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. Let

$$A(L) = A^{\mathrm{Gal}(K^{\mathrm{sep}}/L)} = \{x \in A : \sigma(x) = x \text{ for all } \sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/L)\}.$$

and define

$$H^n(K, A) = \varinjlim_{L/K} H^n(L/K, A(L)),$$

where the limit is taken over all finite Galois extensions L/K.

It is not obvious that the groups $H^n(K, A)$ are actually cohomology groups, i.e., they satisfy the conclusion of Theorem 1.2.5. However one can show they have analogous properties; see [Ser79, Ch. X.3] for references.

Remark 1.4.4. Those familiar with algebraic geometry should compare the groups $H^n(K, A)$ with the Čech cohomology groups on the étale site over $\operatorname{Spec} K$. One can show that Čech cohomology agrees with the derived functor groups of $A \mapsto A^G$, see [Mil80, Ch. 10]. Therefore $H^n(K, A)$ do indeed define a cohomology theory.

Example 1.4.5. The following are examples of continuous $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules:

$$\overline{\mathbb{Q}}, \quad \overline{\mathbb{Q}}^*, \quad \overline{\mathbb{Z}}, \quad \overline{\mathbb{Z}}^*, \quad E(\overline{\mathbb{Q}}), \quad E(\overline{\mathbb{Q}})[n], \quad \mathrm{Tate}_\ell(E),$$

where E is an elliptic curve over $\mathbb{Q}$. Can you identify the action for each module A? What about $A(L)$ for any finite Galois extension $L/\mathbb{Q}$? It is important to notice that $\overline{\mathbb{Q}}^*(L) = L^*$.

Theorem 1.4.6 (Hilbert 90)**.** *We have* $H^1(K, \overline{K}^*) = 0$.

Proof. Our proof follows [Ser79, pg. 150] closely.

Because $H^1(K, \overline{K}^*) = \varinjlim_{L/K} H^1(L/K, L^*)$ It suffices to prove $H^1(L/K, L^*) = 0$ for every finite Galois extension L/K. Let $G = \mathrm{Gal}(L/K)$ and f be a 1-cocycle so that $f : G \to L^*$ such that $f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$. Here " $\cdot$ " represents multiplication in L^*. A standard fact from Galois theory is that the elements of G are L linearly independent. Hence we can find some $c \in L$ such that

$$b = \sum_{\tau \in G} f(\tau) \cdot \tau(c) \neq 0.$$

Now apply σ to both sides to get

$$\begin{aligned}
\sigma(b) &= \sum_{\tau \in G} \sigma(f(\tau)) \cdot \sigma\tau(c) \\
&= \sum_{\tau \in G} f(\sigma)^{-1} \cdot f(\sigma\tau) \cdot \sigma\tau(c) \\
&= f(\sigma)^{-1} \cdot \sum_{\tau \in G} f(\sigma\tau) \cdot (\sigma\tau)(c) \\
&= f(\sigma)^{-1} \cdot b.
\end{aligned}$$

This shows f is a coboundary. Specifically, it shows $f = f_{b^{-1}}$ in the notation we used to define coboundaries above. $\square$

Exercise 1.4.7. Let $K = \mathbb{Q}(\sqrt{5})$ and let $A = U_K$ be the group of units of K, which is a module over the group $G = \mathrm{Gal}(K/\mathbb{Q})$. Compute the cohomology groups $H^0(G, A)$ and $H^1(G, A)$. (You shouldn't use a computer, except maybe to determine U_K.)

Exercise 1.4.8. Let $K = \mathbb{Q}(\sqrt{-23})$ and let C be the class group of $\mathbb{Q}(\sqrt{-23})$, which is a module over the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Determine $H^0(G, C)$ and $H^1(G, C)$.

Bibliography

[Cp86] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, London, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], 1986, Reprint of the 1967 original.

[DF04] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Wiley, 2004.

[Mil80] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980. MR 81j:14002

[Ser79] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.