A Short Course on Galois Cohomology

William Stein

Spring 2010

Contents

1 Preface

These are the notes from a one-quarter course on Galois cohomology, which the author taught at University of Washington in 2010. They are mostly based on the best parts of [AW67] and [Ser67].

Acknowledgement: Sebastian Pancratz (of Cambridge University) typed up the first 9 lectures. The course was attended by Robert Bradshaw, Amelia Chen, Alison Deines, Ralph Greenberg, Jacob Lewis, Robert Miller, Amy Supple, and Wenhan Wang who all made numerous comments. The author learned Galois cohomology mainly in person from Hendrik Lenstra, to whom he's greatly indebted.

2 Introduction

Number Theory is the study of $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the group of automorphisms of the algebraic closure $\bar{\mathbb{Q}}$, and the sets G naturally acts on. The following question, for example, is an open problem: is every finite group a quotient of G?

Galois cohomology involves studying the group G by applying homological algebra. This provides a natural way to classify objects, e.g. twists of a curve, and linearizes problems by defining new invariants, revealing previously hidden structure.

This course will consists of mainly two parts, one on group cohomology in greater generality and one on Galois cohomology. In the first part, we will apply homological algebra to groups, solving problems like the following: given a group G acting on an abelian group A, find *all* extensions of G by A, that is, exact sequences

$$0 \to A \to E \to G \to 1,$$

where we write both 0 and 1 for the trivial group with one element. In the second part, we will apply group cohomology to number theory. This is a very important tool, vital to most advances in algebraic number theory in the last thirty years.

We now give further details of the course structure. The first part will cover the basic theory, involving essentially no number theory:

- G-modules
- cocycles, coboundaries
- basic homological algebra
- dimension shifting
- inflation/ restriction
- cup products, etc.

We will include most proofs in this part. In the second part, on Galois cohomology, we will specialize to number theory, focussing more on examples and including fewer proofs. The topics we will consider are:

- Profinite groups and their cohomology; topological groups
- Hilbert 90, and applications

- Kummer theory
- Descent of the field of definitions of a variety
- Twists of algebraic curves
- Brauer groups, which are are classes of simple algebras
- Elliptic curves
- Duality: Tate local duality, and Pouitou–Tate global duality
- Lang's theorem
- Shafarevich–Tate group
- Étale cohomology

3 G-modules

We will follow Chapter VII of Serre's *Local Fields* for a while.

Definition 1. Suppose G is any group and A is an abelian group with a G-action, that is, a map $G \times A \to A$ such that

$$1.a = a, \quad s.(a + a') = s.a + s.a', \quad (st).a = s.(t.a)$$

Let $\Lambda = \mathbb{Z}[G]$, the abelian group of formal finite sums of elements of G. This makes A a $\Lambda-$module, which we will also refer to as a G-module.

Remark 2. The category Mod_G of G-modules is an abelian category. Thus, we have direct sums, kernels, co-kernels, etc.

Definition 3. A sequence $A \xrightarrow{f} B \xrightarrow{g} C$, where A, B, and C are objects in Mod_G and f, g are morphisms, is *exact at* B if $\mathrm{Im}(f) = \ker(g)$. A sequence $0 \to A \to B \to C \to 0$ is a *short exact sequence* if it is exact at A, B, and C.

Definition 4. The map $\mathrm{Mod}_G \to \mathfrak{Ab}$ from Mod_G to the category $\mathfrak{Ab}$ of abelian group given by $A \mapsto A^G$, which is the G-invariant subgroup of A,

$$A^G = \{a \in \mathcal{A} : \forall g \in G \quad g.a = a\}$$

is a functor.

Let $H^0(G, A) = A^G$.

Proposition 5. If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence of G-modules, then the sequence

$$0 \to A^G \to B^G \to C^G$$

is exact at A^G and B^G. We say the functor $A \mapsto A^G$ is *left exact*.

Proof. Suppose that $b \in B^G$ and $g(b) = 0$. Then there exists $a \in A$ such that $f(a) = 0$. But for any $s \in G$,

$$f(s.a) = s.f(a) = s.b = b$$

so $f(s.a) = f(a)$, hence $a \in A^G$, since f is injective. The proof can be completed in a similar way. □

Definition 6. Formally, one can define functors $H^q(G, -) : \mathrm{Mod}_G \to \mathfrak{Ab}$ for all $q \geq 0$ such that if $0 \to A \to B \to C \to 0$ is exact then we have a *long exact sequence*

$$\begin{aligned} 0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \\ \to H^2(G, A) \to H^2(G, B) \to H^2(G, C) \to \dots \end{aligned}$$

Definition 7. A (co-variant) functor $\mathcal{F} : \mathrm{Mod}_G \to \mathfrak{Ab}$ is *exact* if for every short exact sequence $0 \to A \to B \to C \to 0$ the sequence $0 \to \mathcal{F}(A) \to \mathcal{F}(B) \to \mathcal{F}(C) \to 0$ is also exact. If $\mathcal{F}$ is contravariant, we similarly require that the sequence $0 \leftarrow \mathcal{F}(A) \leftarrow \mathcal{F}(B) \leftarrow \mathcal{F}(C) \leftarrow 0$ is exact.

Definition 8. A G-module A is *projective* if the functor $\mathrm{Hom}_G(A, -)$ is exact. A is called *injective* if the (contravariant) functor $\mathrm{Hom}_G(-, A)$ is exact.

Definition 9. A is *induced* if $A \cong \Lambda \otimes_{\mathbb{Z}} X$ for some $X \in \mathfrak{Ab}$, that is, if there is a subgroup $X \subset A$ such that $A = \bigoplus_{s \in G} s.X$. A is *co-induced* if $A \cong \mathrm{Hom}_{\mathbb{Z}}(\Lambda, X)$ for some $X \in \mathfrak{Ab}$.

Remark 10. If G is a finite group, then $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, X) \cong \Lambda \otimes_{\mathbb{Z}}$ via the isomorphism $f \mapsto \sum_{s \in G} s \otimes f(s)$ for all $X \in \mathfrak{Ab}$, so that the notions of induced and co-induced G-modules coincide.

Lemma 11. Every $A \in \mathrm{Mod}_G$ is a quotient of an induced module.

Proof. Let A_0 denote the group underlying A. Then $t.(s \otimes a) = (ts) \otimes a$. Thus,

$$\Lambda \otimes A_0 \twoheadrightarrow A$$ □

Definition 12. The functors $H^q(G,-)$, for $q \geq 0$, are called *right derived functors* of the left exact functor $A \mapsto A^G$. The construction is functorial in exact sequences, that is, from a short exact sequence $0 \to A \to B \to C \to 0$ we obtain a long exact sequence

$$0 \to H^0(G,A) \to H^0(G,B) \to H^1(G,C) \\ \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \xrightarrow{\delta} \dots$$

with connecting homomorphisms δ. $H^q(G,-)$ is a cohomological δ-functor.

Theorem 13. $H^q(G,-)$ is the *unique* δ-functor such that

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

(ii) if A is injective then, for all $q \geq 1$, $H^q(G,A) = 0$.

Thus, everything we can prove about the functor $H^q(G,-)$ must follow from the two properties above.

4 H^q and Ext

Noting that $A^G = \mathrm{Hom}_G(\mathbb{Z}, A)$, we deduce that $H^q(G,A) = \mathrm{Ext}^q_G(\mathbb{Z}, A)$. Thus, we can in principle compute the group $H^q(G,A)$ as follows:

(i) Find a resolution of $\mathbb{Z}$ by projective G-modules $P_0, P_1, \dots$

$$\dots \to P_1 \to P_0 \to \mathbb{Z} \to 0.$$

(ii) Apply the functor $\mathrm{Hom}_G(-,A)$ to obtain groups $K^i = \mathrm{Hom}_G(P_i, A)$ and the complex

$$0 \to \mathrm{Hom}_G(P_0,A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1,A) \xrightarrow{d_1} \mathrm{Hom}_G(P_2,A) \xrightarrow{d_2} \dots .$$

Then $H^q(G,A) = \ker(d_q)/\operatorname{Im}(d_{q-1})$.

We will later carry out the above procedure to obtain a very explicit representation.

Suppose that G acts diagonally on P_i, that is, that $P_i = \mathbb{Z}[G^{i+1}] = \mathbb{Z}[G \times \dots \times G]$. Then the map $d\colon P_{i+1} \to P_i$ is given by

$$d(g_0, \dots, g_i) = \sum_{j=0}^{i} (-1)^j (g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_i).$$

Definition 14. A G-module $A \in \mathrm{Mod}_G$ is *relatively injective* if it is a direct factor of a co-induced module, i.e., if $A \oplus B$ is co-induced for some $B \in \mathrm{Mod}_G$.

Proposition 15. If $A \in \mathrm{Mod}_G$ is relatively injective then $H^q(G, A) = 0$ for all $q \geq 1$.

Proof. It suffices to consider co-induced G-modules, since we can then deduce the general case from the identity $H^q(G, A \oplus B) = H^q(G, A) \oplus H^q(G, B)$. So assume that A is co-induced, that is, $A \cong \mathrm{Hom}_{\mathbb{Z}}(\Lambda, X)$ for some $X \in \mathfrak{Ab}$. For $B \in \mathrm{Mod}_G$,

$$\mathrm{Hom}_{\mathbb{Z}}(B, X) \cong \mathrm{Hom}_G(B, A), \quad f \mapsto (b \mapsto (s \mapsto f(s.b))).$$

From the above it follows that $\mathrm{Hom}_G(P_i, A) = \mathrm{Hom}_{\mathbb{Z}}(P_i, X)$, so

$$H^q(G, A) = \mathrm{Ext}^q_{\mathbb{Z}}(\mathbb{Z}, X) = 0$$

for $q \geq 1$. Moreover, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, X) \cong X$ so the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$ is exact. □

Corollary 16 (Dimension shifting)**.** If $0 \to A \to A^* \to A' \to 0$ is exact with A^* co-induced then

$$H^q(G, A') = H^{q+1}(G, A)$$

for all $q \geq 1$.

Remark 17. This shows that the functor $H^{q+1}(G, -)$ is completely determined by $H^i(G, -)$ for $i \leq q$, giving the claimed uniqueness.

We now explicitly consider $H^q(G, A)$ as a quotient of cocycles by coboundaries. We have the following free resolution of $\mathbb{Z}$ as a G-module

$$\ldots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0 \qquad (\dagger)$$

where $P_i = \mathbb{Z}[G^{i+1}] = \mathbb{Z}[G \times \cdots \times G]$ with G-action given by $s.(g_0, \ldots, g_i) = (s.g_0, \ldots, s.g_i)$ and $d\colon (g_0, \ldots, g_i) \mapsto \sum_{j=0}^{i} (-1)^j (g_0, \ldots, \hat{g_j}, \ldots, g_i)$.

Lemma 18. P_i is a free G-module.

Proof. The set $\{(1, g_1, g_1 g_2, \ldots, g_1 \cdots g_i) : g_1, \ldots, g_i \in G\}$ is a basis for P_i over $\mathbb{Z}[G]$. □

Proposition 19. The free resolution (†) is exact.

Proof. We first show that $d_i \circ d_{i+1} = 0$. This is a standard calculation from the definitions, for example

$$\begin{aligned}(d_1 d_2)(g_0, g_1, g_2) &= d_1((g_1, g_2) - (g_0, g_2) + (g_0, g_1)) \\ &= ((g_2) - (g_1)) - ((g_2) - (g_0)) + ((g_1) - (g_0)) = 0.\end{aligned}$$

Thus, $\mathrm{Im}(d_{i+1}) \subset \ker(d_i)$. To prove equality, fix $s \in G$ and define a family of maps $h\colon P_i \to P_{i+1}, h(g_0, \ldots, g_i) \mapsto (s, g_0, \ldots, g_i)$. We claim that $dh + hd = 1$,

$$\begin{aligned}(dh + hd)(g_0, \ldots, g_i) &= (dh)(g_0, \ldots, g_i) + hd(g_0, \ldots, g_i) \\ &= d(s, g_0, \ldots, g_i) + \sum_{j=0}^{i} (-1)^j (s, g_0, \ldots, \hat{g_j}, \ldots, g_i) \\ &= (g_0, \ldots, g_i) + \sum_{j=1}^{i+1} (-1)^{j+1} (s, g_0, \ldots, \hat{g_j}, \ldots, g_i) \\ &\quad + \sum_{j=0}^{i} (-1)^j (s, g_0, \ldots, \hat{g_j}, \ldots, g_i) \\ &= 0\end{aligned}$$

Let $x \in \ker(d_i)$. Then $dhx + hdx = x$, and since $hdx = 0$ we have $d(hxd) = x$ so $x \in \mathrm{Im}(d_{i+1})$. □

Recall that $\mathrm{Hom}_G(-, A)$ is a contravariant functor and let $K_i = \mathrm{Hom}_G(P_i, A)$. We obtain a complex

$$0 \to K_0 \xrightarrow{d_0} K_1 \xrightarrow{d_1} K_2 \xrightarrow{d_2} K_3 \xrightarrow{d_3} \ldots$$

such that $H^q(G, A) = \ker(d_q)/\,\mathrm{Im}(d_{q-1})$.

Suppose that $f \in \mathrm{Hom}_G(P_i, A)$ and define the set-theoretic map $\phi\colon G^i \to A$ by $\phi(g_1, \ldots, g_i) = f(1, g_1, g_1 g_2, \ldots, g_1 \cdots g_i)$.

Proposition 20.

$$\begin{aligned}(d\phi)(g_1, \ldots, g_{i+1}) = g_1 \phi(g_2, g_3, \ldots, g_{i+1}) &+ \sum_{j=1}^{i} (-1)^j \phi(g_1, g_2, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) \\ &+ (-1)^{i+1} \phi(g_1, \ldots, g_i)\end{aligned}$$

Proof. The map $d\colon P_{i+1} \to P_i$ induces a map $\mathrm{Hom}_G(P_i, A) \to \mathrm{Hom}_G(P_{i+1}, A)$ via $\phi \mapsto \phi \circ d$,

$$\begin{aligned}(d\phi)(g_1, \ldots, g_n) &= f\big(d(1, g_1, g_1g_2, \ldots, g_1 \cdots g_{i+1})\big) \\ &= f\Big((g_1, g_1g_2, \ldots, g_1 \cdots g_{i+1}) \\ &\quad + \sum_{j=1}^{i} (-1)^j (1, g_1, \ldots, \widehat{g_1 \cdots g_j}, \ldots, g_1 \cdots g_{i+1}) \\ &\quad + (-1)^{i+1}(1, g_1, g_1g_2, \ldots, g_1 \cdots g_i)\Big) \\ &= g_1\phi(g_2, g_3, \ldots, g_{i+1}) + \sum_{j=1}^{i} (-1)^j \phi(g_1, \ldots, g_jg_{j+1}, \ldots, g_{i+1}) \\ &\quad + (-1)^{i+1}\phi(g_1, \ldots, g_i)\end{aligned}$$

□

We now make some explicit considerations in small cases. Begin with the case $i = 0$. If $\phi \in \mathrm{Hom}_G(P_0, A)$ then there is an $a \in A$ such that $\phi() = a$. Thus, $(d\phi)(g) = g\phi() - \phi() = ga - a$. Now let $i = 1$ and take $\phi \in \mathrm{Hom}_G(P_1, A)$. Then

$$(d\phi)(g_1, g_2) = g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1)$$

Thus

$$\begin{aligned}H^0(G, A) &= A^G \\ H^1(G, A) &= \{\phi\colon G \to A : d\phi = 0\}/\{d\phi : \phi \in \mathrm{Hom}_G(P_0, A)\} \\ &= \{\phi\colon G \to A : \phi(g_1g_2) = \phi(g_1) + g_1\phi(g_2)\}/\{\phi_a\colon G \to A : a \in A\}\end{aligned}$$

where $\phi_a(g) = ga - a$,

$$\begin{aligned}H^2(G, A) = \{\phi\colon G \times G \to A : {} & g_1\phi(g_2, g_3) - \phi(g_1g_2, g_3) \\ & + \phi(g_1, g_2g_3) - \phi(g_1, g_2) = 0\}/\star\end{aligned}$$

5 Morphisms of pairs

5.1 Morphism of pairs

A morphism of pairs $(G, A) \to (G', A')$ together with homomorphisms $f\colon G' \to G$ and $g\colon A \to A'$ such that $g(f(s').a) = s'.g(a)$ for all $s' \in G', a \in A$ induces morphisms $H^q(G, A) \to H^q(G', A')$ for all $q \geq 0$.

We now explain this in detail. $f\colon G' \to G$ induces a morphism of the resolutions of $\mathbb{Z}$ in Mod_G and $\mathrm{Mod}_{G'}$.

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & \mathbb{Z}[G' \times G'] & \longrightarrow & \mathbb{Z}[G'] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle f} & & & & \\
\cdots & \longrightarrow & \mathbb{Z}[G \times G] & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

Hence we obtain a morphism of corresponding complexes, in the other direction:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G], A) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G \times G], A) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}[G'], A) & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}[G' \times G'], A) & \longrightarrow & \cdots
\end{array}$$

where the map $\mathrm{Hom}_G(\mathbb{Z}[G], A) \to \mathrm{Hom}_{G'}(\mathbb{Z}[G'], A)$ is given by $(\phi\colon \mathbb{Z}[G] \to A) \mapsto (g \circ \phi \circ f\colon \mathbb{Z}[G'] \to A')$. Thus, a morphism of pairs $(G, A) \to (G', A')$ induces a morphism on cohomology $H^q(G, A) \to H^q(G', A')$.

5.2 Shapiro's lemma

We begin by considering a special case. Let $G' \leq G$ be a subgroup and $A' \in \mathrm{Mod}_{G'}$. Then form a *left* G-module $A = \mathrm{Hom}_{G'}(\mathbb{Z}[G], A')$ by coinduction from A'.

Given a G-action $\phi\colon \mathbb{Z}[G] \to A'$ we set, for $s \in G$, $s.\phi\colon t \mapsto \phi(ts)$. For fixed $s \in G$, the map $\psi_s\colon \mathbb{Z}[G] \to \mathbb{Z}[G]$ given by $t \mapsto ts$ is a left G-module homomorphism; $\phi \circ \psi_s$ would thus give a right G-action, so $s.\phi$ as above is a left action.

Theorem 21 (Shapiro)**.** For all $q \geq 0$,

$$H^q(G, A) \cong H^q(G', A').$$

Remark 22. This is very important in making Eichler–Shimura explicit and computable.

Proof. If $L^\bullet \twoheadrightarrow \mathbb{Z}$ is a free $\mathbb{Z}[G]$-resolution, then $L'^\bullet \twoheadrightarrow \mathbb{Z}$ is also a free $\mathbb{Z}[G']$-resolution, since $G' \leq G$ is a subgroup. We have an isomorphism

$$\mathrm{Hom}_G\big((L^i, \mathrm{Hom}_{G'}(\mathbb{Z}, A')\big) = \mathrm{Hom}_G(L^i, A) \cong \mathrm{Hom}_{G'}(L^i, A')$$

given by $\psi \mapsto \psi(b)(1)$ with inverse $\phi \mapsto \big(b \mapsto (s \mapsto \phi(bs))\big)$. We conclude that (G, A) and (G', A') have the same complexes and thus the same cohomology. □

6 Inflation and restriction

Suppose that H is a subgroup of G and let $A \in \mathrm{Mod}_G$. A morphism of pairs $(G, A) \to (H, A)$ by $H \to G$ and $\mathrm{id}\colon A \to A$ induces a *restriction homomorphism*

$$\mathrm{res}_H\colon H^q(G, A) \to H^q(H, A).$$

For example, in terms of 1-cocyles, we see that the homomorphism $\mathrm{res}_H\colon H^1(G, A) \to H^1(H, A), [f] \mapsto [f|_H]$ is given by the usual restriction map.

Next suppose that $H \triangleleft G$. We obtain a morphism of pairs $(G/H, A^H) \to (G, A)$. This induces an *inflation homomorphism*

$$\inf\colon H^q(G/H, A^H) \to H^q(G, A).$$

We shall later consider the following theorem, whose full proof uses spectral sequences:

Theorem 23. The sequence

$$0 \to H^1(G/H, A^H) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, A) \to H^2(G/H, A^H) \to \dots$$

is exact.

7 Inner automorphisms

Suppose $t \in G$. The conjugation $s \mapsto tst^{-1}$ is an inner automorphism of G. This induces a morphism of pairs $(G, A) \to (G, A)$: $G \leftarrow G, tst^{-1} \leftarrow\shortmid s$, $A \to A, a \mapsto t^{-1}a$.

We obtain a homomorphism $H^q(G, A) \to H^q(G, A)$, that is, a *natural action* of G on $H^q(G, A)$.

Proposition 24. This action is trivial, that is, the map $t \in G$ induces the identity map on $H^q(G, A)$.

Proof. Use dimension shifting. For $q = 0$, consider

$$\begin{array}{ccc} H^0(G,A) & & \\ \| & & \\ \mathrm{Hom}_G(\mathbb{Z}[G],A) & \xrightarrow{d} & \cdots \\ \downarrow & & \\ \mathrm{Hom}_G(\mathbb{Z}[G],A) & \xrightarrow{d} & \cdots \\ \| & & \\ H^0(\mathbb{Z}[G],A) & & \end{array}$$

If we let $f\colon G \to G, s \mapsto tst^{-1}$ and $g\colon A \to A, a \mapsto t^{-1}.a$ then, for $\phi \in \ker(d) \subset \mathrm{Hom}_G(\mathbb{Z}[G],A)$ so that $\phi(1) \in A^G$, we have that

$$(g \circ \phi \circ f)(1) = g(\phi(t1t^{-1})) = t^{-1}.\phi(1) = \phi(1).$$

Thus, the induced map on $H^0(G,A)$ is the identity.

Now let $q \geq 1$ and consider the short exact sequence $0 \to A \to A^* \to A' \to 0$ with A^* co-induced. We have the following functorial isomorphisms:

$$\begin{aligned} H^1(G,A) &\cong \mathrm{coker}(H^0(G,A^*) \to H^0(G,A')), \\ H^q(G,A) &\cong H^{q-1}(G,A'), \quad \text{for } q \geq 2. \end{aligned}$$

By induction, $H^{q-1}(G,A') \cong H^{q-1}(G,A')$ via conjugation by t, so the proposition follows. □

8 An application of inner automorphisms

Let k be a field with $\mathrm{char}(k) \neq 2$. Let $G = GL_n(k)$ and $A = k^n$, equipped with the natural G-action.

Proposition 25. *$H^q(G,A) = 0$ for all $q \geq 0$.*

Proof. Let

$$t = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in G.$$

Then we proved above that $(G,A) \to (G,A)$ induced by conjugation by t induces the identity map $H^q(G,A) \to H^q(G,A)$.

But in fact it induces multiplication by -1 on A:

$$s = t^{-1}st \longleftarrow\!\shortmid\ s$$

$$\begin{array}{ccc} G & \longleftarrow & G \\ \downarrow & & \downarrow \\ A & \longrightarrow & A \end{array}$$

$$a \longmapsto t^{-1}a = -a$$

Thus it induces the map $H^q(G,A) \xrightarrow{-1} H^q(G,A)$, and we conclude that, on the k-vector space $H^q(G,A)$, we have $-1 = 1$ and so $H^q(G,A) = 0$ for all $q \geq 0$. □

Remark 26. In the proof we can replace G by any subgroup of $GL_n(k)$ that contains a non-identity scalar t.

Example 27. Let E/k be an ellipctic curve and suppose that $\bar{\rho}_{E,p}\colon G_k \twoheadrightarrow \mathrm{Aut}(E[p])$ is surjective. Then

$$H^q(\mathrm{Gal}(k(E[p])/k), E[p]) = 0$$

for all $q \geq 0$.

9 The restriction-inflation sequence

Proposition 28. Let $H \triangleleft G$ be a normal subgroup and $A \in \mathrm{Mod}_G$. Then we have an exact sequence

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

Proof. We check this directly on 1-cocycles, following Atiyah–Wall. We begin with exactness at $H^1(G/H, A^H)$, that is, the injectivity of inf. Consider $H^1(G/H, A^H) \xrightarrow{\inf} H^1(G,A), [f] \mapsto [\bar{f}]$ where

$$\begin{array}{ccc} G & \xrightarrow{\bar{f}} & A \\ & \searrow & \uparrow \\ & G/H \xrightarrow{f} & A^H \end{array}$$

and suppose that $[\bar{f}] = 0$. Thus, $\bar{f}$ is a coboundary and so there exists an $a \in A$ such that $\bar{f}(s) = s.a - a$ for all $s \in G$. Note that $\bar{f}$ is constant on each coset of H in G, and so, for all $t \in H$,

$$s.a - a = \bar{f}(s) = \bar{f}(st) = (st).a - a$$

hence $s.a = (st).a$ and $a = t.a$, which implies $a \in A^H$. Thus, f is also a coboundary (attached to $a \in A^H$), and hence $[f] = 0$.

Next we show that $\mathrm{res} \circ \mathrm{inf} = 0$, i.e., $\mathrm{Im}(\mathrm{inf}) \subset \ker(\mathrm{res})$. Consider the composition

$$H^1(G/H, A^H) \xrightarrow{\mathrm{inf}} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, A), [f] \mapsto [\bar{f}] \mapsto [\bar{f}|_H].$$

But $\bar{f}$ is constant on cosets of H, so $\bar{f}|_H(t) = \bar{f}|_H(1) = 0$ since $f(1.1) = f(1) + 1.f(1) = f(1) + f(1)$.

Finally, we prove the exactness at $H^1(G, A)$, i.e., $\mathrm{iker}(\mathrm{res}) \subset \mathrm{Im}(\mathrm{inf})$. Consider an $f\colon G \to A$ such that

$$H^1(G, A) \to H^1(H, A), [f] \mapsto [0].$$

Then there exists an $a \in A$ such that, for all $t \in H$, $f(t) = t.a - a$. It follows that $[f] = [f - \phi_a]$ where ϕ_a is defined by $\phi_a(s) = s.a - a$, for all $s \in G$. Thus, we may assume that $f|_H = 0$.

If $t \in H$, then

$$f(st) = f(s) + s.f(t) = f(s)$$

so f is constant on cosets of H in G. Thus, f defines a function $\tilde{f}\colon G/H \to A$. For $s \in H$, $t \in G$, we have

$$f(t) = f(st) = 0 + s.f(t)$$

and hence $f(t) \in A^H$ and so the image of $\tilde{f}$ lies in A^H. Thus, $[\tilde{f}] \mapsto [f]$, completing the proof. □

10 Cohomology sets

For this section, we refer to pp. 123–126 of Serré's *Local Fields*. As before, we let G be a group and A a group with a G-action. But A is no longer assumed to be abelian.

For example, we could consider $G = \mathrm{Gal}(\bar{k}/k)$ and A the points of any algebraic group over k, e.g., $GL_n(\bar{k})$ or $SL_n(\bar{k})$.

Definition 29. We set $H^0(G,A) = A^G = \{a \in A : s.a = a \text{ for all } s \in G\}$, which is a subgroup of A. We define $H^1(G,A)$ as 1-cocycles modulo an equivalence relation. Here, a 1-cocycle is a set-theoretic map $G \to A, s \mapsto a_s$ such that $a_{st} = a_s.s(a_t)$, and we say $a_s \sim b_s$ if there exists an $a \in A$ with $b_s = a^{-1}.a_s.s(a)$ for all $s \in G$.

Remark 30. $H^1(G,A)$ is a pointed set, with distinguished element the image of the 1-cocycle $a_s = 1$, i.e., the map sending the all of G to $1 \in A$.

We have described two functors: $H^0(G,-)$ is a functor from the category of non-abelian G-modules to the category of groups, and $H^1(G,-)$ is a functor from the same category to the category of pointed sets. For example, this means that a G-morphism $A \to B$ induces morphisms $H^0(G,A) \to H^0(G,B)$ and $H^1(G,A) \to H^1(G,B)$.

We now explain how the long exact sequence can be salvaged in the context of non-abelian G-modules. Suppose we have a short exact sequence

$$1 \to A \xrightarrow{\iota} B \xrightarrow{\rho} C \to 1 \tag{$\dagger$}$$

of non-abelian G-modules. We want to show the existence of a connecting morphism $\delta\colon C^G \to H^1(G,A), c \mapsto [a_s]$.

Let $c \in C^G$ and $b \in B$ such that $\rho(b) = c$. Then $s(b) \equiv b$ modulo $\iota(A)$ for all $s \in G$, since

$$\rho(s(b).b^{-1}) = s(c).c^{-1} = cc^{-1} = 1.$$

So let $a_s = \iota^{-1}(b^{-1}.s(b)) \in A$. We claim that a_s is a well-defined cocycle.

In order to simplify notation, let us assume $A \subset B$. Then

$$a_{st} = b^{-1}(st)(b) = b^{-1}s(b)s(b^{-1}t(b)) = a_s.s(a_t),$$

showing that a_s is a cocycle. Moreover, if $\rho(b') = \rho(b) = c$ then $b' = ba$ for some $a \in A$ by exactness and hence

$$a'_s = a^{-1}b^{-1}s(b)s(a) = a^{-1}a_s s(a) \sim a_s,$$

which shows that a_s is well-defined.

If we suppose that A lies in the centre of B, so that A is abelian, we can define $H^2(G,A)$ as before and also obtain a morphism $\Delta\colon H^1(G,C) \to H^2(G,A)$.

Proposition 31. (i) Let $1 \to A \xrightarrow{\iota} B \xrightarrow{\rho} \to 1$ be any exact sequence of non-abelian G-modules. Then the sequence

$$1 \to H^0(G,A) \xrightarrow{\iota_0} H^0(G,B) \xrightarrow{\rho_0} H^0(G,C) \xrightarrow{\delta} H^1(G,A) \xrightarrow{\iota_1} H^1(G,B) \xrightarrow{\rho_1} H^1(G,C)$$

is exact.

(ii) If, moreover, A lies in the centre of B then the above exact sequence can be extended by $H^1(G,C) \xrightarrow{\Delta} H^(G,A)$ to another exact sequence.

Proof. See book. (Serre??) □

11 Long exact sequence of cohomology sets

This section is motivated by the following example. Let C be a curve defined over a field k with non-abelian automorphism group $\mathrm{Aut}(C)$. Then $H^0(\mathrm{Gal}(\bar{k},k), \mathrm{Aut}(C))$ is isomorphic to the twists of C over k.

Consider a map $\pi\colon X \to Y$ of pointed sets with distinguished elements x and y. By definition, $\ker(\pi) = \pi^{-1}(y) \subset X$.

We first revisit the connecting homomorphism δ. Suppose that $1 \to A \xrightarrow{\iota} B \xrightarrow{\rho} C \to 1$ is an exact sequence of non-abelian G-modules. The connecting homomorphism is a map $\delta\colon H^0(G,C) \to H^1(G,A)$.

Proposition 32. The sequence

$$1 \to H^0(G,A) \xrightarrow{\iota_0} H^0(G,B) \xrightarrow{\rho_0} H^0(G,C) \xrightarrow{\delta} H^1(G,A) \xrightarrow{\iota_1} H^1(G,B) \xrightarrow{\rho_1} H^1(G,C)$$

is exact.

Proof. We continue to identify $A \subset B$. Firstly, the sequence is exact at $H^0(G,A)$ since ι_0 is injective since $A^G \to B^G$. For exactness at $H^0(G,B)$, note that $(\rho \circ \iota)(a) = 0$ for all $a \in A$, so the same is true on A^G and B^G. Furthermore, if $b \in \ker(\rho_0) \subset B^G$ then $b \in \ker(\rho) = \mathrm{Im}(\iota) = A$, so $b \in A \cap B^G = A^G$ and hence $b \in \mathrm{Im}(\iota_0)$, showing that $\ker(\rho_0) \subset \mathrm{Im}(\iota_0)$.

Next, we prove exactness at $H^0(G,C)$. We can describe $\rho_0(B^G)$ as the set of $c \in C^G$ that lift to invariant elements of B, and $\ker(\delta)$ as the set of $c \in C^G$ such that $a_s = b^{-1}s(b) \sim 1$ in $H^1(G,A)$ whenever $b \mapsto c$. Suppose that $c \in \ker(\delta)$ so that $c \in C^G$ and there exists $b \in B^G$ such that $b \mapsto c$ and $a_s = b^{-1}s(b) \sim 1$. Then a_s is trivial if and only if $a_s \sim 1$, i.e., there exists an $a \in A$ with

$$a^{-1}b^{-1}.s(b)s(a) = 1$$

for all $s \in G$, that is, $s(ba) = ba$ and thus $ba \in B^G$.

Then $a_s \sim (ba)^{-1}s(ba)$ and $ba \in B^G$. But $a \in A$ so $\rho(ba) = \rho(b) = c$, so $ba \mapsto c$ and $ba \in B^G$ hence $c \in \rho_0(B^G)$.

Now, we prove exactness at $H^1(G, A)$. Suppose that ι_1 sends $[a_s]$ to the trivial element of $H^1(G, B)$. Then there exists a $b \in B$ such that $a_s \sim b^{-1}s(b)$ for all $s \in G$. Thus $[a_s] = \delta(\rho(b))$, which shows that $\ker(\iota_1) \subset \mathrm{Im}(\delta)$. For the other direction, note that $\delta(c)$ is given by $a_s = b^{-1}s(b)$ for some b such that $b \mapsto c$. But this *means* that $\iota_1(a_s) \sim 1$.

Finally, we prove exactness $H^1(G, B)$. First, note that $a_s \in H^1(G, A)$ maps to $s \mapsto \rho_1(\iota_1(a_s)) = 1$, since $rho \circ \iota = 1$, showing that $\mathrm{Im}(\iota_1) \subset \ker(\rho_1)$. For the other direction, let $b_s \in H^1(G, B)$ such that $(s \mapsto \rho_1(b_s)) \sim 1$. Then there exists a $c \in C$ such that $\rho_1(b_s) = c^{-1}s(c)$. We may modify by a lift of c so that $\rho_1(b_s) = 1$ for all s. It then follows that $b_s \in A$ for all s, so that $[b_s] \in \mathrm{Im}(\iota_1)$. □

12 Homology

In this section, we let G be a group, A an abelian G-module and set $DA = \langle s.a - a : a \in A, s \in G \rangle$, a subgroup of A.

We first observe that DA is in fact a G-module,

$$t.(s.a - a) = t.s.a - t.a = (tst^{-1}).(t.a) - t.a \in DA.$$

Thus, A/DA is also a G-module, with trivial G-action.

Definition 33. We define $H_0(G, A) = A/DA$, which is the largest quotient of A with trivial G-action. For $q \geq 1$, we also let

$$H_q(G, A) = \mathrm{Tor}_q^{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

so that $H_q(G, -)$ are the left-derived functors of $H_0(G, -)$.

Given a short exact sequence $0 \to A \to B \to C \to 0$, as before we obtain a long exact sequence

$$\cdots \to H_1(G, A) \to H_1(G, B) \to H_1(G, C) \xrightarrow{\delta} H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0.$$

Example 34. For any group G, we have $H_1(G, \mathbb{Z}) = G/G'$, the abelianisation of G, where $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ is the commutator subgroup. See Serre §VII.4 for a proof.

13 Tate cohomology groups

The Tate cohomology groups naturally relate homology and cohomology, and make several results much more natural.

Suppose that G is a *finite* group and let A be a G-module. We define the *norm* element, linking homology and cohomology, by

$$N = \sum_{s \in G} s.$$

This induces a map $N\colon A \to A, a \mapsto N(a) = \sum_{s\in G} s.a$, which is in fact a G-module homomorphism, since

$$t \sum_{s\in G} s.a = \sum_{s\in G} (ts).a = \sum_{s\in G} (st).a,$$

noting that st and ts range over the same elements of G for $s \in G$.

We define the *augmentation ideal* as

$$I_G = (s - 1 : s \in G) \subset \mathbb{Z}[G].$$

Lemma 35. (i) $I_G A \subset \ker(N)$, which we will also denote $A[N]$.

(ii) $\mathrm{Im}(N) \subset A^G$.

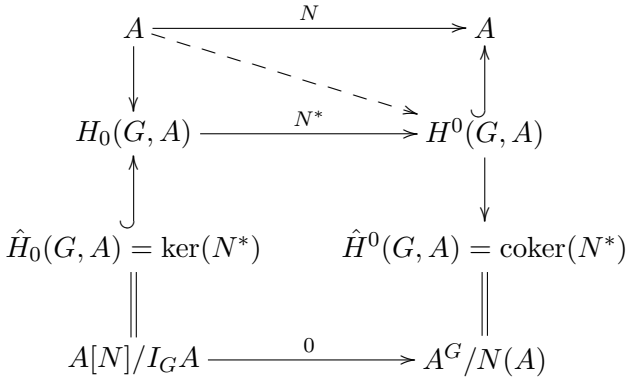
Proof. We use that, for fixed $s \in G$ and variable $t \in G$, st ranges over all elements of G as t does:

(i)
$$N((s-1).a) = \Big(\sum_{t\in G} t\Big).(s-1).a = \Big(\sum_{t\in G} ts - \sum_{t\in G} t\Big).a = 0.$$

(ii)
$$s.N(a) = s.\sum_{t\in G} t.a = \sum_{t\in G} (st).a = \sum_{t\in G} t.a = N(a). \qquad \square$$

This induces the aforementioned link between homology and cohomology

as follows:



Proposition 36. If A is induced then $\hat{H}^0(G, A) = 0$.

Proof. The assumption that A is induced *means* that $A \cong \bigoplus_{s \in G} s.X \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$, where $X \leq A$ is a subgroup. This is easy to see since G is finite.

Thus, each $a \in A$ can be expressed uniquely as

$$a = \sum_{s \in G} s.x_s, \quad x_s \in X$$

Now $a \in A^G$ if and only if all x_s are equal if and only if $a = N(x_s)$. This shows that $A^G = N(A)$, as claimed. □

Remark 37. If A is induced, we also have that $\hat{H}_0(G, A) = 0$. The proof of this statement will appear on the problem sheet.

Definition 38. We define the *Tate cohomology* groups as follows:

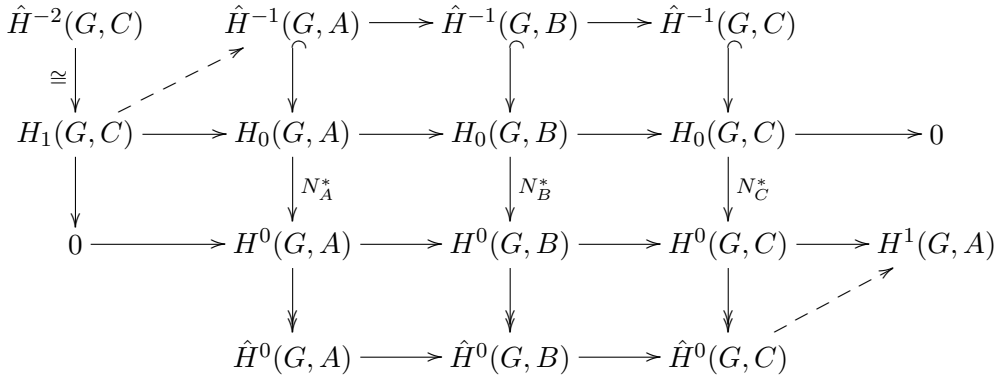
$$\begin{aligned} \hat{H}^q(G, A) &= H^q(G, A), \quad q \geq 1 \\ \hat{H}^0(G, A) &= A^G/N(A) \\ \hat{H}^{-1}(G, A) &= A[N]/I_G A \\ \hat{H}^{-q}(G, A) &= H_{q-1}(G, A), \quad q \geq 2 \end{aligned}$$

Remark 39. The functor $\hat{H}^0(G, -)$ is *not* left exact.

Proposition 40. Given a short exact sequence of G-modules $0 \to A \to B \to C \to 0$, we have the long exact sequence

$$\begin{aligned} \cdots \to \hat{H}^{-2}(G, C) \to \hat{H}^{-1}(G, A) \to \hat{H}^{-1}(G, B) \to \hat{H}^{-1}(G, C) \\ \to \hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C) \\ \to \hat{H}^1(G, A) \to \hat{H}^1(G, B) \to \hat{H}^1(G, C) \to \hat{H}^2(G, A) \to \cdots \end{aligned}$$

Proof. We have the following commutative diagram of exact sequences:



which yields a connecting homomorphism $\hat{H}^{-1}(G,C) \to \hat{H}^0(G,A)$ by the Snake Lemma. □

Fact 41. (i) Every G-module A embeds in a G-module A^* such that

$$\hat{H}^q(G, A^*) = 0$$

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

(ii) Every G-module A is a quotient of some G-module A_* such that

$$\hat{H}^q(G, A_*) = 0$$

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

This is extremely useful, see p. 129 of Serre.

We continue with the assumption that G is a *finite* group and that A is a G-module. In this lecture, we will obtain the following results, each valid for every $q \in \mathbb{Z}$:

(i) $\hat{H}^q(G,A)$ is killed by $|G|$;

(ii) if A is finitely generated then $\hat{H}^q(G,A)$ is finite;

(iii) if $S \leq G$ is a Sylow p-subgroup, then we have an injection

$$\text{res}\colon \hat{H}^q(G,A)(p) \to \hat{H}^q(S,A),$$

where $\hat{H}^q(G,A)(p)$ denotes the p-primary subgroup.

So far we do not have the tools to prove these facts!

14 Complete resolution of G

Recall our earlier definition of $P_\bullet$, giving a free $\mathbb{Z}[G]$-resolution of $\mathbb{Z}$. Dualising this by defining $P_i^* = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$ over $\mathbb{Z}$, *not* $\mathbb{Z}[G]$, we obtain a second exact sequence

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \xrightarrow{\varepsilon} & \mathbb{Z} & \longrightarrow & 0 & & \\
 & & & & & & & & \| & & & & \\
 & & & & & & & & \mathbb{Z} & \xrightarrow{\varepsilon^*} & P_0^* & \longrightarrow & P_1^* & \longrightarrow & P_2^* & \longrightarrow & \cdots
\end{array}$$

We extend this to negative indices by setting $P_{-n} = P_{n-1}^*$. Thus, we obtain a long exact sequence

$$\ldots \to P_2 \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to \ldots$$

called a *complete resolution*.

Proposition 42. $\hat{H}^q(G, A)$ is the q-th cohomology group of the complex and we have an exact sequence

$$\cdots \leftarrow \mathrm{Hom}(P_1, A) \leftarrow \mathrm{Hom}(P_0, A) \leftarrow \mathrm{Hom}(P_{-1}, A) \leftarrow \mathrm{Hom}(P_{-2}, A) \leftarrow \cdots .$$

Proof. In the case $q \geq 1$, this follows immediately from the definition.

Suppose now that $q \leq -2$. By definition, $H_n(G, A)$ is the nth homology of the complex $P_\bullet \otimes_{\mathbb{Z}[G]} A$, i.e., the standard complex, although any projective resolution of $\mathbb{Z}$ will work. But for a finitely generated *free* $\mathbb{Z}[G]$-module B,

$$B \times A \xrightarrow{\sim} \mathrm{Hom}(B^*, A), \quad c \times a \mapsto (f \mapsto f(c).a),$$

where $B^* = \mathrm{Hom}(B, \mathbb{Z})$, is an isomorphism of $\mathbb{Z}[G]$-modules. So we obtain an isomorphism τ

$$\begin{aligned}
\tau \colon B \otimes_{\mathbb{Z}[G]} A = (B \otimes A)/I_G.(B \otimes A) &\xrightarrow[N^*]{\sim} (B \otimes A)^G \\
&\to \mathrm{Hom}(B^*, A)^G = \mathrm{Hom}_G(B^*, A),
\end{aligned}$$

which can be verified using the identities $b \otimes s.a = s^{-1}.b \otimes a$, $s.b \otimes s.a = b \otimes a$, and $(s-1).(b \otimes a) = s.b \otimes s.a - b \otimes a$. Moreover, we note that N^* is an isomorphism since $B \otimes_{\mathbb{Z}} A$ is induced, which is the case because B is free and the tensor product is formed over $\mathbb{Z}$. Thus

$$\mathrm{Hom}_G(P_{-n}, A) = \mathrm{Hom}_G(\mathrm{Hom}(P_{n-1}, \mathbb{Z}), A) \cong P_{n-1} \otimes_{\mathbb{Z}[G]} A$$

and the result follows since we are computing cohomology of the *same* complex.

For the cases $q = 0$ and $q = 1$, see Cassels–Fröhlich, p. 103. □

Recall the technique of *dimension shifting*: given an exact sequence $0 \to A' \to A_* \to A \to 0$, where A_* is an induced G-module, say of the form $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A$, then, for all $q \in \mathbb{Z}$,

$$\hat{H}^q(G, A) \xrightarrow[\delta]{\sim} \hat{H}^{q+1}(G, A').$$

Taking $H \leq G$ allows us to define the restriction map for all $q \in \mathbb{Z}$ via the following commutative diagram

$$\begin{array}{ccc} \hat{H}^q(G, A') & \xrightarrow{\text{res}} & \hat{H}^q(H, A') \\ \cong\downarrow & & \\ \hat{H}^{q-1}(G, A) & \xrightarrow{\text{res}} & \hat{H}^{q-1}(H, A) \end{array}$$

15 Corestriction

For homology, a morphism of pairs

$$\begin{array}{ccc} G' & \longrightarrow & G \\ \vdots & & \vdots \\ A' & \longleftarrow & A \end{array}$$

induces a homomorphism $H_q(G', A') \to H_q(G, A)$.

Thus, for $H \to G$ we obtain a homomorphism $H_q(H, A) \to H_q(G, A)$ for all q. It follows that, for an exact sequence $0 \to A \to A^* \to A' \to 0$ as above, we have the following commutative diagram for all $q \in Z$

$$\begin{array}{ccc} \hat{H}^q(G, A) & \xrightarrow{\sim} & \hat{H}^{q-1}(G, A') \\ \uparrow{\scriptstyle \text{cores}} & & \uparrow{\scriptstyle \text{cores}} \\ \hat{H}^q(H, A) & \xrightarrow{\sim} & \hat{H}^{q-1}(H, A') \end{array}$$

Proposition 43.

- The homomorphism res: $\hat{H}^0(G, A) \to \hat{H}^0(H, A)$ is given by the homomorphism $A^G/N(A) \to A^H/N(A)$, induced by the inclusion $A^G \to A^H$.
- The homomorphism res: $\hat{H}^{-1}(G, A) \to \hat{H}^{-1}(H, A)$ is induced by the homomorphism $N'_{G/H}\colon A/I_G(A) \to A/I_H(A)$ sending the image of a to $\sum s_i^{-1}.a$, where the $s_i \in G$ are chosen such that $G/H = \bigcup s_i.H$.

- The homomorphism cores: $\hat{H}^0(H,A) \to \hat{H}^0(G,A)$ is induced by the homomorphism $N_{G/H}\colon A^H/N_H(A) \to A^G/N_G(A)$ where $N_{G/H}(a) = \sum s_i.a$.

Proof. See Cassels–Fröhlich. □

Proposition 44. For all $q \in \mathbb{Z}$,

$$\mathrm{cores}_{G/H} \circ \mathrm{res}_H\colon \hat{H}^q(G,A) \to \hat{H}^q(G,A)$$

and the composition cores ∘ res is multiplication by $[G:H]$.

Proof. We check this for $q = 0$; the general result will then follow by dimension shifting.

$$\begin{array}{ccc} \hat{H}^0(G,A) & = & A^G/N(A) \\ & {\scriptstyle \mathrm{res}}\big(\quad \big){\scriptstyle \mathrm{cores}} & \\ \hat{H}^0(H,A) & = & A^H/N(A) \end{array}$$

where the restriction map is induced by $A^G \subset A^H$ and the co-restriction map is induced by $N_{G/H}(a) = \sum s_i.a$, where the s_i are coset representatives of H in G. Observe that, for $a \in A^G$,

$$\mathrm{cores}(\mathrm{res}(a)) = \left[\sum s_i.a\right] = n.a$$

where $n = [G:H]$. □

Corollary 45. (i) $\hat{H}^q(G,A)$ is killed by $|G|$, for all $q \in \mathbb{Z}$.

(ii) If A is finitely generated then $\hat{H}^q(G,A)$ is finite for all $q \in \mathbb{Z}$.

(iii) Suppose $S \leq G$ is a Sylow p-subgroup, that is, $|S| = p^n \mid |G|$ but $p^{n+1} \nmid |G|$. Then $\hat{H}^q(G,A)(p) \to \hat{H}^q(S,A)$, for all $q \in \mathbb{Z}$.

Proof. (i) Take $H = \{1\} \leq G$ above and note that $\hat{H}^q(H,A) = 0$ for all $q \in \mathbb{Z}$.

(ii) This is a calculation of $\hat{H}^q(G,A)$ using the standard resolution. One shows that $\hat{H}^q(G,A)$ is finitely generated, but since every element is killed by $|G|$, it follows that it is finite.

(iii) We use the composition of maps

$$\hat{H}^q(G,A) \underset{\text{res}}{\overset{\text{cores}}{\rightleftarrows}} \hat{H}^q(S,A)$$

Suppose $|G| = p^n m$ and let $x \in \hat{H}^q(G,A)$ be an element of order a power of p. Then $(\text{cores} \circ \text{res})(x) = 0 = m \cdot x$, thus $x = 0$ and $\text{res}(x) = 0$. □

16 Cup Product

We will define and construct the cup product pairing on Tate cohomology groups and describe some of its basic properties. The main references are §7 of Atiyah-Wall, §VIII.3 of Serre's *Local Fields*, Washington's paper *Galois Cohomology* (in Cornell-Silverman-Stevens), and §7 of Tate's *Galois Cohomology* (PCMI). The cusp product is absolutely central to Galois cohomology, in that many of the central theorems and constructions involve various types of *duality* results, which involve cup products at their core.

16.1 The Definition

Let G be a finite group.

Theorem 16.1. *There is a unique family of "cup product" homomorphisms*

$$\hat{H}^p(G,A) \otimes \hat{H}^q(G,B) \to \hat{H}^{p+q}(G, A \otimes B)$$
$$a \otimes b \mapsto a \cup b,$$

for all $p, q \in \mathbb{Z}$ and G-modules A, B, such that:

(i) Cup product is functorial in A, B, e.g., if $A \to A'$, $B \to B'$ are G-module homomorphisms, then we have a commutative diagram (with vertical maps that I have not typeset below):

$$\hat{H}^p(G,A) \otimes \hat{H}^q(G,B) \to \hat{H}^{p+q}(G, A \otimes B)$$
$$\hat{H}^p(G,A') \otimes \hat{H}^q(G,B') \to \hat{H}^{p+q}(G, A' \otimes B')$$

(ii) When $p = q = 0$ the cup product is induced by the natural map

$$A^G \otimes B^G \to (A \otimes B)^G.$$

(iii) A natural compatibility statement that allows for dimension shifting and ensure uniqueness (see Cassels-Frohlich or Serre for the exact statement).

16.2 Existence

Let P_n be a complete resolution of G, e.g., P_n could be the standard resolution:

$$P_n = \begin{cases} \mathbb{Z}[G^{n+1}] & \text{if } n \geq 0, \\ \mathrm{Hom}(P_{|n|-1}, \mathbb{Z}) & \text{if } n < 0. \end{cases}$$

Recall that this fit together to form an exact sequence of free G-modules:

$$\cdots \xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{d} P_{-1} \xrightarrow{d} P_{-2} \xrightarrow{d} \cdots .$$

Moreover, we have

$$\hat{H}^q(G, A) = \mathrm{H}^q(\mathrm{Hom}_G(P_*, A))$$

is the qth cohomology of the complex $\mathrm{Hom}_G(P_*, A)$. In particular

$$\hat{H}^q(G, A) = \frac{\ker(\mathrm{Hom}_G(P_q, A) \to \mathrm{Hom}_G(P_{q+1}, A))}{\mathrm{im}(\mathrm{Hom}_G(P_{q-1}, A) \to \mathrm{Hom}_G(P_q, A))}.$$

To prove that the family of cup product morphisms exist, we will construct a G-module homomorphism from the complete resolution with certain properties.

Proposition 16.2. *There exist G-module homorphisms*

$$\varphi_{p,q} : P_{p+q} \to P_p \otimes Q_q$$

for all $p, q \in \mathbb{Z}$ such that

(i) $\varphi_{p,q} \circ d = (d \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes d) \circ \varphi_{p,q+1}$, *and*

(ii) $(\varepsilon \otimes \varepsilon) \circ \varphi_{0,0} = \varepsilon$, *where $\varepsilon : P_0 \to \mathbb{Z}$ is defined by $\varepsilon(g) = 1$ for all $g \in G$.*

Assume that the proposition has been proved. Then we define the cup product explicitly on the level of cochains as follows. Let

$$f \in \mathrm{Hom}_G(P_p, A), \qquad g \in \mathrm{Hom}_G(P_q, B)$$

be cochains (so elements of the kernel of d). Define the cochain

$$f \cup g \in \mathrm{Hom}_G(P_{p+q}, A \otimes B)$$

by

$$f \cup g = (f \otimes g) \circ \varphi_{p,q}.$$

Lemma 16.3. *We have*

$$f \cup g = (df) \cup g \ + \ (-1)^p f \cup (dg).$$

Corollary 16.4. *If f, g are cochains, then:*

(i) $f \cup g$ is a cochain

(ii) $f \cup g$ only depends on the classes of f and g.

We conclude that we have a well-defined homomorphism

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \to \hat{H}^{p+q}(G, A \otimes B).$$

Proposition 16.5. *Condition (ii) of Theorem 16.1 is satisfied.*

Proof. This uses from Proposition 16.2 that $(\varepsilon \otimes \varepsilon) \circ \varphi_{0,0} = \varepsilon$. □

It remains to construct the maps $\varphi_{p,q}$. These maps are constructed in a natural way in terms of the standard complete resolution P_n mentioned above, as follows. First note that if $q \geq 1$, then $P_{-q} = P_{q-1}^* = \mathrm{Hom}(P_{q-1}, \mathbb{Z})$ has a $\mathbb{Z}$-module basis consisting of all $(g_1^*, \ldots, g_q^*)$, where $(g_1^*, \ldots, g_q^*)$ maps $(g_1, \ldots, g_q) \in P_{q-1}$ to $1 \in \mathbb{Z}$, and every other basis element of P_{q-1} to 0. The map $d : P_{-q} \to P_{-q-1}$ is then

$$d(g_1^*, \ldots, g_q^*) = \sum_{s \in G} \sum_{i=0}^{q} (-1)^i (g_1^*, \ldots, g_i^*, s^*, g_{i+1}^*, \ldots g_q^*).$$

and $d : P_0 \to P_{-1}$ is given by $d(g_0) = \sum_{s \in G} s^*$.

If $p \geq 0$ and $q \geq 0$, then

$$\varphi_{p,q}(g_0, \ldots g_{p+q}) = (g_0, \ldots, g_p) \otimes (g_p, \ldots g_{p+q}),$$

and if $p, q \geq 1$ then

$$\varphi_{-p,-q}(g_1^*, \ldots, g_{p+q}^*) = (g_1^*, \ldots g_p^*) \otimes (g_{p+1}^*, \ldots, g_{p+q}^*),$$

and similar definitions in other cases, when one of p, q is positive and the other is negative. (Again, see Cassels-Frohlich for more details.) The moral of all this is that one can construct the cup product by simply following your nose.

16.3 Properties

Proposition 16.6. *The cup product has these properties:*

(i) $(a \cup b) \cup c = a \cup (b \cup c)$

(ii) $\mathrm{res}(a \cup b) = \mathrm{res}(a) \cup \mathrm{res}(b)$

(iii) $\mathrm{cores}(a \cup \mathrm{res}(b)) = \mathrm{cores}(a) \cup b.$

The above properties are proved by proving them when $p = q = 0$, then using dimension shifting.

Finally, notice that if $A \otimes B \to C$ is a G-homomorphism, then cup product induces

$$\hat{H}^p(G, A) \otimes \hat{H}^q(G, B) \to \hat{H}^{p+q}(G, C).$$

See Tate's paper *Galois Cohomology* for an explicit description of the cup product for $p, q \geq 0$ on cocycles, which would make computation of the cup product of classes represented by cocycles explicit.

16.4 Cohomology of a Cyclic Group

Suppose that $G = \langle s \rangle$ is a finite cyclic group. In this section we give a quick summary of the basic facts about $\hat{H}^q(G, A)$.

Let $K_i = \mathbb{Z}[G]$ and define maps $d : K_{i+1} \to K_i$ by multiplication by $s - 1$ if i is even and multiplication by $N = \sum_{t \in G} t$ if i is odd. Then

$$\cdots \xrightarrow{d} K_i \xrightarrow{d} K_{i-1} \xrightarrow{d} K_{i-2} \xrightarrow{d} \cdots$$

is a complete resolution of G, since

$$\ker(T) = \mathbb{Z}[G]^G = N(\mathbb{Z}[G]) = \mathrm{image}(N),$$

and since $\hat{H}^0(G, \mathbb{Z}[G]) = 0$,

$$\ker(N) = I_G \mathbb{Z}[G] = \mathrm{image}(T).$$

Then $\mathrm{Hom}_G(K_\bullet, A)$ is

$$\cdots \leftarrow A \xleftarrow{N} A \xleftarrow{T} A \xleftarrow{N} \cdots .$$

Proposition 16.7. *For every integer q we have*

$$\hat{H}^{2q}(G, A) \cong \hat{H}^0(G, A) = A^G/N(A)$$

and

$$\hat{H}^{2q+1}(G, A) \cong \hat{H}^{-1}(G, A) = \ker(N_A)/I_G(A).$$

If $n = \#G$, then we have

$$\hat{H}^2(G, \mathbb{Z}) \cong \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}^G/N(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

Theorem 16.8. *Cup product by a generator of $\hat{H}^2(G, \mathbb{Z})$ induces an isomorphism*

$$\hat{H}^q(G, A) \xrightarrow{\cong} \hat{H}^{q+2}(G, A)$$

for all $q \in \mathbb{Z}$ and all G-modules A.

For the proof, see Cassels-Frohlich, Section 8.

17 Galois Cohomology

In this course we have developed a foundation for group cohomology. The goal for the rest of the course (about 15 lectures), is to see some applications of group cohomology to Galois theory and algebraic number theory that are important to understanding contemporary research in number theory. For the rest of the course, our group will always be the Galois G of an extension of fields, and our module A will "arise in nature", equipped with a *natural* action of G. The main topics are Galois cohomology of abelian varieties, the Brauer group of a field, local and global duality, and étale (and other) cohomology which generalizes the idea of Galois cohomology to bases other than fields. This part of the course requires more background in number theory.

Excellent references include the many articles with the title *Galois Cohomology*, such as Tate's, Washington's, etc.

17.1 The Definition

Let K be a field, e.g., a number field such as $\mathbb{Q}(\sqrt[3]{2})$, a finite field such as $\mathbb{F}_9$, a p-adic field such as $\mathbb{Q}_{11}$, or a function such as $\mathbb{F}_7(t)$ or $\mathbb{C}(u, v)$. Let L/K be a *finite* separable Galois extension of K with Galois group $G = \mathrm{Gal}(L/K)$. For any G-module A, let

$$\mathrm{H}^q(L/K, A) = \mathrm{H}^q(\mathrm{Gal}(L/K), A), \qquad \text{for } q \geq 0$$

and

$$\hat{H}^q(L/K, A) = \hat{H}^q(\mathrm{Gal}(L/K), A), \qquad \text{for all } q \in \mathbb{Z}.$$

We call A a *Galois module*.

17.2 Infinite Galois extensions

John Tate pioneered the study of $\mathrm{H}^q(L/K, A)$ when L/K is *infinite*. When L is infinite, let

$$\mathrm{H}^q(L/K, A) = \varinjlim_M \mathrm{H}^q\left(M/K,\ A^{\mathrm{Gal}(L/M)}\right),$$

where the injective limit is over all finite Galois extensions M of K contained in L, and the maps are the inflation maps. We will often write

$$A(M) = A^{\mathrm{Gal}(L/M)},$$

motivated by similar notation for the group of rational points on an elliptic curve.

When $K \subset M \subset M'$, we have a morphism of pairs

$$(\mathrm{Gal}(M/K),\ \ A(M)) \to (\mathrm{Gal}(M'/K),\ \ A(M')),$$

given by the natural map $\mathrm{Gal}(M'/K) \to \mathrm{Gal}(M/K)$ and the inclusion $A(M) \hookrightarrow A(M')$, which defines

$$\mathrm{H}^q(M/K, A(M)) \xrightarrow{\mathrm{inf}} \mathrm{H}^q(M'/K, A(M')).$$

When $q = 1$, the inf-res sequence is exact, so all of the maps used to define the above injective limit are injections, and we can think of $\mathrm{H}^1(L/K, A)$ as simply being the "union" of the groups $\mathrm{H}^1(M/K, A(M))$, over all finite Galois M. When $q > 1$, (presumably) the above inflation maps need not be injective.

Finally, we let

$$\mathrm{H}^q(K, A) = \mathrm{H}^q(K^{\mathrm{sep}}/K, A).$$

With this notation, the inf-res sequence is

$$0 \to \mathrm{H}^1(M/K, A(M)) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(K, A) \xrightarrow{\mathrm{res}} \mathrm{H}^1(M, A).$$

The correct topology on the group $\mathrm{Gal}(L/K)$ is the one for which the open subgroups are the subgroups $\mathrm{Gal}(L/M)$ for M any finite Galois extension of K.

Exercise 17.1. Use the axiom of choice to show that there exists a finite index normal subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that is not open. [Hint: Consider the compositum of infinitely many distinct quadratic extensions of $\mathbb{Q}$. Their Galois group is $\prod \mathbb{F}_2$. The ideal $\oplus \mathbb{F}_2$ in $\prod \mathbb{F}_2$ contains a maximal ideal I. Consider the inverse image of I in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.]

We always equip A with the discrete topology.

Proposition 17.2. *Fix topologies on* $\mathrm{Gal}(L/K)$ *and* A *as above. Then* $\mathrm{H}^q(L/K, A)$ *is the group of* continuous *cocycles modulo coboundaries.*

Proof. We first show that if $[f] \in \mathrm{H}^q(L/K, A)$ then f is continuous. By definition we have $[f] \in \mathrm{H}^q(M/K, A(M))$ for some finite Galois extension M/K. Since the natural restriction map $\mathrm{Gal}(L/K)^q \to \mathrm{Gal}(M/K)^q$ is continuous and both $\mathrm{Gal}(M/K)$ and $A(M)$ are discrete, we conclude that the composite map f is continuous.

Next suppose $f : \mathrm{Gal}(L/K)^q \to A$ is a continuous cocycle. Because A has the discrete topology, the inverse image of $0 \in A$ is an open set. From the cocycle condition, the inverse image of 0 is a subgroup as well. Thus f factors through some finite Galois extension M, $\mathrm{Gal}(L/K)^q \to \mathrm{Gal}(M/K)^q$, hence $[f]$ is defined by an element of $\mathrm{H}^q(M/K, A(M))$. □

17.3 Some Galois Modules

The following are all examples of $G = \mathrm{Gal}(L/K)$-modules:

(i) The groups $A = \mathbb{Z}$ and $A = \mathbb{Q}/\mathbb{Z}$ with the trivial action.

(ii) The additive group $A = (L, +)$ of L.

(iii) The multiplicative group $A = L^*$ of L.

(iv) When $n \geq 2$, the non-commutatative G-modules $A = \mathrm{GL}_n(L)$ and $\mathrm{SL}_n(L)$.

(v) When L is a number field, the ring of integers $\mathcal{O}_L$, the units $\mathcal{O}_L^*$, and the class group $\mathrm{Cl}(\mathcal{O}_L)$ are all G-modules.

(vi) For E an elliptic curve defined over K, the group $A = E(L)$ of L-rational points.

(vii) The group $B(L)$, where B ia an abelian variety over K.

(viii) If S is any (commutative) group scheme over K, then $A = S(L)$ is a (commutative) G-module.

(ix) For any integer n and any (commutative) A elsewhere in this list, the group $A[n]$ of elements of order dividing n is a G-module.

(x) The p-adic Tate module $\mathrm{Tate}_p(A) = \varprojlim A[p^n]$ associated to an abelian variety A.

17.4 The Additive and Multiplicative Groups of a Field

We recall some basic facts from Galois theory. Suppose L/K is a finite Galois extension of fields, which means that $\#\operatorname{Aut}(L/K) = [L : K]$, or equivalently, L is the splitting field of a single irreducible separable polynomial $f \in K[x]$. We write $\mathrm{Gal}(L/K) = \operatorname{Aut}(L/K)$.

Proposition 17.3. *Let L/K be any Galois extension of fields. Then for all $q \in \mathbb{Z}$,*

$$\hat{H}^q(L/K, L) = 0.$$

Proof. Without loss, we may assume that L is a finite extension of K, since otherwise, we use the result on each finite subextension and take the limit. Since L/K is finite separable, by the normal basis theorem from Galois theory, there exists $\alpha \in L$ such that, letting $K\beta$ denote the 1-dimensional K-vector space spanned by β, we have

$$L = \bigoplus_{\sigma \in \mathrm{Gal}(L/K)} K\sigma(\alpha) \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(L/K)]. \tag{17.1}$$

But then L is induced, from which the conclusion follows. □

Proposition 17.4. *Let L/K be any Galois extension of fields. Then*

$$\mathrm{H}^1(L/K, L^*) = 0.$$

Proof. As above, we may assume that L/K is a finite extension. Suppose $f : \mathrm{Gal}(L/K) \to L^*$ is a 1-cocycle. For any $c \in L$, consider the sum

$$b = \sum_{\sigma \in \mathrm{Gal}(L/K)} f(\sigma)\sigma(c).$$

If $b = 0$ for all c, then the elements of $\mathrm{Gal}(L/K)$ are linearly dependent. But in view of Equation (17.1), this would imply that the conjugates of a normal basis element α would generate a field of degree $< [L : K]$, a contradiction. Thus there exists $c \in L$ with $b \neq 0$. Then for any $\sigma \in \mathrm{Gal}(L/K)$, we have

$$0 \neq \sigma(b) = \sum_{\tau} \sigma(f(\tau))\sigma\tau(c) = \sum_{\sigma\tau} f(\sigma)^{-1} f(\sigma\tau)\sigma\tau(c) = f(\sigma)^{-1} b,$$

so $f(\sigma) = b\sigma(b)^{-1}$, hence f is a coboundary. □

Theorem 17.5 (Hilbert's Theorem 90)**.** *Suppose* $\mathrm{Gal}(L/K)$ *is finite cyclic, with generator* σ*. If* $\alpha \in L^*$ *has norm* 1*, then there exists* $\beta \in L^*$ *such that* $\alpha = \beta/\sigma(\beta)$*.*

Proof. Recall that when G is a finite cyclic group and A is a G-module, then

$$\mathrm{H}^1(G, A) \cong \ker(N_A)/I_G(A).$$

By Proposition 17.4, we have $\mathrm{H}^1(L/K, L^*) = 0$, so the kernel of norm on L^* equals the image of $1 - \sigma \in \mathbb{Z}[\mathrm{Gal}(L/K)]$. Thus α, which is in the kernel of the norm, is of the form $(1 - \sigma)\beta = \beta/\sigma(\beta)$ for some β. (Note that the group ring is written additively, which is why minus changes to inverse.) □

Remark 17.6. Here is an amusing consequence of Theorem 17.5. Let $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Then $\alpha = a + bi \in \mathbb{Q}(i)$ has norm 1 if and only if $a^2 + b^2 = 1$, i.e., (a, b) is a rational point on the unit circle. Theorem 17.5 asserts that there is $\beta = c + di$ such that

$$a + bi = \frac{\beta}{\sigma(\beta)} = \frac{c + di}{c - di} = \frac{(c + di)^2}{c^2 + d^2} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i.$$

This recovers the standard parameterization of rational points on the unit circle.

Later we will study the *Brauer group* of a field K

$$\mathrm{Br}(K) = \mathrm{H}^2(K, (K^{\mathrm{sep}})^*),$$

which can be very large and subtle.

18 Kummer Theory

18.1 Kummer Theory of Fields

Kummer theory is concerned with classifying the abelian extensions of exponent n of a field K, assuming that K contains the nth roots of unity. It's a generalization of the correspondence between quadratic extensions of $\mathbb{Q}$ and non-square squarefree integers.

Let n be a positive integer, and let K be a field of characteristic prime to n. Let L be a separable closure of K. Let $\mu_n(L)$ denote the set of elements of order dividing n in L.

Lemma 18.1. $\mu_n(L)$ *is a cyclic group of order* n*.*

Proof. The elements of $\mu_n(L)$ are exactly the roots in L of the polynomial $x^n - 1$. Since n is coprime to the characteristic, all roots of $x^n - 1$ are in L, so $\mu_n(L)$ has order at least n. But K is a field, so $x^n - 1$ can have at most n roots, so $\mu_n(L)$ has order n. Any finite subgroup of the multiplicative group of a field is cyclic, so $\mu_n(L)$ is cyclic. $\square$

Consider the exact sequence

$$1 \to \mu_n(L) \to L^* \xrightarrow{x \mapsto x^n} L^* \to 1$$

of $G_K = \mathrm{Gal}(L/K)$-modules. The associated long exact sequence of Galois cohomology yields

$$1 \to K^*/(K^*)^n \to \mathrm{H}^1(K, \mu_n(L)) \to \mathrm{H}^1(K, L^*) \to \cdots .$$

We proved that $\mathrm{H}^1(K, L^*) = 0$, so we conclude that

$$K^*/(K^*)^n \cong \mathrm{H}^1(K, \mu_n(L)),$$

where the isomorphism is via the δ connecting homomorphism. If $\alpha \in L^*$, we obtain the corresponding element $\delta(\alpha) \in \mathrm{H}^1(K, \mu_n(L))$ by finding some $\beta \in L^*$ such that $\beta^n = \alpha$; then the corresponding cocycle is $\sigma \mapsto \sigma(\beta)/\beta \in \mu_n(L)$.

As a special case, consider $n = 2$ and $K = \mathbb{Q}$. Then we have $\mu_2(\bar{\mathbb{Q}}) = \{\pm 1\}$, on which $G_{\mathbb{Q}}$ acts trivially. Recall that $\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A)$ when G acts trivially on A. Thus

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 \cong \mathrm{Hom}(G_{\mathbb{Q}}, \{\pm 1\}),$$

where the homomorphisms are continuous. The set of squarefree integers are representative elements for the left hand side of the above isomorphism. The right hand side is the set of *continuous* homomorphisms $\varphi : G_{\mathbb{Q}} \to \{\pm 1\}$. To give such a nontrivial homorphism φ is exactly the same as giving a quadratic extension of $\mathbb{Q}$. We thus recover—in a conceptual way—the standard bijection between quadratic fields and squarefree integers $\neq 1$, which is one of the basic facts one learns in a first algebraic number theory course.

We generalize the above construction as follows. Suppose $\mu_n \subset K$, i.e., all the nth roots of unity are already in K. Then we have

$$K^*/(K^*)^n \cong \mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}), \tag{18.1}$$

where as usual the homomorphisms are continuous. We associate to a homomorphism $\varphi : G_K \to \mathbb{Z}/n\mathbb{Z}$ an extension L^H of K, where $H = \ker(\varphi)$, and by Galois theory, $\mathrm{Gal}(L^H/K) \cong \mathrm{image}(\varphi) \subset \mathbb{Z}/n\mathbb{Z}$. Conversely, given any Galois extension M/K with Galois group contained in $\mathbb{Z}/n\mathbb{Z}$, there is an associated homorphism $\varphi : G_K \to \mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$. Define an equivalence relation $\sim$ on $\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})$ by $\varphi \sim \psi$ if $\ker(\varphi) = \ker(\psi)$ (equivalently, $\varphi = m\psi$ for some integer m coprime to n). Then we have a bijection

$$\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z})_{/\sim} \xrightarrow{\cong} \{ \text{ Galois extensions } M/K \text{ with } \mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z} \ \}.$$

Using Equation 18.1 along with the explicit description of δ mentioned above, we thus see that the Galois extensions of K with $\mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$ are the extensions of the form $K(\sqrt[n]{\alpha})$ for some $\alpha \in K^*$. An element $\sigma \in \mathrm{Gal}(M/K)$ acts by $\sqrt[n]{\alpha} \mapsto \sqrt[n]{\alpha}^b$ for some b, and the map $\mathrm{Gal}(M/K) \subset \mathbb{Z}/n\mathbb{Z}$ is $\sigma \mapsto b$.

The above observation is **Kummer theory**: *There is a conceptually simple description of the exponent n abelian extensions of K, assuming that all nth roots of unity are in K.* Of course, understanding $K^*/(K^*)^n$ well involves understanding the failure of unique factorization into primes, hence understanding the unit group and class group of the ring of integers of K well.

When the nth roots of unity are not in K, the situation is much more complicated, and is answered by Class Field Theory.

Remark 18.2. A concise general reference about Kummer theory of fields is Birch's article *Cyclotomic Fields and Kummer Extensions* in Cassels-Frohlich. For a Galois-cohomological approach to Class Field Theory, see the whole Cassels-Frohlich book.

18.2 Kummer Theory for an Elliptic Curve

Let n be a positive integer, and let E be an elliptic curve over a field K of characteristic coprime to n, and let $L = K^{\mathrm{sep}}$. We mimic the previous section, but for the G_K-module $E(L)$ instead of L^*. Consider the exact sequence

$$0 \to E[n] \to E \xrightarrow{[n]} E \to 0.$$

Taking cohomology we obtain an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K, E)[n] \to 0.$$

Unlike the above situation where $\mathrm{H}^1(K, L^*) = 0$, the group $\mathrm{H}^1(K, E)[n]$ is often very large, e.g., when K is a number field, this group is always infinite.

In Kummer theory, we obtained a nice result under the hypothesis that $\mu_n \subset K$. The analogous hypothesis in the context of elliptic curves is that every element of $E[n]$ is defined over K, in which case

$$\mathrm{H}^1(K, E[n]) \approx \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2),$$

where we have used that $E[n](L) \approx (\mathbb{Z}/n\mathbb{Z})^2$, which is a standard fact about elliptic curves, and as usual all homomorphisms are continuous. Another consequence of our hypothesis that $E[n](K) = E[n]$ is that $\mu_n \subset K$; this later fact can be proved using the Weil pairing, which is a nondegenerate G_K-invariant map

$$E[n] \otimes E[n] \to \mu_n.$$

As above, we can interpret the elements $\varphi \in \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2)$ (modulo an equivalence relation) as corresponding to abelian extensions M of K such that $\mathrm{Gal}(M/K) \subset (\mathbb{Z}/n\mathbb{Z})^2$. Moreover, we have upon fixing a choice of basis for $E[n]$, an exact sequence

$$0 \to E(K)/nE(K) \to \mathrm{Hom}(G_K, (\mathbb{Z}/n\mathbb{Z})^2) \to \mathrm{H}^1(K, E)[n] \to 0,$$

or, using Kummer theory from the previous section,

$$0 \to E(K)/nE(K) \to (K^*/(K^*)^n)^2 \to \mathrm{H}^1(K, E)[n] \to 0.$$

Another standard fact about elliptic curves—the (weak) Mordell-Weil theorem—is that when K is a number field, then $E(K)/nE(K)$ is finite. Thus when $E[n](K) = E[n]$, we have a fairly explicit description of $\mathrm{H}^1(K, E)[n]$ in terms of K^* and $E(K)$. This idea is one of the foundations for using descent to compute Mordell-Weil groups of elliptic curves.

If we restrict to classes whose restriction everywhere locally is 0 we obtain the sequence

$$0 \to E(K)/nE(K) \to \mathrm{Sel}^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Here

$$\mathrm{Sel}^{(n)}(E/K) = \ker\left(\mathrm{H}^1(K, E[n]) \to \bigoplus_{\text{all } v} \mathrm{H}^1(K_v, E)\right),$$

and

$$Ш(E/K) = \ker\left(\mathrm{H}^1(K, E) \to \bigoplus_{\text{all } v} \mathrm{H}^1(K_v, E)\right).$$

When K is a number field, it is possible to describe $\mathrm{Sel}^{(n)}(E/K)$ so explicitly as a subgroup of $(K^*/(K^*)^n)^2$ that one can prove that $\mathrm{Sel}^{(n)}(E/K)$ is computable.

Theorem 18.3. *Given any elliptic curve E over any number field K, and any integer n, the group $\mathrm{Sel}^{(n)}(E/K)$ defined above is computable.*

It is a major open problem to show that $E(K)$ is computable. A positive solution would follow from the following conjecture:

Conjecture 18.4 (Shafarevich-Tate)**.** *The group $Ш(E/K)$ is finite.*

Conjecture 18.4 is extremely deep; for example, it is a very deep (hundreds of pages!) theorem when $E/\mathbb{Q}$ has "analytic rank" 0 or 1, and is not known for even a single elliptic curve defined over $\mathbb{Q}$ with analytic rank ≥ 2.

Example 18.5. Consider an elliptic curve E over $\mathbb{Q}$ of the form $y^2 = x(x-a)(x+b)$, so that all the 2-torsion of E is $\mathbb{Q}$-rational. As above, we obtain an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to ((\mathbb{Q}^*)/(\mathbb{Q}^*)^2)^2 \to \mathrm{H}^1(\mathbb{Q}, E)[2] \to 0.$$

From this diagram and the fact that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, we see that $\mathrm{H}^1(\mathbb{Q}, E)[2]$ is infinite. Moreover, given any pair (α, β) of nonzero rational numbers, we can write down an explicit Galois cohomology class in $\mathrm{H}^1(\mathbb{Q}, E)[2]$, and given any rational point $P \in E(\mathbb{Q})$ we obtain a pair of rationals in $((\mathbb{Q}^*)/(\mathbb{Q}^*)^2)^2$.

19 Brauer Groups

This lecture is about Brauer groups.

Reference: Chapter X of Serre's *Local Fields*.

19.1 The Definition

Let k be a field, and fix a separable closure k^{sep} of k.

Definition 19.1. The *Brauer group* of k is

$$\mathrm{Br}_k = \mathrm{H}^2(k, (k^{\mathrm{sep}})^*).$$

The Brauer group of a field is a measure of the complexity of the field. It also plays a central role in duality theorems, and in class field theory.

19.2 Some Motivating Examples

(i) Let E be an elliptic curve over k and n a positive integer coprime to $\mathrm{char}(k)$. Consider the Weil pairing

$$E[n] \otimes E[n] \to \mu_n.$$

Cup product defines a map

$$\mathrm{H}^1(k, E[n]) \otimes \mathrm{H}^1(k, E[n]) \to \mathrm{H}^2(k, \mu_n).$$

The inclusion $\mu_n \hookrightarrow (k^{\mathrm{sep}})^*$ defines a homomorphism

$$\mathrm{H}^2(k, \mu_n) \to \mathrm{H}^2(k, (k^{\mathrm{sep}})^*) = \mathrm{Br}_k\,.$$

We thus have a pairing on $\mathrm{H}^1(k, E[n])$ with values Br_k. It would thus be very handy to understand Brauer groups better.

(ii) If A is a simple abelian variety over k, then $R = \mathrm{End}(A) \otimes k$ is a division algebra over k. Its center is an extension F of k, and R is a central simple F-algebra. As we will see later, the isomorphism classes of central simple F-algebras are in natural bijection with the elements of Br_F. It would thus be very handy, indeed, to understand Brauer groups better.

19.3 Examples

Recall that if G is a finite *cyclic* group and A is a G-module, then $\hat{H}^{2q}(G, A) \approx \hat{H}^0(G, A)$ and $\hat{H}^{2q+1}(G, A) \approx \hat{H}^1(G, A)$, a fact we proved by explicitly writing down the following very simple complete resolution of G:

$$\cdots \to \mathbb{Z}[G] \xrightarrow{s-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{s-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \to \cdots\,,$$

where $N = \sum s^i$ is the norm.

Proposition 19.2. *The Brauer group of the field $\mathbb{R}$ of real numbers has order 2.*

Proof. We have $\mathbb{C} = \mathbb{R}^{\mathrm{sep}}$, and $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is cyclic of order 2. Thus

$$\mathrm{Br}_{\mathbb{R}} = \mathrm{H}^2(G, \mathbb{C}^*) \cong \hat{H}^0(G, \mathbb{C}^*) \approx (\mathbb{C}^*)^G / N\mathbb{C}^* \cong \mathbb{R}^*/\mathbb{R}^*_+ \cong \{\pm 1\}.$$

□

Lemma 19.3. *Suppose G is a finite cyclic group and A is a finite G-module. Then*

$$\#\hat{H}^q(G,A) = \#\hat{H}^0(G,A)$$

for all $q \in \mathbb{Z}$, i.e., $\#\hat{H}^q(G,A)$ is independent of q.

Proof. Since, as was mentioned above, $\hat{H}^{2q}(G,A) \approx \hat{H}^0(G,A)$ and $\hat{H}^{2q+1}(G,A) \approx \hat{H}^1(G,A)$, it suffices to show that $\#\hat{H}^{-1}(G,A) = \#\hat{H}^0(G,A)$. Let s be a generator of G. We have an exact sequence

$$0 \to A^G \to A \xrightarrow{s-1} A \to A/(s-1)A \to 0.$$

Since every term in the sequence is finite,

$$\#A^G = \#(A/(s-1)A).$$

Letting $N_G = \sum s^i$ be the norm, we have by definition an exact sequence

$$0 \to \hat{H}^{-1}(G,A) \to A/(s-1)A \xrightarrow{N_G} A^G \to \hat{H}^0(G,A) \to 0.$$

The middle two terms in the above sequence have the same cardinality, so the outer two terms do as well, which proves the lemma. □

Proposition 19.4. *If k is a finite field, then* $\mathrm{Br}_k = 0$.

Proof. By definition,

$$\mathrm{Br}_k = \mathrm{H}^2(k, \bar{k}^*) = \varinjlim_F \mathrm{H}^2(F/k, F^*),$$

where F runs over finite extensions of k. Because $G = \mathrm{Gal}(F/k)$ is a finite cyclic group, Lemma 19.3 and triviality of the first cohomology of the multiplicative group of a field together imply that

$$\#\,\mathrm{H}^2(F/k, F^*) = \#\hat{H}^1(F/k, F^*) = 1.$$

□

Example 19.5. The following field all have $\mathrm{Br}_k = 0$.

(i) Let k be any algebraically or separably closed field. Then $\mathrm{Br}_k = 0$, obviously, since $k^{\mathrm{sep}} = k$.

(ii) Let k be any extension of transcendance degree 1 of an algebraically closed field. Then $\mathrm{Br}_k = 0$. (See §X.7 of Serre's *Local Fields* for references.)

(iii) Let k be the maximal unramified extension K^{ur} of a local field K with perfect residue field (e.g., the maximal unramified extension of a finite extension of $\mathbb{Q}_p$). Then $\mathrm{Br}_k = 0$. (See §X.7 of Serre's *Local Fields* for references.)

(iv) Let k be any algebraic extension k of $\mathbb{Q}$ that contains *all* roots of unity (thus k is necessarily an infinite degree extension of $\mathbb{Q}$). Then $\mathrm{Br}_k = 0$.

The following theorem is one of the main results of *local class field theory.*

Theorem 19.6. *Let k be a local field with perfect residue field (e.g., a finite extension of $\mathbb{Q}_p$). Then $\mathrm{Br}_k \cong \mathbb{Q}/\mathbb{Z}$.*

The following theorem is one of the main results of *global class field theory.*

Theorem 19.7. *Let k be a number field, and for any place v of k, let k_v be the completion of k at v, so k_v is a p-adic local field, $\mathbb{R}$, or $\mathbb{C}$. We have a natural exact sequence*

$$0 \to \mathrm{Br}_k \to \bigoplus_v \mathrm{Br}_{k_v} \xrightarrow{(x_v)\mapsto\sum x_v} \mathbb{Q}/\mathbb{Z} \to 0,$$

We obtain the map to $\mathbb{Q}/\mathbb{Z}$ by using Theorem 19.6 to view each Br_{k_v} as $\mathbb{Q}/\mathbb{Z}$, and we view $\mathrm{Br}_{\mathbb{R}} = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

19.4 Brauer Groups and Central Simple Algebras

Definition 19.8. Let k be a field. Then a *central simple k-algebra* is a finite dimensional k-algebra A that satisfies any one of the following equivalent conditions:

(i) A has no nontrivial two-sided ideals, and A has center k.

(ii) The algebra $A_{\bar{k}} = A \otimes_k \bar{k}$ is isomorphic to a matrix algebra over $\overline{k}$.

(iii) There is a finite extension F/k such that A_F is isomorphic to a matrix algebra over F.

(iv) A is isomorphic to a matrix algebra over a division algebra D with center k.

We say that two central simple k-algebras are equivalent if the corresponding division algebras D in (iv) above are k-isomorphic. Tensor product endows the set of equivalence classes of central simple k-algebras with the structure of abelian group.

Theorem 19.9. *The group $\mathcal{B}_k$ of equivalence classes of central simple k-algebras is isomorphic to the Brauer group* Br_k.

The proof of Theorem 19.9 is somewhat involved. We will content ourselves with sketching some of the main ideas; in particular, we will explicitly construct the homomorphism $\mathcal{B}_k \to \mathrm{Br}_k$, but will not prove that it is an isomorphism (the argument, which uses descent, is given in Serre's *Local Fields*).

Fix a finite Galois extension F of k and let $\mathcal{B}(n, F/k)$ be the set of equivalence classes of central simple k-algebras A such that $A_F \approx M_n(F)$, where $M_n(F)$ is the algebra of $n \times n$ matrices over F. Then $\mathcal{B}$ is the union of all $\mathcal{B}(n, F/k)$ over all n and F.

Given $A \in \mathcal{B}(n, F/k)$, let $\varphi : A_F \to M_n(F)$ be a fixed choice of isomorphism. Define a set-theoretic map

$$f : \mathrm{Gal}(F/k) \to \mathrm{Aut}_F(M_n(F)) \approx \mathrm{PGL}_n(F)$$

by

$$f(s) = \varphi^{-1} \circ s(\varphi) = \varphi^{-1} \circ s \circ \varphi \circ s^{-1}$$

Then

$$[f] \in \mathrm{H}^1(F/k, \mathrm{PGL}_n(F)),$$

where this H^1 is a cohomology *set* (!).

Proposition 19.10. *The above construction $A \mapsto [f]$ defines a bijection between $\mathcal{B}(n, F/K)$ and $\mathrm{H}^1(F/k, \mathrm{PGL}_n(F))$.*

(The above proposition is proved in Serre's *Local Fields*.)

Consider the exact sequence

$$1 \to F^* \to \mathrm{GL}_n(F) \to \mathrm{PGL}_n(F) \to 1.$$

There is a well-defined connecting homorphism

$$\mathrm{H}^1(F/k, \mathrm{PGL}_n(F)) \to \mathrm{H}^2(F/k, F^*).$$

Since $\mathrm{H}^2(F/k, F^*) \xrightarrow{\mathrm{inf}} \mathrm{Br}_k$, we thus obtain a natural map

$$\mathcal{B}(n, F/K) \to \mathrm{Br}_k\,.$$

This induces the claimed isomorphism $\mathcal{B} \to \mathrm{Br}_k$.

20 Galois Cohomology of Abelian Varieties

20.1 Principal Homogenous Spaces for Abelian Varieties

See also Pete Clark's http://math.uga.edu/~pete/wcnotes.pdf.

An *abelian variety* A over a field k is a projective group variety, i.e., a projective variety that is equipped with a group structure $A \times A \to A$ and $1_A : k \to A$. Perhaps the first basic theorem about abelian varieties is that their group structure is commutative. We will not prove this here, since it requires too much algebraic geometry (for a complete proof readable by anybody who has read Hartshorne's *Algebraic Geometry*, see Milne's *Abelian Varieties* article in Cornell-Silverman).

A *principal homogenous space* for an abelian variety A over a field k is a variety X over k and a morphism $\iota : A \times X \to X$ that satisfies the axioms of a simply transitive group action.

If F is any field such that $X(F) \neq \emptyset$, then $A_F \approx X_F$, so we can view the principal homogenous spaces for A as twists of A as algebraic varieties (not as abelian varieties). Two principal homogenous spaces are equivalent if there is a morphism $X \to Y$ such that natural compatibility holds.

Given principal homomogenous spaces X and Y, the *Baer sum* defines a new principal homogenous space. Define an action of A on $X \times Y$ by $(a, x \times y) = (a, x) \times (-a, y)$. The Baer sum of X and Y is the quotient of $X \times Y$ by this action. The diagonal action $a.(x \times y) = ax \times ay$ then gives the Baer sum the structure of principal homogeneous space for A.

The collection of isomorphism classes of principal homomogenous spaces for a fixed abelian variety A over k equipped with Baer sum is an abelian group, called the *Weil-Chatalet* group of A, and denoted $\mathrm{WC}(A/k)$.

Theorem 20.1 (Lang-Tate, 1958)**.** *There is a natural isomorphism* $\mathrm{WC}(A/k) \to \mathrm{H}^1(k, A)$.

Sketch of Proof. Given a principal homogenous space X for A, we construct an element of $\mathrm{H}^1(k, A)$ as follows. Since X is a variety of positive dimension, there is a finite extension of k such that $X(F) \neq \emptyset$. Fix a choice of $P \in X(F)$. For $a \in A$ and $x \in X$, write $a + x$ for the image of (a, x) under the principal homogenous space map $A \times X \to X$. Define a map $f : G_k \to A$ by sending $\sigma \in G_k$ to

$$\sigma(P) - P$$

which means "the unique element $a \in A$ such that

$$a + P = \sigma(P).$$

The map f is a 1-cocycle because

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

where we have used the axioms that the principal homogenous space structure satisfy.

Conversely, constructing a principal homogenous space from a cycle f, is called "descent of the base field". The idea is that we find a finite extension F such that $f|_{G_F} = 0$, i.e., an extension that splits f. Then the data of (A_F, f_{G_F}) is "descent datum", which determines an algebraic variety X over k. See Serre *Algebraic Groups and Class Fields*, Section ???, for more details. □

Example 20.2. If A has dimension 1 then A is an elliptic curve. The principal homogenous spaces X for A are genus 1 curves with $\mathrm{Jac}(X) = A$. If A is defined over a number field k, then the nonzero elements of $Ш(A)$ are in bijection with the set of equivalence classes of principal homogenous spaces X such that $X(k_v) \neq \emptyset$ for all places v of k, yet $X(k) = \emptyset$. Thus $Ш(A)$ measures the obstruction to a local-to-global principal.

20.2 Galois Cohomology of Abelian Varieties over Finite Fields

Let A be an abelian variety over a finite field k.

The following theorem was proved by Lang in 1956. A more modern prove is given in the first few sections of Chapter VI of Serre's *Algebraic Groups and Class Fields*. Note that Lang actually proved a more general result about algebraic groups.

Theorem 20.3 (Lang, 1956)**.** *Let A be any connected algebraic group over a finite field (e.g., an abelian variety). Then* $\mathrm{H}^1(k, A) = 0$.

Proof. The following proof is based on what Pete Clark posted in the notes mentioned above. This proof has the advantage that it uses techniques that fit very nicely in the context of the rest of this course.

It suffices to show that $\mathrm{H}^1(k, A)[n] = 0$ for every positive integer n. The Kummer sequence associated to $0 \to A[n] \to A \to A \to 0$ is

$$0 \to A(k)/nA(k) \to \mathrm{H}^1(k, A[n]) \to \mathrm{H}^1(k, A)[n] \to 0.$$

It thus sufficies to prove that

$$\#(A(k)/nA(k)) = \#\,\mathrm{H}^1(k, A[n]).$$

We have an exact sequence of finite abelian groups

$$0 \to A(k)[n] \to A(k) \xrightarrow{[n]} A(k) \to A(k)/nA(k) \to 0.$$

Thus

$$\#A(k)[n] = \#(A(k)/nA(k)),$$

so now we just have to show that

$$\#\,\mathrm{H}^1(k, A[n]) = \#A(k)[n].$$

We have

$$\#\hat{H}^0(F/k, A(F)[n]) = \#\hat{H}^1(F/k, A(F)[n])$$

for all finite extensions F of k. In particular let F be any extension of $k(A[n])$ of degree divisible by n. Because the norm map is multiplicative in towers, we have

$$\mathrm{Tr}_{F/k}(A[n]) = \mathrm{Tr}_{k(A[n])/k}(\mathrm{Tr}_{F/k(A[n])}(A[n])) = \mathrm{Tr}_{k(A[n])/k}([n]A[n]) = \mathrm{Tr}_{k(A[n])/k}(0) = 0.$$

Thus

$$\hat{H}^0(F/k, A[n](F)) = A(k)[n]/\,\mathrm{Tr}_{F/k}(A[n]) = A(k)[n],$$

where here we write Tr instead of the usual "norm" to denote the element $\sum \sigma^i$, where $\mathrm{Gal}(F/k) = \langle\sigma\rangle$. Thus for all finite extensions of M/F, we have

$$\#\hat{H}^1(M/k, A[n](M)) = \#A(k)[n].$$

By taking compositums, we see that *every* extension of k is contained in a finite extension of F, so

$$\#\,\mathrm{H}^1(k, A[n]) = \#\varinjlim_{M/F} \hat{H}^1(M/k, A[n]) = \#A(k)[n].$$

This proves the theorem. □

Remark 20.4. When A is an elliptic curve the Hasse bound and Theorem 20.1 imply the theorem. Indeed, any $X \in \mathrm{WC}(A/k)$ is a genus 1 curve over the finite field k, hence

$$|\#X - \#k - 1| \leq 2\sqrt{\#k}.$$

It follows that $\#X \geq \#k + 1 - 2\sqrt{\#k} > 0$.

We have the following incredibly helpful corollary:

Corollary 20.5. *If $0 \to A \to B \to C \to 0$ is an exact sequence of abelian varieties over a finite field k, then $0 \to A(k) \to B(k) \to C(k) \to 0$ is also exact.*

Proof. The cokernel of $B(k) \to C(k)$ is contained in $\mathrm{H}^1(k, A) = 0$. □

Example 20.6. Suppose E is an optimal elliptic curve quotient of $J = J_0(N)$ and $p \nmid N$ is a prime. Then for any integer $n \geq 1$, the induced natural map

$$J(\mathbb{F}_{p^n}) \to E(\mathbb{F}_{p^n})$$

is surjective. If $E[\ell]$ is irreducible, one can use Ihara's theorem to also prove that $J(\mathbb{F}_{p^2})^{\mathrm{ss}}(\ell) \to E(\mathbb{F}_{p^2})(\ell)$ is surjective, where $J(\mathbb{F}_{p^2})^{\mathrm{ss}}$ is the group generated by supersingular points.

Corollary 20.7. *We have $\mathrm{H}^q(k, A) = 0$ for all $q \geq 1$. (In fact, we have $\hat{H}^q(k, A) = 0$ for all $q \in \mathbb{Z}$.)*

Proof. Suppose F is any finite extension of the finite field k. Then $\mathrm{Gal}(F/k)$ is cyclic, so by a result we proved before (lecture 13), we have

$$\#\hat{H}^q(F/k, A(F)) = \#\hat{H}^1(F/k, A(F)) = 1$$

for all $q \in \mathbb{Z}$. □

Corollary 20.8. *If F/k is a finite extension of finite fields, and A is an abelian variety, then the natural trace map*

$$\mathrm{Tr}_{F/k} : A(F) \to A(k)$$

is surjective.

Proof. By Corollary 20.7 and the definition, we have

$$0 = \hat{H}^0(F/k, A(F)) = A(k)/\mathrm{Tr}_{F/k}(A(F)).$$

□

Let A be an abelian variety over a number field K, and v a prime of K, with residue class field $k = k_v$. The Néron model $\mathcal{A}$ of A is a smooth commutative group scheme over the ring $\mathcal{O}_K$ of integer of K with generic fiber A such that for all smooth commutative group schemes S the natural map

$$\mathcal{A}(S) \to A(S_K)$$

is an isomorphism. Reducing modulo v we have an exact sequence

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_{A,v} \to 0, \tag{20.1}$$

where $\mathcal{A}_k^0$ is the connected component that contains the identity and $\Phi_{A,v}$ is a finite flat group scheme over k, called the *component group* of A at v.

Proposition 20.9. *For every integer q, we have*

$$\hat{H}^q(k, \mathcal{A}_k) = \hat{H}^q(k, \Phi_{A,v}).$$

Proof. Take Galois cohomology associated to the exact sequence (20.1), and use Corollary 20.7. □

21 Duality

WARNING: For the rest of this book, we're going to let $\bar{k}$ denote a separable closure of k, since it's much easier notation to work with (I'll go back and change the notation above later).

Let k be a field and $\bar{k}$ a choice of separable closure of k.

21.1 Duality over a Local Field

Let M be any $G_k = \mathrm{Gal}(\bar{k}/k)$-module and set

$$\hat{M} = \mathrm{Hom}(M, \bar{k}^*),$$

which we give the structure of (left) G_k-module by

$$(g.\varphi)(a) = g(\varphi(g^{-1}a)).$$

To see that this gives $\hat{M}$ a G_k-module structure, note that if $g, h \in G_K$, then

$$((gh).\varphi)(a) = (gh)(\varphi((gh)^{-1}a)) = (gh)(\varphi(h^{-1}g^{-1}a))$$

and

$$(g.(h.\varphi))(a) = g((h.\varphi)(g^{-1}a)) = g(h(\varphi(h^{-1}g^{-1}a))).$$

Theorem 21.1 (Tate Local Duality)**.** *Let k be a local field and M a finite G_k-module of order coprime to the characteristic of k. Then for $r = 0, 1, 2$, the cup product pairing*

$$\mathrm{H}^r(k, M) \times \mathrm{H}^{2-r}(k, \hat{M}) \to \mathrm{H}^2(k, \bar{k}^*) \cong \mathbb{Q}/\mathbb{Z}$$

is nondegenerate. Also $\mathrm{H}^q(k, M) = 0$ for $q \geq 3$.

The proof of this theorem is beyond the scope of this course, since it requires developing too much general machinery. See [Ser97] for complete details.

21.1.1 Example: n-torsion on an elliptic curve

Let k be a local field and $M = E[n]$ the points of order n on an elliptic curve over k. The Weil pairing is a nondegenerate perfect pairing

$$E[n] \otimes E[n] \to \mu_n,$$

hence defines a G_k-isomorphism $E[n] \cong \widehat{E[n]}$. Thus for $r = 0, 1, 2$, we obtain nondegenerate pairings

$$\mathrm{H}^r(k, E[n]) \times \mathrm{H}^{2-r}(k, E[n]) \to \mathbb{Q}/\mathbb{Z}.$$

For $r = 0$, the nondegenerate pairing is

$$E(k)[n] \times \mathrm{H}^2(k, E[n]) \to \mathbb{Q}/\mathbb{Z},$$

which thus allows us to compute

$$\mathrm{H}^2(k, E[n]) \cong \mathrm{Hom}(E(k)[n], \mathbb{Q}/\mathbb{Z}) \approx E(k)[n].$$

For $r = 1$, the pairing is

$$\mathrm{H}^1(k, E[n]) \times \mathrm{H}^1(k, E[n]) \to \mathbb{Q}/\mathbb{Z}. \tag{21.1}$$

Thus given any element $x \in \mathrm{H}^1(k, E[n])$ we obtain a homomorphism

$$\varphi_x : \mathrm{H}^1(k, E[n]) \to \mathbb{Q}/\mathbb{Z},$$

and $\varphi_x = 0$ if and only if $x = 0$.

Tate also proved the following related duality theorem, which gives a very nice way to think about the Galois cohomology of an abelian variety over a local field. Let A be an abelian variety over a local field k, and let $A^\vee$ denote tha dual abelian variety. When A has dimension 1 or when A is the Jacobian of a curve, then $A^\vee \cong A$.

Theorem 21.2 (Tate)**.** *We have* $\mathrm{H}^q(k, A) = 0$ *for* $q \geq 2$*. Moreover, there is a canonical pairing*

$$\mathrm{H}^0(K, A^\vee) \times \mathrm{H}^1(K, A) \to \mathbb{Q}/\mathbb{Z},$$

which induces an isomorphism (of discrete groups)

$$\mathrm{H}^1(K, A) \xrightarrow{\cong} \mathrm{Hom}(A^\vee(K), \mathbb{Q}/\mathbb{Z}).$$

(All homs are continuous.)

The following proposition is proved using formal groups; it's Proposition VII.6.3 in [Sil92].

Proposition 21.3. *Suppose E is an elliptic curve over a finite extension k of $\mathbb{Q}_p$ and let R be the ring of integers of k. Then $E(k)$ contains a subgroup of finite index that is isomorphic to $(R, +)$.*

For simplicity, assume that $R = \mathbb{Z}_p$. Then we have an exact sequence

$$0 \to \mathbb{Z}_p \to E(\mathbb{Q}_p) \to M \to 0,$$

where M is a finite group. Applying the $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ (continuous homomorphisms) *Pontryagin duality* gives an exact sequence

$$0 \to \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(E(\mathbb{Q}_p), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}_p, \mathbb{Q}/\mathbb{Z}) \to 0.$$

We have

$$\mathrm{Hom}(\mathbb{Z}_p, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}_p/\mathbb{Z}_p,$$

where the isomorphism sends $\varphi : \mathbb{Z}_p \to \mathbb{Q}/\mathbb{Z}$ to $\varphi(1) \in \mathbb{Q}_p/\mathbb{Z}_p \subset \mathbb{Q}/\mathbb{Z}$. Thus we have an exact sequence

$$0 \to F \to \mathrm{H}^1(\mathbb{Q}_p, E) \to \mathbb{Q}_p/\mathbb{Z}_p \to 0,$$

where F is a finite group. So that's what cohomology of an elliptic curve over a local field looks like:

> *The group $\mathrm{H}^1(\mathbb{Q}_p, E)$ has a lot of elements of order a power of p, and not much else.*

21.2 Duality over a Finite Field

Let k be a finite field. Then the dualizing module is $\mathbb{Q}/\mathbb{Z}$ with trivial action (not $\bar{k}^*$ as above), and we define

$$M^* = \mathrm{Hom}(M, \mathbb{Q}/\mathbb{Z}).$$

Theorem 21.4. *For every finite module M and $r = 0, 1$, cup product induces a nondegenerate pairing*

$$\mathrm{H}^r(k, M) \times \mathrm{H}^{1-r}(k, M^*) \to \mathbb{Q}/\mathbb{Z}.$$

22 A Little Background Motivation for Étale Cohomology

22.1 Schemes

Schemes are algebraic-geometric objects that generalize the notion of variety and, like manifolds, are built by glueing together special types of objects called affine schemes. The category of commutative rings is equivalent (via a contravariant functor) to a subcategory of the category of schemes, so schemes generalize the notion of commutative rings.

Affine schemes $X = \mathrm{Spec}(R)$ are geometric objects attached to commutative rings. Here X is a locally ringed topological space. The set of points of X is the set of prime ideals of the ring R. The closed sets for the (Zariski) topology on X are the subsets

$$V(I) = \{\mathfrak{p} \in X : I \subset \mathfrak{p}\}$$

attached to ideals $I \subset R$. To say that X is locally ringed means that there is a sheaf $\mathcal{O}_X$ of rings on X, i.e., a certain type of functor from the category of open subsets of X to the category of rings. In particular, if $U = X - V(I)$ is an open set with I prime, then

$$\mathcal{O}_X(U) = R_I$$

is the localization of R at I, which is obtained by adjoining to R the inverses of the multiplicatively closed subset all elements of R not in I.

Example 22.1. Let $X = \mathrm{Spec}(K)$, where K is a field. Then there is exactly one prime ideal, the 0 ideal, so $\#X = 1$, i.e., X is a point. The structure sheaf is $\mathcal{O}_X(X) = K$.

Example 22.2. Let $X = \mathrm{Spec}(\mathbb{Z}_p)$, where $\mathbb{Z}_p$ is the ring of p-adic integers. Then as a set $X = \{(0), (p)\}$, since $\mathbb{Z}_p$ has exactly two prime ideals. There are two nonempty open sets: X itself and $U = \{(0)\} = X - V((p))$. We have $\mathcal{O}_X(X) = \mathbb{Z}_p$ and $\mathcal{O}_X(U) = R_{(p)} = \mathbb{Z}_p$, since everything not in (p) is already invertible in $\mathbb{Z}_p$. One interesting thing about $\mathrm{Spec}(\mathbb{Z}_p)$ is that the natural quotient homomorphism $\mathbb{Z}_p \to \mathbb{F}_p$ induces a morphism of schemes:

$$\mathrm{Spec}(\mathbb{F}_p) \hookrightarrow \mathrm{Spec}(\mathbb{Z}_p).$$

Example 22.3. The multiplicative group $\mathbb{G}_m$ is the scheme

$$\mathbb{G}_m = \mathrm{Spec}(\mathbb{Z}[X, Y]/(XY - 1)).$$

It has a group scheme structure, in that there is a multiplication map $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ and an identity section $\mathrm{Spec}(\mathbb{Z}) \to \mathbb{G}_m$.

22.2 Étale Cohomology

Inspired by Serre's introduction of homological techniques into Algebraic Geometry, Grothendieck introduced the idea of étale cohomology in 1958. He was partly motivated by a desire to more deeply understand and prove Weil's conjectures, which imply the function field analogue of the Riemann Hypothesis (Deligne did indeed prove these conjectures in the 1970s using étale cohomology). Étale cohomology gives a precise meaning to

$$\mathrm{H}^q_{\text{ét}}(X, \mathcal{F}),$$

where X is a scheme and $\mathcal{F}$ is a "sheaf for the étale site on X", which is a generalization of the notion of module (and also related to the notion of sheaf for the Zariski topology on X). An example of a scheme is $X = \mathrm{Spec}(K)$, where K is a field, in which case étale sheaves are in bijection with G_K-modules, and

$$\mathrm{H}^q_{\text{ét}}(X, \mathcal{F}) = \mathrm{H}^q_{\text{ét}}(\mathrm{Spec}(K), \mathcal{F}) = \mathrm{H}^q(K, \mathcal{F}(\bar{K}))$$

is just the usual concrete notion of Galois chomology that we now know and love.

Thus étale cohomology is an extremely powerful and natural generalization of Galois cohomology.

Remark 22.4. If you know sheaf cohomology in the context of algebraic geometry and the Zariski topology on a scheme (e.g., chapter 3 of Hartshorne's book *Algebraic Geometry*), then you'll find the following interesting:

> "The reason that the Zariski topology does not work well is that it is too coarse: it has too few open sets. There seems to be no good way to fix this by using a finer topology on a general algebraic variety. Grothendieck's key insight was to realize that there is no reason why the more general open sets should be subsets of the algebraic variety: the definition of a sheaf works perfectly well for any category, not just the category of open subsets of a space. He defined étale cohomology by replacing the category of open subsets of a space by the category of étale mappings to a space: roughly speaking, these can be thought of as open subsets of finite unbranched covers of the space. These turn out (after a lot of work) to give just enough extra open sets that one can get reasonable cohomology groups..."
>
> – the Wikipedia article on étale cohomology

23 Étale Cohomology over a DVR

As mentioned above, étale cohomology of $\mathrm{Spec}(K)$, when K is a field, is the same thing as Galois cohomology over K. Perhaps the simplest example in which étale cohomology is *not* just usual Galois cohomology is the case when $X = \mathrm{Spec}(R)$ is the spectrum of a discrete valuation ring. In this section, we study this case in explicit detail.

23.1 Discrete Valuation Rings

A local ring is a ring with a unique maximal ideal, and a *discrete valuation ring (DVR)* is a local principal ideal domain. We let R be a discrete valuation ring (DVR) with field of fractions K and perfect residue field k. Any DVR is equipped with a valuation $v : K \to \mathbb{Q}$ such that $R = \{\alpha \in K : v(\alpha) \geq 0\}$.

Example 23.1. We give some examples and non-examples of DVR's:

(i) For example, we could take $R = \mathbb{Z}_p$ with p-adic valuation, $K = \mathbb{Q}_p$, and $k = \mathbb{F}_p$. This choice of R is a (topologically) complete local ring.

(ii) We could take
$$R = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\} \subset \mathbb{Q}$$
with its p-adic valuation, $K = \mathbb{Q}$ and $k = \mathbb{F}_p$. Note that this R is not complete, though R is a local ring.

(iii) We could take $R = \mathbb{F}_p[[t]]$, the ring of power series in t, and $K = \mathbb{F}_p((t))$ and $k = \mathbb{F}_p$.

(iv) The ring $\mathbb{Z}$ with a p-adic valuation is not a DVR, since it has more than one maximal ideal.

(v) The ring $R = \mathbb{F}_p(t)[[X]]$ does not have perfect residue field, so isn't allowed as one of the R's.

23.2 Galois Groups associated to DVR's

Let $\bar{K}$ be a separable closure of K and extend the valuation v of R to $\bar{K}$. Let the subscript of v denote *completion with respect to* v. Let K^{ur} be the maximal unramified extension of K contained in $\bar{K}$. The decomposition group is
$$G_v = \mathrm{Gal}(\bar{K}_v / K_v) \subset \mathrm{Gal}(\bar{K}/K),$$

the inertia group is

$$I_v = \mathrm{Gal}(\bar{K}_v/K_v^{\mathrm{ur}}) \subset G_v,$$

and we set

$$G_k = \mathrm{Gal}(\bar{k}/k).$$

A standard fact, which one proves in a first course in algebraic number theory, is that we have a natural exact sequence

$$1 \to I_v \to G_v \to G_k \to 1.$$

(The nontrivial part is that $G_v \to G_k$ is surjective.)

23.3 Galois Modules over a DVR

For any G_K-module M, let $M^0 = M^{I_v}$, which is a $G_k = G_v/I_v$-module.

Following [Maz73] (Mazur, *Notes on Étale Cohomology of Number Fields*, 1973, extracted from a course he once gave at Orsay in France), we define the category of *Galois modules over* R as follows. The *objects* are diagrams

$$N \xrightarrow{\varphi} M,$$

where N is a G_k-module, M is a G_K-module, and φ is a homomorphism of abelian groups that sends N into $M^0 \subset M$, and when viewed as a map of N into M^0 is a homomorphism of G_k-modules. A morphism is a commuting square

$$\begin{array}{ccc} N & \xrightarrow{\varphi} & M \\ \downarrow & & \downarrow \\ N' & \xrightarrow{\psi} & M' \end{array}$$

We will also frequently write the above diagram as a tuple

$$(M, N, \varphi),$$

where of course $\varphi : N \to M$ satisfies the above conditions.

In Section 24.3 we will define the category of "abelian sheaves on the étale site over $\mathrm{Spec}(R)$".

Theorem 23.2. *There is a natural equivalence of categories between the category S_R of triples (M, N, φ) and the category of "abelian sheaves for the étale topology on* $\mathrm{Spec}(R)$*".*

Thus studying cohomology in the category S_R of Galois modules over R is exactly the same as studying étale cohomology of abelian sheaves on the étale site over $\mathrm{Spec}(R)$. However, it is more explicit and concrete.

Example 23.3. Let M be any G_K-module and let $N = M^0$ and $\mathrm{id} : N \hookrightarrow M$ be the natural inclusion. Then (M, M^0, id) is a Galois module over R.

Example 23.4. Let A be any abelian group equipped with trivial Galois action, and set $N = M = A$ above and φ the identity map. In terms of a triple, we write this element of S_R as $(A, A, 1_A)$. We call such a Galois module *constant*. For example, we denote by $\mathbb{Z}$ the Galois module obtained in this way by taking $A = \mathbb{Z}$.

Example 23.5. Let

$$U = \{\alpha \in (K^{\mathrm{ur}})^* : v(\alpha) = 0\}$$

be the group of units in the ring of integers of the maximal unramified extension K^{ur} of K. Then

$$\mathbb{G}_{m,R} = (\bar{K}^*, U, \mathrm{id}).$$

is a Galois module, since $(\bar{K}^*)^0 = (K^{\mathrm{ur}})^*$ contains U.

23.4 The Natural Functors

In order to better understand S_R, we introduce several natural functors. We define the following functors:
pullbacks:

$$i^* : (M, N, \varphi) \mapsto N; \qquad j^* : (M, N, \varphi) \to M;$$

push forward:

$$i_* : N \mapsto (0, N, 0); \qquad j_* : M \mapsto (M, M^0, \mathrm{id}).$$

extension by zero over a closed point:

$$j_! : M \mapsto (M, 0, 0)$$

sections with support on a closed point:

$$i^! : (M, N, \varphi) \mapsto \ker(\varphi)$$

Thus we have defined functors as follows:

$$i^* : S_R \to S_k,\ j^* : S_R \to S_K,\ i_* : S_k \to S_R,$$
$$j_* : S_K \to S_R,\ j_! : S_K \to S_R,\ i^! : S_R \to S_k.$$

The functors $i^*, i_*, j^*, j_!$ are exact, and j_* and $i^!$ are left exact.

23.5 Cohomology of Galois Modules over a DVR

Let $\mathbb{Z}$ be the Galois module from Definition 23.4 and let F be any Galois module. In this section, we define

$$\mathrm{H}^q(R, F)$$

for Galois modules F over a DVR R. This is our first generalization of Galois cohomology in the direction of *étale cohomology*.

Definition 23.6 (Cohomology over a DVR)**.** Let

$$\mathrm{H}^q(R, F) = \mathrm{Ext}^q_{S_R}(\mathbb{Z}, F)$$

Letting

$$\Gamma_R(F) = \mathrm{Hom}_{S_R}(\mathbb{Z}, F),$$

we have

$$\mathrm{Ext}^q_{S_R}(\mathbb{Z}, F) = (R^q\Gamma_R)(F),$$

where R^q denotes the qth right derived functor of the left exact functor Γ_R. Thus to compute $\mathrm{H}^q(R, F)$ we find a resolution of either $\mathbb{Z}$ or F in the category S_R of Galois modules over R, then apply the appropriate Hom functor in the category S_R and take the (co-)homology of the resulting complex.

The following result generalizes Hilbert's theorem 90, and also emphasizes how étale cohomology and Galois cohomology can differ.

Theorem 23.7. *We have*

$$\mathrm{H}^q(R, \mathbb{G}_{m,R}) = \begin{cases} R^* & \text{if } q = 0, \\ 0 & \text{otherwise.} \end{cases}$$

24 The Étale Topology

See §III.3 of Hartshorne for the following general definition of étale morphism $f : X \to Y$ of schemes: *f is étale if it is smooth of relative dimension* 0. Since "smooth" and "relative dimension" take some work to define, we will instead give a more concrete definition. By Corollary I.3.16 in Milne's published book [Mil80], we may define étale as follows.

Definition 24.1. A morphism $f : X \to Y$ of schemes is *étale* if for every $x \in X$, there exists open affine neighborhoods $V = \mathrm{Spec}(C)$ of x and $U = \mathrm{Spec}(A)$ of $y = f(x)$, and polynomials $P, b \in A[t]$ with P monic, such that

$$C \approx A[t, u]/(P,\, bu - 1),$$

with P' a unit in C. (Here the map $A \to C$ is induced by f.)

Figure 24.1: Typical Result of Google Image Search for "Étale"

Thus locally on rings, any étale morphism is obtained by adjoining an element and inverting an element to remove any ramified primes.

Example 24.2. Let $X = \mathrm{Spec}(\mathbb{Z}[i, 1/2])$ and $Y = \mathrm{Spec}(\mathbb{Z})$. Then the map $\mathbb{Z} \hookrightarrow \mathbb{Z}[i, 1/2]$ induces an étale morphism $X \to Y$, since taking $P = t^2 + 1$ and $b = 2t$, we have

$$\mathbb{Z}[i, 1/2] \cong \mathbb{Z}[t, u]/(t^2 + 1, 2tu - 1),$$

and $P' = 2t$ is a unit in $\mathbb{Z}[t, u]/(t^2 + 1, 2tu - 1)$. Note that if we took $b = 1$ instead of $b = 2$, then P' would not be a unit. More generally, if P is any squarefree monic polynomial, then $\mathbb{Z}[t, u]/(P, P' \cdot tu - 1)$ is étale over $\mathbb{Z}$.

An incredibly useful fact about étale morphisms is that they are "closed under base extension", in the sense of the following theorem:

Theorem 24.3. *If $f : X \to Y$ is étale and $g : Z \to Y$ is any morphism of schemes at all, then the map $f' : Z \times_Y X \to Z$ obtained by fiber product is étale.*

$$\begin{array}{ccc} Z \times_Y X & \longrightarrow & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ Z & \xrightarrow{\;g\;} & Y \end{array}$$

Proof. Hartshorne. □

Remark 24.4. It is frequently the case in algebraic geometry that interesting classes of morphisms are "closed under base extension".

Example 24.5. Suppose R is a DVR with fraction field K and residue class field k. Suppose L is any finite seperable extension of K. Then the morphism $\mathrm{Spec}(L) \to X = \mathrm{Spec}(R)$ induced by $R \hookrightarrow K \subset L$ is an étale morphism. To see this, in Definition 24.1, take $V = \mathrm{Spec}(K)$, which is an affine open subset of $X = \mathrm{Spec}(R)$, as $\{(0)\}$ is open, and the map $\mathrm{Spec}(K) \hookrightarrow \mathrm{Spec}(R)$ has image $\{(0)\}$. Since L is finite separable, we have $L = K[t]/(P)$ for some polynomial P with $0 \neq P' \in L$.

24.1 Special Cases of Interest

Suppose $X = \mathrm{Spec}(R)$, where R is a Dedekind domain, DVR, or field. Suppose $R \subset E$ is an extension (with E of the same type as R, e.g., Dedekind domain, DVR, or field) with E finitely generated as an R-module. In case R is a Dedekind domain, suppose $0 \neq b \in E$ and let

$$R' = E_b = E[1/b]$$

be the localization of E away from b. Geometrically

$$\mathrm{Spec}(E_b) = \mathrm{Spec}(E) - \{ \text{ finitely many points } \},$$

where the omitted points are the prime ideals that contain b, i.e., those that divide the ideal generated by b. Then the extension $R \subset R'$ induces an étale morphism $\mathrm{Spec}(R') \to X$ if and only if every prime of R' is unramified over R.

If R is a field, then $\mathrm{Spec}(E) \to X$ is étale if and only if E is a finite separable extension of R (note that E just has to be a product of fields). When R and E are both DVR's, then $\mathrm{Spec}(E) \to X$ is étale if E is unramified over R.

24.2 Étale Coverings

For $X = \mathrm{Spec}(R)$, let $\acute{\mathrm{E}}\mathrm{t}(X)$ denote the category of all schemes Y/X where the structure morphism $Y \to X$ is étale.

An *étale covering* of an object Y in $\acute{\mathrm{E}}\mathrm{t}(X)$ is a collection $\{U_i \xrightarrow{f_i} Y\}$ of $U_i \in \acute{\mathrm{E}}\mathrm{t}(X)$ such that the union of the images equals Y, i.e.,

$$Y = \bigcup_i f_i(U_i).$$

Example 24.6. Let $Y = X = \mathrm{Spec}(\mathbb{Z})$, let $U_1 = \mathbb{Z}[i][\frac{1}{2}]$ and $U_2 = \mathbb{Z}[\zeta_3][\frac{1}{3}]$. Then $U_1 \to Y$ and $U_2 \to Y$ are étale morphisms and $\{U_1, U_2\}$ is an étale covering of Y.

24.3 Étale Sheaves

Definition 24.7 (Étale Site on X)**.** The *(small) étale site* on X is the category $\text{Ét}(X)$ with "topology" given by étale coverings.

Definition 24.8 (Étale Presheaf)**.** An *étale presheaf* on X is a contravariant functor P from $\text{Ét}(X)$ to the category of abelian groups.

Thus P associates to each étale morphism $f : Y \to X$ an abelian group $P(Y)$. Moreover, if $Y \to Y'$ is a morphism of objects in $\text{Ét}(X)$, there is a corresponding morphism of abelian groups $\text{res}_{Y,Y'} : P(Y') \to P(Y)$, which we think of as "restriction maps".

Example 24.9. Suppose G is a commutative group scheme over a scheme X. Define a functor on $\text{Ét}(X)$ by sending a scheme Y/X to the abelian group

$$G(Y) = \text{Hom}_{\text{Ét}(X)}(Y, G) \qquad \text{(scheme morphisms over } X\text{)}.$$

Then this functor is an étale presheaf. As a concrete example, we can take G to be the multiplicative group scheme $\mathbb{G}_m$, the additive group scheme $\mathbb{G}_a$, or the Néron model $\mathcal{A}$ over $X = \text{Spec}(R)$ of an abelian variety A over $\text{Spec}(K)$.

Definition 24.10 (Étale Sheaf)**.** An *étale sheaf* on X is a presheaf P such that for all covers $\{U_i \to U\}$ of all objects $U \in \text{Ét}(X)$, the sequence

$$P(U) \to \prod_i P(U_i) \to \prod_{i,j} P(U_i \times_U U_j)$$

is exact. Here, the first morphism sends a section $s \in P(U)$ to the sequence $(\text{res}_{U_i,U}(s))_i$. The second map sends $s_i \in P(U_i)$ to the tuple of differences

$$\text{res}_{U_i \times_U U_j, U_i}(s) - \text{res}_{U_i \times_U U_j, U_j}(s) \in P(U_i \times_U U_j)$$

Thus P is a sheaf if it is completely determined by its restriction to a covering, and any compatible family of sections on a covering arises from a global section.

Let S_X denote the category of all étale sheaves on X.

Theorem 24.11. *If G is a commutative group scheme over a scheme X (see Example 24.9 above) then the presheaf defined by G is in fact a sheaf for the étale site on X.*

Proof. See [Mil80, Cor. 1.7, page 52]. □

24.4 Direct and Inverse Image Functors

Suppose $\pi : X' \to X$ is a morphism of schemes. Then π induces a functor

$$\text{Ét}(X) \to \text{Ét}(X'),$$

that sends an étale morphism $Y \to X$ to its base change $Y \times_X X' \to X'$:

$$\begin{array}{ccc} Y \times_X X' & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X' & \longrightarrow & X \end{array}$$

Next we define the *direct image functor* π_p on presheaves. Given an étale presheaf P' on X' we obtain an étale presheaf $\pi_p(P')$ on X, which for $U \in \text{Ét}(X)$, is given by

$$(\pi_p(P'))(U) = P'(U_{X'}).$$

Here $U_{X'} = U \times_X X'$ is the fiber product, which is an étale cover of X':

$$\begin{array}{ccc} U_{X'} & \longrightarrow & U \\ \downarrow & & \downarrow \\ X' & \longrightarrow & X \end{array}$$

We continue to fix an étale morphism $f : X' \to X$. Given an étale presheaf P on X, the *inverse image functor* π^p associates to P an étale presheaf $P' = \pi^p(P)$ on X'. By abstract nonsense, the functor π^p is completely determined by the assertion that it is the adjoint of π_p, i.e.,

$$\text{Hom}(\pi^p(P), Q) \approx \text{Hom}(P, \pi_p(Q)),$$

where the homsets are in the categories of étale presheaves for X' and X, respectively. Explicitly, for $U' \in \text{Ét}(X')$

$$(\pi^p(P))(U') = \varinjlim_{U} P(U),$$

where the limit is over all commuting squares

$$\begin{array}{ccc} U' & \longrightarrow & U \\ \downarrow & & \downarrow \\ X' & \longrightarrow & X \end{array}$$

with $U \to X$ in $\text{Ét}(X)$. Note that these are merely commuting squares; we do not require that $U' = X' \times_X U$. (See [Mil80, pg. 57] for more details about the precise meaning of this direct limit, e.g., what the maps are.)

Proposition 24.12. *Both π_p and π^p are exact functors.*

Proof. See [Mil80, II.2.6, pg. 59]. □

24.5 Stalks

Let X be a scheme and $x \in X$ a point of the underlying topological space of X, so there is an affine open subset $U = \text{Spec}(A) \subset X$ such that x corresponds to a prime ideal $\mathfrak{p} \subset A$. The field associated to x is $k(x) = \text{Frac}(A/\mathfrak{p})$, and we let $\bar{x} = \text{Spec}(\bar{k})$, where $\bar{k}$ is a fixed choice of separable closure of $k(x)$. The inclusion $k(x) \hookrightarrow \bar{k}$ induces a scheme map

$$\bar{x} \xrightarrow{u_x} X.$$

The functor $F \mapsto F(\bar{x})$ is an equivalence of categories between the category of étale sheaves on $\bar{x}$ and the category of abelian groups.

Let P be an étale presheaf on X. The *stalk* of P at $\bar{x}$ is

$$P_{\bar{x}} = (u_x^p P)(\bar{x})$$

From the definition of u_x^p, we see that

$$(u_x^p P)(\bar{x}) = \varinjlim P(U)$$

where the limit is over all commutative triangles

$$\begin{array}{ccc} U & \longleftarrow & \bar{x} \\ \downarrow & \swarrow_{u_x} & \\ X & & \end{array}$$

with $U \in \text{Ét}(X)$. (Think of these as the "open sets U that contain x".)

The following proposition asserts that any question about an étale sheaf can be attacked by instead studying the stalks of the sheaf. This is why sheaves are much better to work with than presheaves.

Proposition 24.13. *Let F be an étale sheaf on X. Then for $U \in \text{Ét}(X)$, a section $s \in F(U)$ is completely determined by the stalks $s_{\bar{x}}$ of s at all points $\bar{x}$.*

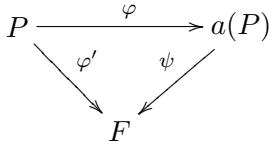
Proof. Suppose s, s' are two sections and $s_{\bar{x}} = (s')_{\bar{x}}$ for all $\bar{x}$. Then $(s-s')_{\bar{x}} = 0$ for all $\bar{x}$, so [Mil80, Prop. II.2.10, pg. 60] implies that $s - s' = 0$. The proof of Proposition II.2.10 in Milne is just an easy application of the definitions and sheaf property. □

The Galois group $G_{k(x)} = \mathrm{Gal}(\bar{k}/k(x))$ acts on the abelian group $P_{\bar{x}}$, so the stalk $P_{\bar{x}}$ is an element of a Galois module. In light of Proposition 24.13, sections of étale sheaves are thus "compatible" families of elements of all of the natural Galois modules attached to the points $x \in X$.

Example 24.14. Suppose $X = \mathrm{Spec}(R)$ with R a DVR with fraction field K and perfect residue field k. Then as a set $X = \{\mathfrak{p}, (0)\}$ has two points $x_p = \mathfrak{p}$ and $x_0 = (0)$. If P is an étale sheaf on X, then the stalks of P are $M = P_{\bar{x}_0}$ and $N = P_{\bar{x}_p}$, which are G_K and G_k-modules, respectively. This defines the M and N in the equivalence of categories between the category S_R of triples (M, N, φ) and the category of étale sheaves on X. The map φ then encodes the compatibility alluded to above; see Section 26.2 for precisely how φ is defined.

Using stalks one proves the following theorem (see [Mil80, Thm. II.2.11, pg. 61]) via a construction involving direct and inverse image functors to reduce to the case of stalks:

Theorem 24.15. *For any étale presheaf P on X, there is an étale sheaf $a(P)$ on X (called the étale* **sheafification** *of P) and a morphism $\varphi : P \to a(P)$ such that for any sheaf F and morphism $\varphi' : P \to F$ there is a unique map $\psi : a(P) \to F$ making the following diagram commute:*



24.6 Pullback and Pushforward of Étale Sheaves

Suppose $\pi : X' \to X$ is a morphism of schemes. If F' is an étale sheaf on X', then the *pushforward* of F' is the sheaf

$$\pi_*(F') = \pi_p(F'),$$

which is an étale sheaf on X. If F is an étale sheaf on X, then the *pullback* is the sheaf

$$\pi^*(F) = a(\pi^p(F)),$$

which is an étale sheaf on X'. These are adjoint functors, which means that in the appropriate categories of étale sheaves we have

$$\mathrm{Hom}(F, \pi_*(F')) \cong \mathrm{Hom}(\pi^*(F), F').$$

The functor π^* is exact and π_* is left exact. In general, π_* is *not* right exact (even though π_p is).

25 Étale Cohomology

Before defininining étale cohomology, we recall an import theorem. Recall that an object I in an abelian category $\mathcal{C}$ is *injective* if the contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-, I)$ is exact. Suppose that $\mathcal{C}$ has *enough injectives*, i.e., for every object X in $\mathcal{C}$ there is a monomorphims $X \to I$ for some injective I.

Theorem 25.1. *If $f : \mathcal{C} \to \mathcal{D}$ is any left exact functor, then there is an essentially unique collection of* right derived functors $R^i f : \mathcal{C} \to \mathcal{D}$ *such that*

(i) $R^0 f = f$,

(ii) $(R^i f)I = 0$ *if I is injective and $i \geq 1$,*

(iii) Long exact sequences: if $0 \to A \to B \to C \to 0$ is exact, then there is a long exact sequence

$$\cdots \to (R^i f)B \to (R^i f)C \xrightarrow{\delta} (R^{i+1} f)A \to (R^{i+1} f)B \to \cdots.$$

Theorem 25.2. *Let X be any scheme. The category of étale sheaves on X has enough injectives.*

Proof. The following proof is from [Mil80, §III.1]. Let $u_x : \bar{x} \to X$ be a geometric point of X. The category $S_{\bar{x}}$ of étale sheaves on $\bar{x}$ is isomorphic to the category **Ab** of abelian groups, so has enough injectives. Let $F \in S_X$ be an étale sheaf, and choose for each $x \in X$ an embedding $u_x^* F \hookrightarrow F'_x$ of $u_x^* F$ into an injective sheaf. Define

$$F^* = \prod_{x \in X} (u_x)_* u_x^* F$$

and

$$F^{**} = \prod_{x \in X} (u_x)_* F'_x.$$

Then the canonical maps $F \to F^*$ and $F^* \to F^{**}$ are both monomorphisms, and F^{**} is an injective object because products of injective objects are injective. □

Let X be a scheme and consider étale sheaves F on X. The global sections functor $S_X \to \mathbf{Ab}$

$$\Gamma(X, -) : F \mapsto F(X)$$

is left exact.

Definition 25.3 (Étale Cohomology)**.** The Étale cohomology groups $\mathrm{H}^i(X_{\text{ét}}, F)$ are the right derived functors of the global sections functor. Thus

$$\mathrm{H}^i(X_{\text{ét}}, -) = R^i\Gamma(X, -).$$

26 Galois Modules and Étale Sheaves

For essentially the rest of this course, we will only consider the the spectrums of DVR's and fields. For a scheme X, we continue to let S_X denote the category of étale sheaves on X. For a ring R we let S_R denote the category of Galois modules over R, which is a category of triples (M, N, φ) that we have only defined when R is a field or DVR (with perfect residue field).

26.1 The Spectrum of a Field

Let K be a field and $X = \mathrm{Spec}(K)$. Suppose $F \in S_X$ is an étale sheaf. If M/K is a finite separable extension, then $\mathrm{Spec}(M) \to X$ is an étale covering, and $F(\mathrm{Spec}(M))$ is defined. The only other étale coverings are of the form (disjoint union)

$$\coprod \mathrm{Spec}(M_i) \to \mathrm{Spec}(K),$$

which by the sheaf condition are completely determined by the groups $F(\mathrm{Spec}(M_i))$.

Define a functor $S_X \to S_K$ by associating to an (abelian) étale sheaf $F \in S_X$ the G_K-module

$$\varinjlim_{M/K} F(\mathrm{Spec}(M)),$$

where the limit is over all finite field extensions M of K contained in $\bar{K}$ (the separable closure).

Theorem 26.1. *The above functor is an equivalence of categories between* $S_{\mathrm{Spec}(K)}$ *and* S_K*.*

Proof. See [Mil80, Thm. 1.9, pg. 53] or [Maz73, Example 1, pg. 532] This can be proved by defining a functor in the other direction $S_K \to S_{\mathrm{Spec}(K)}$, and being careful about what happens with morphisms. □

Remark 26.2. The above functor $S_{\mathrm{Spec}(K)} \to S_K$ is just the functor that associates to a sheaf F its stalk at the point of $\mathrm{Spec}(K)$ (see Section 24.5).

26.2 The Spectrum of a DVR

In this section, we revisit and make more explicit Theorem 23.2, which we restate as follows. Recall that S_R denotes the category of triples (M, N, φ) where M is a G_K-module, N is a G_k-module and $\varphi : N \to M^0 = M^{I_v}$ is a G_k-module homomorphism (where I_v is the inertia group).

Let $X = \mathrm{Spec}(R)$ and consider the category S_X of étale sheaves on X. Define a functor $S_X \to S_R$ by

$$F \mapsto (M_F, N_F, \varphi_F),$$

as follows.

- **Define M_F:** The open immersion

  $$j : \mathrm{Spec}(K) \hookrightarrow X$$

  induces by pullback a functor $j^* : S_X \to S_{\mathrm{Spec}(K)}$. We describe this functor explicitly as follows. If $F \in S_X$ and L/K is a finite extension (with L contained in $\bar{K}$), then $j^*(F)(\mathrm{Spec}(L)) = F(\mathrm{Spec}(L))$, where $\mathrm{Spec}(L) \in \acute{\mathrm{E}}\mathrm{t}(X)$ via the composition

  $$\mathrm{Spec}(L) \to \mathrm{Spec}(K) \xrightarrow{j} X.$$

  We define M_F to be the G_K-module obtained by the composition of functors,

  $$S_X \xrightarrow{j^*} S_{\mathrm{Spec}(K)} \xrightarrow{\cong} S_K,$$

  where j^* is as above and and the functor $S_{\mathrm{Spec}(K)} \to S_K$ is the equivalence of categories from Theorem 26.1. Thus

  $$M_F = \varinjlim_{L/K \text{ as above}} F(\mathrm{Spec}(L)).$$

- **Define N_F:** Let

  $$N_F = \varinjlim_{L/K \text{ unramified}} F(\mathrm{Spec}(\mathcal{O}_L)),$$

where L runs through all finite extensions of K contained in K^{ur}, and $\mathcal{O}_L$ is the integral closure of R in L, i.e., the ring of integers of L. We regard N_F as a $G_k \cong \mathrm{Gal}(K^{\mathrm{ur}}/K)$-module since $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ acts naturally and compatibly on each group $F(\mathrm{Spec}(\mathcal{O}_L))$, since F is a functor.

- **Define φ_F:** The morphism φ_F is induced by the restriction maps on sheaves
$$F(\mathrm{Spec}(\mathcal{O}_L)) \to F(\mathrm{Spec}(L)),$$
which are induced by the inclusion $\mathrm{Spec}(L) \hookrightarrow \mathrm{Spec}(\mathcal{O}_L)$.

Remark 26.3. The Galois modules M_F and N_F can alternatively be defined using stalks (see Example 24.14).

Theorem 26.4. *The functor $F \mapsto (M_F, N_F, \varphi_F)$ is an equivalence of categories.*

Proof. See [Maz73, pg. 533], where Mazur in turn cites "the decomposition lemma". □

27 Étale Cohomology over a DVR

Our immediate goal is to master étale cohomology over a DVR, by understanding various exact sequences, some of which relate étale cohomology to Galois cohomology.

As usual, let R be a DVR with perfect residue field k and field of fractions K, and let $X = \mathrm{Spec}(R)$. Let $F \in S_R$ be a Galois module over R, which we can equivalently view as an étale sheaf in S_X by Theorem 26.4. Also, we continue to let

$$i : \mathrm{Spec}(k) \hookrightarrow X \qquad \text{and} \qquad j : \mathrm{Spec}(K) \to X$$

denote the natural closed embedding and open immersion, respectively, which induce many functors (see Section 23.4): $i^*, j^*, i_*, j_*, j_!, i^!$, the functors $i^*, i_*, j^*, j_!$ are exact, and j_* and $i^!$ are left exact.

Proposition 27.1. *We have an exact sequence of étale sheaves*

$$0 \to j_! j^* F \to F \to i_* i^* F \to 0. \tag{27.1}$$

Proof. View F as the triple (M, N, φ). Using the definitions of the functors in the sequence from Section 23.4, we see that the sequence in the statement of the proposition is:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & N & \longrightarrow & N & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle\varphi} & & \downarrow & & \\ 0 & \longrightarrow & M & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & 0. \end{array}$$

Since each row is exact, the claim follows. □

The long exact sequence associated to (27.1) is:

$$\cdots \to \mathrm{H}^r(R, j_! j^* F) \to \mathrm{H}^r(R, F) \to \mathrm{H}^r(R, i_* i^* F) \to \cdots \tag{27.2}$$

Thus it would be extremeley helpful if we could better understand both

$$\mathrm{H}^q(R, j_! j^* F) = \mathrm{H}^q(R, (M, 0, 0))$$

and

$$\mathrm{H}^q(R, i_* i^* F) = \mathrm{H}^q(R, (0, N, 0)).$$

You might hope that $\mathrm{H}^q(R, (M, 0, 0))$ is $\mathrm{H}^q(K, M)$ and $\mathrm{H}^q(R, (0, N, 0))$ is $\mathrm{H}^q(k, N)$, but this is *WRONG* in general. However, there are relationships, which we can make precise using *compact étale cohomology*.

Recall that

$$\mathrm{H}^q(R, F) = \mathrm{Ext}^q_{S_R}(\mathbb{Z}, F),$$

since

$$\mathrm{Hom}_{S_R}(\mathbb{Z}, F) = \mathrm{Hom}_{S_R}((\mathbb{Z}, \mathbb{Z}, \mathrm{id}), (M, N, \varphi)) = N^{G_k} = F(R) = \Gamma(X, F). \tag{27.3}$$

We use the above observation about how H^q is defined to motivate the introduction of "compact cohomology", which will help us to better understand the cohomology of $j_! j^* F$ and $i_* i^* F$. Note that if $\mathbb{Z}$ is the constant sheaf in S_k, then

$$i_* \mathbb{Z} = (0, \mathbb{Z}, 0).$$

Definition 27.2 (Compact Cohomology)**.** Define the *compact étale cohomology* groups by

$$\mathrm{H}^q_{\mathrm{comp}}(R, F) = \mathrm{Ext}^q_{S_R}(i_* \mathbb{Z}, F).$$

Because there is a long exact sequence of Ext groups, we have a long exact sequence of compact cohomology, etc. (i.e., the $\mathrm{H}^q_{\mathrm{comp}}(R, -)$ are derived functors). However, the best part is that there is a relative cohomology exact sequence.

Proposition 27.3. *Let $F \in S_R$ be any sheaf. Then we have an exact sequence*

$$\cdots \to \mathrm{H}^q_{\mathrm{comp}}(R, F) \to \mathrm{H}^q(R, F) \to \mathrm{H}^q(K, j^* F) \to \cdots$$

Proof. In this proof, we write $\mathrm{Ext} = \mathrm{Ext}_{S_R}$. We also let $\mathbb{Z}$ denote the constant sheaf in either S_k and S_R, with the context making which clear. By Proposition 27.1, we have an the exact sequence

$$0 \to j_! j^* \mathbb{Z} \to \mathbb{Z} \to i_* i^* \mathbb{Z} \to 0$$

in the category S_R. Apply the $\mathrm{Ext}^q(-, F)$ functor to this exact sequence, to obtain a long exact sequence

$$\cdots \to \mathrm{Ext}^q(i_* i^* \mathbb{Z}, F) \to \mathrm{Ext}^q(\mathbb{Z}, F) \to \mathrm{Ext}^q(j_! j^* \mathbb{Z}, F) \to \cdots$$

We have $i_* i^* \mathbb{Z} = i_* \mathbb{Z}$, so $\mathrm{Ext}^q(i_* i^* \mathbb{Z}, F) = \mathrm{H}^q_{\mathrm{comp}}(R, F)$, and of course by definition $\mathrm{Ext}^q(\mathbb{Z}, F) = \mathrm{H}^q(R, F)$.

It thus remains to show that

$$\mathrm{Ext}^q(j_! j^* \mathbb{Z}, F) \cong \mathrm{H}^q(K, j^* F). \tag{27.4}$$

Since $j_!j^*\mathbb{Z} = (\mathbb{Z}, 0, 0)$, we have

$$\begin{aligned}\mathrm{Hom}_{S_R}(j_!j^*\mathbb{Z}, F) &= \mathrm{Hom}_{S_R}((\mathbb{Z}, 0, 0), (M, N, \varphi)) \\ &\cong \mathrm{Hom}_{S_K}(\mathbb{Z}, M) = \mathrm{H}^0(K, M) \cong \mathrm{H}^0(K, j^*F).\end{aligned}$$

Also, recall that the functor j^* is exact (see, e.g., [Maz73, pg. 525] or just note that this is easy to see from the definition in terms of triples). The functor

$$F \to \mathrm{H}^q(K, j^*F)$$

is thus a delta functor (since j^* is exact and $\mathrm{H}^q(K, -)$ is a delta functor), and for $q = 0$ the above functor agrees with $\mathrm{Hom}_{S_R}(j_!j^*\mathbb{Z}, -)$. By uniqueness of derived functors we have compatible isomorphisms as in (27.4), *at least as long as we show that j^* sends injectives to acyclics!*, which we do in the next paragraph. In fact, we will show that if I is injective, then j^*I is also injective.

Claim: *j^* preserves injectives.* Suppose $I = (M, N, \varphi)$ is an injective element of S_R, so $\mathrm{Hom}_{S_R}(-, I)$ is exact. Suppose $0 \to M_0 \to M_1 \to M_2 \to 0$ is an exact sequence in S_K. Consider the exact sequence

$$0 \to j_!(M_0) \to j_!(M_1) \to j_!(M_2) \to 0.$$

Then the sequence

$$0 \to \mathrm{Hom}_{S_R}(j_!(M_2), I) \to \mathrm{Hom}_{S_R}(j_!(M_1), I) \to \mathrm{Hom}_{S_R}(j_!(M_0), I) \to 0$$

is exact (since I is injective). But for $a = 0, 1, 2$,

$$\mathrm{Hom}_{S_R}(j_!(M_a), I) = \mathrm{Hom}((M_a, 0, 0), (M, N, \varphi)) \cong \mathrm{Hom}_{S_K}(M_a, M) \cong \mathrm{Hom}_{S_R}(M_a, j^*I).$$

(In fact, we have just proved that $j_!$ and j^* are adjoint functors.) Thus

$$0 \to \mathrm{Hom}_{S_K}(M_2, I) \to \mathrm{Hom}_{S_K}(M_1, I) \to \mathrm{Hom}_{S_K}(M_0, I) \to 0$$

is exact, as required. □

We introduced $\mathrm{H}^q_{\mathrm{comp}}(R, F)$ because it is useful for computing the cohomology of certain sheaves in S_R. For example, it nails down shreaks:

Proposition 27.4. *For any G_K module M and any $q \geq 1$, we have*

$$\mathrm{H}^q_{\mathrm{comp}}(R, j_!M) \cong \mathrm{H}^{q-1}(K, M).$$

and

$$\mathrm{H}^q(R, j_!(M)) = 0.$$

Proof. If we take $F = j_!M$ in Proposition 27.3, then we see that the second assertion that for all $q \geq 0$, we have $\mathrm{H}^q(R, j_!M) = 0$, implies the first assertion about $\mathrm{H}^q_{\mathrm{comp}}$. First, we start with $q = 0$. We have $j_!M = (M, 0, 0)$, so as in (27.3),

$$\mathrm{H}^0(R, j_!M) = \Gamma(\mathrm{Spec}(R), (M, 0, 0)) = \mathrm{Hom}(\mathbb{Z}, (M, 0, 0)) = 0.$$

Recall that the functor $j_!$ is exact (as asserted in Section 23.4). As Mazur remarks on [Maz73, pg. 529], "one is tempted to use that $j_!$ is exact, and that $\mathrm{H}^0(R, j_!)$ is the zero functor. However, one must check that $j_!I$ is acyclic for cohomology over R, whenever I is injective". Thus, at this point, as in the proof of Proposition 27.3, it suffices to show that if $I \in S_K$ is injective, then $\mathrm{H}^q(R, j_!I) = 0$. To do this, consider the exact sequence in S_R:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & I^0 & \longrightarrow & I^0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \downarrow & & \\ 0 & \longrightarrow & I & \longrightarrow & I & \longrightarrow & 0 & \longrightarrow & 0, \end{array}$$

which we may alternatively write as

$$0 \to j_!I \to j_*I \to i_*i^*j_*I \to 0, \tag{27.5}$$

We first establish that this is an injective resolution of $j_!I$.

Claim: *j_* preserves injective.* Suppose $I \in S_K$ is injective and $0 \to F_0 \to F_1 \to F_2 \to 0$ is an exact sequence in S_R. The functor j^* is exact, so $0 \to j^*F_0 \to j^*F_1 \to j^*F_2 \to 0$ is an exact sequence in S_K. By our hypothesis that $I \in S_K$ is injective, the sequence

$$0 \to \mathrm{Hom}(j^*F_2, I) \to \mathrm{Hom}(j^*F_1, I) \to \mathrm{Hom}(j^*F_0, I) \to 0$$

is exact. Because j^* and j_* are adjoint, the sequence

$$0 \to \mathrm{Hom}(F_2, j_*I) \to \mathrm{Hom}(F_1, j_*I) \to \mathrm{Hom}(F_0, j_*I) \to 0$$

is exact. Thus j_*I is injective.

WARNING: In [Maz73, pg. 529] Mazur says in the proof that "the thing to check is that i^* preserves injectives". (See Remark 27.7 below.) Fortunately, something close enough is true:

Claim: *$i_*i^*j_*I$ is injective.* The claim is that the functor on S_R,

$$F \mapsto \mathrm{Hom}(F, i_*i^*j_*I)$$

is exact. Using that i_* and i^* are adjoint, and writing $F = (M, N, \varphi)$, we have

$$\mathrm{Hom}(F, i_* i^* j_* I) \cong \mathrm{Hom}(i^* F, i^* j_* I) \cong \mathrm{Hom}(N, I^0).$$

The functor i_* is exact, so it suffices to show that the functor

$$N \to \mathrm{Hom}(N, I^0)$$

on $G_k = G_v/I_v$-modules is exact, assuming I is an injective G_K-module and recalling that $I^0 = I^{I_v}$ is the submodule fixed by the inertia group. Suppose $0 \to N_0 \to N_1 \to N_2 \to 0$ is an exact sequence of G_v/I_v-modules. Viewing it as an exact sequence of G_v-modules, we see that

$$0 \to \mathrm{Hom}(N_2, I) \to \mathrm{Hom}(N_1, I) \to \mathrm{Hom}(N_0, I) \to 0 \tag{27.6}$$

is exact, since I is injective. However, since each N_i is fixed by I_v, the above homomorphisms all have image in I^0, i.e., $\mathrm{Hom}(N_a, I) \cong \mathrm{Hom}(N_a, I^0)$. Thus the sequence (27.6) with each I replaced by I^0 is exact in the category of G_k-modules, which proves the claim.

Finally, we compute $\mathrm{H}^q(R, j_! I)$ using (27.5). We have

$$\mathrm{H}^0(R, j_* I) = \mathrm{Hom}(\mathbb{Z}, (I, I^0, \mathrm{id})) = (I^0)^{G_k},$$

and

$$\mathrm{H}^0(R, i_* i^* j_* I) = \mathrm{Hom}(\mathbb{Z}, (0, I^0, 0)) = (I^0)^{G_k}.$$

Since $j_* I$ and $i_* i^* j_* I$ are injective, for $q \geq 1$ we have

$$\mathrm{H}^q(R, j_* I) = \mathrm{H}^q(R, i_* i^* j_* I) = 0.$$

The long exact sequence associated to (27.5), then implies that $\mathrm{H}^q(R, j_! I) = 0$ for $q \geq 0$. □

Proposition 27.5. *For any G_k-module N and all q, we have*

$$\mathrm{H}^q_{\mathrm{comp}}(R, i_* N) \cong \mathrm{H}^q(k, N).$$

Proof. Recall that the functor i_* is exact and is adjoint to the functor i^*, which is exact, so we have

$$\mathrm{Hom}(i^* X, Y) = \mathrm{Hom}(X, i_* Y),$$

hence i_* preserves injectives (this is exactly the same argument as in some of the claims above). Thus

$$\mathrm{H}^q_{\mathrm{comp}}(R, i_* N) = \mathrm{Ext}^q_{S_R}(i_* \mathbb{Z}, i_* N) = \mathrm{Ext}^q_{S_k}(\mathbb{Z}, N) = \mathrm{H}^q(k, N).$$

□

The following theorem "computes" étale cohomology over R in terms of Galois cohomology over k. Think of this theorem as saying "étale cohomology over a DVR is just unramified Galois cohomology."

Theorem 27.6. *Let $F = (M, N, \varphi) \in S_R$. Then for all $q \geq 0$, we have a functorial isomorphism*

$$\mathrm{H}^q(R, F) \cong \mathrm{H}^q(k, i^*F) = \mathrm{H}^q(k, N).$$

This isomorphism is induced by the natural map

$$\begin{aligned}\mathrm{H}^q(R, F) &\cong \mathrm{H}^q(R, i_*i^*F) \cong \mathrm{H}^q_{\mathrm{comp}}(R, i_*i^*F) \\ &= \mathrm{Ext}^q_{S_R}(i_*\mathbb{Z}, i_*i^*F) \cong \mathrm{Ext}^q_{S_k}(\mathbb{Z}, i^*F) = \mathrm{H}^q(k, i^*F),\end{aligned}$$

which we can alternatively write as

$$\begin{aligned}\mathrm{H}^q(R, (M, N, \varphi)) &\cong \mathrm{H}^q(R, (0, N, 0)) \cong \mathrm{H}^q_{\mathrm{comp}}(R, (0, N, 0)) \\ &= \mathrm{Ext}^q_{S_R}((0, \mathbb{Z}, 0), (0, N, 0)) \cong \mathrm{Ext}^q_{S_k}(\mathbb{Z}, N) = \mathrm{H}^q(k, N).\end{aligned}$$

Proof. Consider again the canonical exact sequence (27.1)

$$0 \to j_!j^*F \to F \to i_*i^*F \to 0.$$

By Proposition 27.4, we have $\mathrm{H}^q(R, j_!(j^*F)) = 0$ for all q, so

$$\mathrm{H}^q(R, F) \cong \mathrm{H}^q(R, i_*i^*F)$$

for all q. Now apply the relative cohomology exact sequence (Proposition 27.3) to the sheaf i_*i^*F, to obtain an exact sequence

$$\cdots \to \mathrm{H}^q_{\mathrm{comp}}(R, i_*i^*F) \to \mathrm{H}^q(R, i_*i^*F) \to \mathrm{H}^q(K, j^*i_*i^*F) \to \cdots$$

We have

$$j^*i_*i^*F = j^*i_*N = j^*(0, N, 0) = 0.$$

Thus for all q,

$$\mathrm{H}^q(R, i_*i^*F) \cong \mathrm{H}^q_{\mathrm{comp}}(R, i_*i^*F).$$

By Proposition 27.5, we have

$$\mathrm{H}^q_{\mathrm{comp}}(R, i_*i^*F) \cong \mathrm{H}^q(k, i^*F) = \mathrm{H}^q(k, N).$$

Thus combining the above we get that for all q,

$$\mathrm{H}^q(R, F) \cong \mathrm{H}^q(R, i_*i^*F) \cong \mathrm{H}^q_{\mathrm{comp}}(R, i_*i^*F) \cong \mathrm{H}^q(k, N),$$

as claimed. □

Remark 27.7. If i^* preserves injectives, then Theorem 27.6 would follow more easily, by comparing two δ functors. Maybe i^* does preserve injectives – Mazur sort of claims this on [Maz73, pg. 529]. Note that i_* is merely left adjoint to $i^!$, not i^*. Actually, if i^* were right adjoint to a functor, that functor would probably have to be something like $N \mapsto (N, N, \mathrm{id})$, where G_K acts on the second factor through the natural homomorphism $G_K \cong G_v \to G_v/I_v \cong G_k$. The functor $c : N \mapsto (N, N, \mathrm{id})$ does seem to be an exact functor from S_k to S_R, and it seems that

$$\mathrm{Hom}(c(A), B) = \mathrm{Hom}(A, i^*B),$$

which would show that i^* preserves injectives. This would thus also prove Theorem 27.6.

We have thus mastered étale cohomology over a DVR, at least assuming we know everything about Galois cohomology...

28 The Multiplicative Group over a DVR

Consider the element $\mathbb{G}_{m,R} \in S_R$ given by

$$U \hookrightarrow \bar{K}^*,$$

where U is the group of units in the ring of integers of K^{ur}, viewed as a $G_k = G_v/I_v$-module. To get a better sense for $\mathbb{G}_{m,R}$, note that we have an exact sequence in S_R:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \longrightarrow & (K^{\mathrm{ur}})^* & \xrightarrow{v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bar{K}^* & \longrightarrow & \bar{K}^* & \longrightarrow & 0 & \longrightarrow & 0, \end{array}$$

which we write as

$$0 \to \mathbb{G}_{m,R} \to j_*\mathbb{G}_{m,K} \to i_*\mathbb{Z} \to 0.$$

Theorem 28.1. *We have*

$$\mathrm{H}^q(R, \mathbb{G}_{m,R}) = \begin{cases} R^* & \text{if } q = 0 \\ 0 & \text{otherwise.} \end{cases}$$

We also have

$$\mathrm{H}^q_{\mathrm{comp}}(R, \mathbb{G}_{m,R}) = \begin{cases} 0 & \text{if } q = 0 \\ \mathbb{Z} & \text{if } q = 1 \\ 0 & \text{if } q = 2 \\ \mathbb{Q}/\mathbb{Z} & \text{if } q = 3 \\ 0 & \text{if } q \geq 4. \end{cases}$$

Proof. By Theorem 27.6, we have

$$\mathrm{H}^q(R, \mathbb{G}_{m,R}) \cong \mathrm{H}^q(k, U) = \mathrm{H}^q(K^{\mathrm{ur}}/K, U).$$

The computation of the Galois cohomology group $\mathrm{H}^q(k, U)$ then follows from local class field theory, using the exact sequence

$$0 \to U \to (K^{\mathrm{ur}})^* \xrightarrow{v} \mathbb{Z} \to 0, \tag{28.1}$$

For example, applying $G_k = \mathrm{Gal}(K^{\mathrm{ur}}/K)$-cohomology to the short exact sequence (28.1) we get

$$0 \to R^* \to K^* \twoheadrightarrow \mathbb{Z} \to \mathrm{H}^1(k, U) \to \mathrm{H}^1(K^{\mathrm{ur}}/K, (K^{ur})^*) = 0,$$

where we use that the valuation map $K^* \to \mathbb{Z}$ is surjective. Thus

$$\mathrm{H}^1(k, i^*\mathbb{G}_{m,R}) = \mathrm{H}^1(k, U) = 0.$$

The compact cohomology can similarly by computed by diagram chases. □

Note for comparison that

$$\mathrm{H}^q(k, \bar{k}^*) = \begin{cases} k^* & \text{if } q = 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathrm{H}^q(K, \bar{K}^*) = \begin{cases} K^* & \text{if } q = 0, \\ 0 & \text{if } q = 1, \\ \mathbb{Q}/\mathbb{Z} & \text{if } q = 2, \\ 0 & \text{if } q \geq 3. \end{cases}$$

29 Étale Cohomology of Abelian Varieties

Let A be an abelian variety over K. Recall that the Néron model $\mathcal{A}$ of A over R is a smooth commutative group scheme over the ring $\mathcal{O}_K$ of integer of K with generic fiber A such that for all smooth commutative group schemes S the natural map

$$\mathcal{A}(S) \to A(S_K)$$

is an isomorphism (this last statement is called the Néron mapping property).

In terms of sheaves, the Néron model is simply the pushforward of the sheaf in S_K defined by the abelian variety A:

Proposition 29.1. *We have $\mathcal{A} = j_*A$ as sheaves on the étale site over R.*

Proof. Suppose $U \in \text{Ét}(X)$ is an étale morphism. Then $U \to X$ is smooth, since étale is by definition "smooth of relative dimension 0." Then by definition (see Section 24.6),

$$(j_*A)(U) = A(U \times_X \operatorname{Spec}(K)) = A(U_K) \cong \mathcal{A}(U),$$

where we use the Néron mapping property. □

Thus the deep theorem that Néron models exists is really the theorem that the sheaf $j_*A \in S_R$ is *representable* by a smooth group scheme.

Proposition 29.2. *We have*

$$\mathrm{H}^1(R, \mathcal{A}) \cong \mathrm{H}^1(K^{\mathrm{ur}}/K, A(K^{\mathrm{ur}})).$$

Proof. By Theorem 27.6, we have

$$\mathrm{H}^1(R, \mathcal{A}) \cong \mathrm{H}^1(k, \mathcal{A}(R)) \cong \mathrm{H}^1(K^{\mathrm{ur}}/K, A(K^{\mathrm{ur}}))$$

by the Néron mapping property and identification of G_k and G_v/I_v. □

Taking special fibers, we have a canonical "connected-étale" exact sequence

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_A \to 0,$$

where Φ_A is the component group of $\mathcal{A}_k$. In fact, one can show that

$$\mathrm{H}^1(R, \mathcal{A}) \cong \mathrm{H}^1(k, \Phi_A),$$

which has the same order as $\Phi_A(k)$.

Next suppose A is an abelian variety over $\mathbb{Q}$ (say), Mazur does computations with $\mathrm{H}^1(\mathbb{Z}, \mathcal{A})$ in the appendix to *Rational Points on Abelian Varieties with values in Towers of Number Fields*. Let

$$\Sigma = \mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q}, A) \to \bigoplus_{p<\infty} \mathrm{H}^1(\mathbb{Q}_p, A)\right),$$

so Ш $\subset \Sigma$ and the quotient $\Sigma/$Ш is a 2-group. We have an exact sequence

$$0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi_A \to 0,$$

where Φ_A is the component group of $\mathcal{A}$ (at all primes at once).

Theorem 29.3 (Mazur)**.** *The natural map $i : \mathrm{H}^1(\mathbb{Z}, \mathcal{A}) \to \mathrm{H}^1(\mathbb{Q}, A)$ is an inclusion, and i sends the image of $\mathrm{H}^1(\mathbb{Z}, \mathcal{A}^0)$ isomorphically onto Σ.*

Thus we have a long exact sequence

$$0 \to \Sigma \to \mathrm{H}^1(\mathbb{Z}, \mathcal{A}) \to \mathrm{H}^1(\mathbb{Z}, \Phi_A) \to \mathrm{H}^2(\mathbb{Z}, \mathcal{A}^0) \to \dots$$

The upshot is that $\mathrm{H}^1(\mathbb{Z}, \mathcal{A})$ is basically Ш$(A/\mathbb{Q})$, up to a power of 2 and Tamagawa numbers. It is thus an object that combines Ш and something involving component groups.

References

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR MR0219512 (36 #2593)

[Maz73] Barry Mazur, *Notes on étale cohomology of number fields*, Ann. Sci. École Norm. Sup. (4) **6** (1973), 521–552 (1974). MR MR0344254 (49 #8993)

[Mil] J. S. Milne, *Lectures on Étale Cohomology*.

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

[Ser67] J-P. Serre, *Local class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 128–161.

[Ser97] ———, *Galois cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion and revised by the author.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.