QUICK INTRODUCTION TO GALOIS COHOMOLOGY

CALEB SPRINGER

These notes were written to quickly give a review of Galois cohomology for the Penn State Etale Cohomology reading group (Spring 2018). No attempt is made to be self-contained. Here are some better sources for this information:

• Cassels & Fröhlich, *Algebraic Number Theory*;
• Milne, *Class Field Theory* (lecture notes);
• Serre, *Galois Cohomology*;
• Tate, *Galois Cohomology* (lecture from Park City).

The following are great sources for applying Galois cohomology to elliptic curves. This includes Selmer groups and Tate-Shafarevich groups.

• Greenberg, *Introduction to the Iwasawa Theory of Elliptic Curves*;
• Silverman, *The Arithmetic of Elliptic Curves*.

Please let me know if you find an error, or have a suggestion.

1. Group modules

**Definition 1.1.** Let $G$ be a group and let $A$ be an abelian group. $A$ is defined to be a $G$-module if there is a map $G \times A \to A$ denoted $(g, a) \mapsto ga$ which satisfies the following for all $a, b \in A$ and $g, h \in G$.

1. $1 \cdot a = a$
2. $(gh)a = g(ha)$
3. $g(a + b) = ga + gb$

Equivalently, $A$ is a module (in the usual sense) over the group ring $\mathbb{Z}[G]$.

**Definition 1.2.** The set of homomorphisms of $G$-modules $M, N$ is the set of group homomorphisms $\alpha : M \to N$ satisfying $\alpha(gm) = ga(m)$ for all $g \in G$ and $m \in M$. Write $\text{Hom}_G(M, N)$ for this set, which is again a $G$-module.

**Definition 1.3.** We denote the $G$-invariants of $A$ by

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

and say that $G$ acts trivially on $A$ if $A^G = A$.

**Remark:** The functor $(-)^G : \text{Mod}_G \to \text{Ab}$ is left-exact. One may check this directly, or use the fact that it is isomorphic to $\text{Hom}_G(\mathbb{Z}, -)$, which is left-exact.

---

Date: April 18, 2018.
**Examples:** Let $K/k$ be a Galois field extension (not necessarily finite), and write $G = \text{Gal}(K/k)$.

<table>
<thead>
<tr>
<th>$A$</th>
<th>$A^G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(K, +)$</td>
<td>$(k, +)$</td>
</tr>
<tr>
<td>$(K^*, *)$</td>
<td>$(k^*, *)$</td>
</tr>
</tbody>
</table>

$E(K)$ for elliptic curve $E/k$

1.1. **Where we are going:** We will build group cohomology from the functor $(-)^G$. When $A$ is an algebraic group (e.g., the examples $\mathbb{G}_m$ or $E/k$ above), we use the notation $H^r(K/k, A) = H^r(\text{Gal}(K/k), A(K))$.

When $K = \overline{k}$, one often writes simply $H^r(k, A)$. The following are facts:

- $H^0(K/k, A) = A(k)$ (G-invariants)
- $H^1(K/k, \mathbb{G}_m) = H^1(K/k, k^*) = 0$ (Hilbert Theorem 90)
- $H^2(K/k, \mathbb{G}_m) = \text{Br}(K/k) \subseteq \text{Br}(k)$ (Brauer Group)

where $\text{Br}(k)$ is the Brauer group of $k$, which classifies the central simple algebras over $k$.

2. **Group cohomology**

There are multiple equivalent ways to do this section. I do not claim to cover everything, and (in particular) the method of computing cohomology groups from “standard chain complex” is not covered here. We mainly follow Milne in this section. In this section, $G$ is a group.

**Definition 2.1.** A $G$-module $I$ is injective if $\text{Hom}_G(\cdot, I)$ is exact, i.e. if $M_1 \subseteq M_2$ are $G$-modules then every $G$-homomorphism $M_1 \to I$ extends to $M_2 \to I$.

**Proposition 2.2.** The category $\text{Mod}_G$ has “enough injectives”, i.e. any $G$-module $M$ can be injected into some injective $G$-module $I$ as $M \hookrightarrow I$.

Recall that the functor $(-)^G$ is left exact. Now we can build group cohomology out of the theory of derived functors. Take a $G$-module $M$ and choose an injective resolution. (In the end, one may prove that this choice does not matter.)

$$0 \to M \to I^0 \to I^1 \to I^2 \to \ldots$$

This gives a complex

$$0 \xrightarrow{d^1} (I^0)^G \xrightarrow{d^0} (I^1)^G \to \ldots \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to \ldots$$

which is not necessarily exact.

**Definition 2.3.** The $r$-th cohomology group of $G$ with coefficients in $M$ is

$$H^r(G, M) = \frac{\ker d^r}{\text{im } d^{r-1}}.$$

**Facts**

1. $H^0(G, M) = M^G$.
2. If $I$ is injective, then $H^r(G, I) = 0$ for all $r > 0$.
3. Given any short exact sequence

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

there is a long exact sequence

$$0 \to H^0(G, M_1) \to \cdots \to H^r(G, M_1) \to H^r(G, M_2) \to H^r(G, M_3) \xrightarrow{\delta} H^{r+1}(G, M_1) \to \cdots$$

and this association is functorial.
(4) For a fixed group $G$, the preceding three facts uniquely characterize the family of functors $\{H^r(G, \cdot)\}_{r \geq 0}$.

2.1. Cohomology of profinite groups. Gruenberg’s Chapter V of Cassels-Fröhlich is also good to read for this section.

Recall that a profinite group $G$ is the inverse limit of finite groups. For example, the $p$-adic integers $\mathbb{Z}_p$ and Galois groups $\text{Gal}(L/K)$ are profinite groups. A profinite group $G$ has an induced topology and the following theorem gives the topological characterization of a profinite group.

**Theorem 2.4** (Theorem V.1, Cassels-Fröhlich). A topological group is profinite if and only if it is compact and totally disconnected.

**Corollary 2.5** (Corollary V.1, Cassels-Fröhlich). If $G$ is a profinite group, then $G \cong \lim \leftarrow G/U$ where the limit is over all open normal subgroups.

See Chapter V of Cassels-Fröhlich (or Milne’s notes) to learn more of the relevant basics of profinite groups and infinite Galois theory.

**Definition 2.6.** Define $A$ to be a discrete $G$-module if any of the following equivalent conditions hold.

1. $A = \bigcup A^U$ where the union is over all open normal subgroups of $G$.
2. The stabilizers of elements in $A$ are open subgroups of $G$.
3. The pairing $G \times A \rightarrow A$ is continuous when $A$ is viewed as a discrete space acted upon by the topological group $G$ (using the profinite topology).

**Definition 2.7.** Let $G$ be a profinite group and $A$ a discrete $G$ module. The $r$-th cohomology of $G$ in $A$ is

$$H^r(G, A) = \lim \rightarrow H^r(G/U_i, A^{U_i}).$$

An equivalent definition of the profinite cohomology is through “continuous cocycles”. The main point with either formulation is that the profinite topology and structure is being used in the cohomology, which gives the best theory.

3. Working simultaneously with different groups

The section draws mostly from Milne’s exposition.

**Definition 3.1.** Let $M_1$ and $M_2$ be $G_1$ and $G_2$ modules, respectively. Let $\alpha : G_2 \rightarrow G_1$ be a homomorphism of groups, and $\beta : M_1 \rightarrow M_2$ be a homomorphism of abelian groups. We say these homomorphisms are compatible if $\beta(\alpha(g)m) = g(\beta(m))$ for all $g \in G_2$ and $m \in M_1$. In other words, they are compatible if $\beta$ is a morphism of $G_2$-modules when one views $M_1$ as a $G_2$-module via $\alpha$.

**Remark:** Every pair $(\alpha, \beta)$ of compatible homomorphisms gives homomorphisms

$$H^r(G_1, M_1) \rightarrow H^r(G_2, M_2)$$

**Examples.**

1. Consider a subgroup $H \subseteq G$. Every $G$-module $M$ is also an $H$-module, where the action of $H$ is defined by the inclusion map $H \hookrightarrow G$. The map on cohomology is called restriction.

$$\text{Res} : H^r(G, M) \rightarrow H^r(H, M)$$
(2) There is also a way to move from $H$-modules to $G$-modules, called **induction**. Given an $H$-module $N$, the induced module$^1$ is defined as

$$\text{Ind}_H^G N = \{ \text{cts maps } \varphi : G \to N \mid \varphi(hg) = h\varphi(g) \ \forall h \in H \}$$

This is a $G$-module where the $G$-action is $g\varphi(x) = \varphi(xg)$. This induces a map of cohomology $H^r(G, \text{Ind}_H^G N) \to H^r(H, N)$. This is the isomorphism which is seen in Shapiro’s lemma below.

(3) When $H \subseteq G$ is a normal subgroup, there is a quotient map $G \to G/H$ and an inclusion map $M^H \hookrightarrow M$. This setup gives the **inflation** homomorphism

$$\text{Inf} : H^r(G/H, M^H) \to H^r(G, M)$$

Now we will take a deeper look at these constructions.

3.1. **Induction.**

**Lemma 3.2** (Milne CFT, II.1.2). $\text{Ind}_H^G : \text{Mod}_H \to \text{Mod}_G$ is an exact functor

**Proposition 3.3** (Shapiro’s Lemma, Milne’s CFT II.1.11). For any subgroup $H$ of $G$, any $H$-module $N$ and any $r \geq 0$, there is an isomorphism

$$H^r(G, \text{Ind}_H^G N) \cong H^r(H, N).$$

**Proof.** The main ingredient is the exactness of $\text{Ind}_H^G$. See Milne (or any other source) for more. \hfill \Box

This immediately gives the following corollary.

**Corollary 3.4.** If $M$ an induced $G$-module (i.e., $M = \text{Ind}_{\{1\}}^G M_0$ for an abelian group $M_0$), then $H^r(G, M) = 0$ for all $r > 0$.

3.2. **Inflation-Restriction.**

**Proposition 3.5** (The Inflation-Restriction Exact Sequence). Let $H$ be a normal subgroup of $G$ and let $M$ be a $G$-module. For any $r > 0$ such that $0 < i < r$, the following sequence is exact.

$$0 \to H^r(G/H, M^H) \xrightarrow{\text{Inf}} H^r(G, M) \xrightarrow{\text{Res}} H^r(H, M).$$

**Proof.** Use induction. \hfill \Box

4. **Cohomology for $L$ and $L^*$**

For this section, we will follow Chapter V.2.6-7 (Gruenberg) in Cassels-Fröhlich.

4.1. **Cohomology of $L$.** It turns out that the cohomology of $L$ as an additive group is not very exciting.

**Lemma 4.1.** If $L/K$ is a finite Galois extension, then $H^r(L/K, L) = H^r(\text{Gal}(L/K), L) = 0$ for all $r > 0$.

**Proof.** Write $G = \text{Gal}(L/K)$. The Normal Basis Theorem (from field theory) says there is an $\alpha \in L$ such that $\{\sigma \alpha\}_{\sigma \in G}$ is a basis for $L$ as a $K$-vector space, and this gives an isomorphism $K[G] \cong L$ of $G$-modules via $\sum a_\sigma \sigma \leftrightarrow \sum a_\sigma \sigma \alpha$.

But $K[G] = \text{Ind}_{\{1\}}^G K$. Thus the corollary to Shapiro’s lemma gives

$$H^r(G, L) \cong H^r(\{1\}, K) = 0$$

for $r > 0$. \hfill \Box

$^1$Sometimes called the “coinduced module”.


If you know about profinite groups, then you can extend the previous theorem.

**Corollary 4.2.** If $L/K$ is a (possibly infinite) Galois extension, then $H^r(L/K, L) = H^r(\text{Gal}(L/K), L) = 0$ for all $r > 0$.

**Proof.** Write $G = \text{Gal}(L/K)$ and let $\{K_i\}_{i \in I}$ be the set of all finite Galois extensions of $K$ contained in $L$. Set $U_i = \text{Gal}(L/K_i)$. Then infinite Galois theory tells us that $G = \varprojlim G/U_i$ and $L^{U_i} = K_i$. (See either Chapter V of Cassels-Fröhlich or Milne’s appendix I.A in his CFT notes if these ideas are foreign to you.)

\[
H^r(L/K, L) = \varprojlim H^r(G/U_i, L^{U_i}) = \varprojlim H^r(\text{Gal}(K_i/K), K_i).
\]

Now the statement follows immediately from the lemma, which says the groups on the right are all 0. □

4.2. **Cohomology of $L^*$.** The last section shows that the additive theory is not terribly exciting. But the groups $H^r(L/K, L^*)$ are more interesting. Only the first cohomology group is guaranteed to vanish, which is often referred to as “Hilbert Theorem 90”.

**Theorem 4.3 (Hilbert Theorem 90).** If $L/K$ is a (possibly infinite) Galois extension, then $H^1(L/K, L^*) = 0$.

**Proof.** Clever calculation with 1-cocycles. □

(1) The theorem above is an extension of the original Hilbert Theorem 90, which was the following: If $G = \text{Gal}(L/K)$ is a finite cyclic group generated by $g$ and $a \in L^*$ has $N_{L/K}a = 1$, then there is $b \in L^*$ such that $a = b/g(b)$.

(2) If you develop “non-abelian” group cohomology, then you can extend the theorem above farther:

\[
H^1(L/K, \text{GL}_n(L)) = 0.
\]

**Examples where one may apply Hilbert Theorem 90:**

- **Kummer Theory:** Studies the fields $K$ which contain all $n$-th roots of unity for some $n \geq 2$ which does not divide the characteristic of $K$.
  - Example: For such $K$, every cyclic extension $L/K$ of degree dividing $n$ is obtained by taking the $n$-th root of an element of $K$.

- **Artin-Schreier Theory:** Analogue to Kummer theory in the case where $n = p > 0$ is the characteristic of the field.

5. **Selmer groups and Tate-Shafarevich groups**

This section mainly draws from Silverman’s AEC, Chapter X.A. Greenberg in his “Introduction to Iwasawa Theory” takes a wider perspective that leads to a more general definition of a Selmer group, but this would take more time to discuss.

Let $E$ be an elliptic curve over a number field $K$. The Mordell-Weil Theorem says that the group $E(K)$ of $K$-rational points is a finitely generated abelian group. By the structure theorem for finitely generated abelian groups, $E(K) \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$.

Given a particular elliptic curve, it is typically not too hard to figure out the size of the torsion part (i.e. the $n_i$) by looking at reductions of $E$ to finite fields. The rank $r$ is a different story. In general, it is quite difficult to determine the rank of an elliptic curve, even over $\mathbb{Q}$. There are open conjectures around the behavior of ranks, and we will not take the digression of listing them.
Using heights and a descent procedure (Chapter VIII.3 in Silverman), the problem of computing the rank of $E(K)$ reduces to understanding $E(K)/mE(K)$. Since this reduction does not involve Galois cohomology, we will consider it a black box.

Let $E$ and $E'$ be elliptic curves over $K$ and let $\phi : E \to E'$ be an isogeny of elliptic curves defined over $K$. By definition, there is an exact sequence of $\text{Gal}(\overline{K}/K)$:

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

Using Galois cohomology, we get the following long exact sequence:

$$0 \to E(K)[\phi] \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E) \xrightarrow{\phi} H^1(K, E')$$

The first line above uses the fact that the 0-th cohomology group is the $\text{Gal}(\overline{K}/K)$-invariance, and a point is invariant under $\text{Gal}(\overline{K}/K)$ if and only if it is $K$-rational.

Now we have the “fundamental short exact sequence”

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E)[\phi] \to 0.$$

In the case where $E = E'$ and $\phi = m$, we find that the group $E(K)/mE(K)$ is conveniently injected into a cohomology group. Thus, studying the cohomology allows us to learn about $E(K)/mE(K)$, which in turn tells us about the rank of $E$ over $K$.

Additional information is gained by looking at every completion $v$ of $K$. The reason for the benefit is the following: It is easy to determine if a curve has a point defined over a complete local field via Hensel’s Lemma, but no such result exists over number fields. Running through the same arguments, we get the same short exact sequence over the completion $K_v$. We can put this information together:

$$0 \to \prod_v E'(K_v)/\phi(E(K_v)) \xrightarrow{\delta} \prod_v H^1(K_v, E[\phi]) \to \prod_v H^1(K_v, E)[\phi] \to 0$$

The vertical arrows come from using the restriction map and the natural inclusions $\text{Gal}(\overline{K}_v/K_v) \subseteq \text{Gal}(\overline{K}/K)$ and $E(\overline{K}) \subseteq E(K_v)$. Technically, these are dependent on the embedding $K \to \overline{K}_v$, but there is nothing to worry about after this embedding has been fixed once and for all.

**Definition 5.1.** Given an isogeny $\phi : E/K \to E'/K$, the $\phi$-Selmer group is the subgroup

$$S^{(\phi)}(E/K) = \ker \left\{ H^1(K, E[\phi]) \to \prod_v H^1(K_v, E) \right\}$$

The Shafarevich-Tate group of $E/K$ is the subgroup

$$\Sha(E/K) = \ker \left\{ H^1(K, E) \to \prod_v H^1(K_v, E) \right\}$$

**Remark:** Silverman identifies the groups $H^1(K, E)$ and $H^1(K_v, E)$ with Weil-Châtelet groups of equivalence classes of homogenous spaces, which we will not define or study here.

Here is the theorem that shows the usefulness of this construction.
Theorem 5.2. Given an isogeny $\phi : E/K \to E'/K$ of elliptic curves defined over $K$, there is an exact sequence.

$$0 \to E'(K)/\phi(E(K)) \to S^{(\phi)}(E/K) \to \text{III}(E/K)[\phi] \to 0$$

Moreover, the Selmer group $S^{(\phi)}(E/K)$ is finite.