April 25, 2009

LECTURE 1

Galois cohomology

We begin with a *very* quick and selective introduction to the facts from group cohomology and Galois cohomology that will be needed for the following lectures. For basic details see [**AW, Gr, Se2**], and for some of the more advanced results see [**Se1, Mi**]. For another quick overview see the lectures of Tate [**Ta3**] from PCMI 1999. We omit most proofs, although accessible ones are often given as exercises.

1.1. G-modules.

Suppose G is a group. A *G-module* is an abelian group A with an action of G on A that respects the group operation on A. That is, there is a map

$$G \times A \longrightarrow A$$

such that, if we let ga (or sometimes a^g) denote the image of (g, a) in A, then

$$(gh)a = g(ha), \qquad g(a + b) = ga + gb$$

for $g, h \in G$ and $a, b \in A$. Define the fixed subgroup

$$A^G = \{a \in A : ga = a \text{ for every } g \in G\}.$$

Example 1.1.1. If X is an abelian group we can view X as a G-module with trivial G action, and then $X^G = X$.

Example 1.1.2. If F/K is a Galois extension of fields and $G = \mathrm{Gal}(F/K)$, then F and $F^\times$ are G-modules. More generally, if $\mathcal{H}$ is an algebraic group defined over K, then the group of F-points $\mathcal{H}(F)$ is a G-module and $\mathcal{H}(F)^G = \mathcal{H}(K)$.

Example 1.1.3. If A and B are G-modules and $\varphi : A \to B$ is a group homomorphism, we define a new group homomorphism $g\varphi$ for $g \in G$ by $(g\varphi)(a) = g(\varphi(g^{-1}a))$. This makes $\mathrm{Hom}(A, B)$ into a G-module, and $\mathrm{Hom}(A, B)^G$ is the group of G-module homomorphisms from A to B.

We say that a G module A is *co-induced* if $A \cong \mathrm{Hom}(\mathbf{Z}[G], X)$ for some abelian group X.

Exercise 1.1.4. Suppose A is a G-module, and A_0 is the G-module whose underlying abelian group is A, but whose G action is trivial. Show that the map $a \mapsto \varphi_a$, where $\varphi_a(g) = g^{-1}a$, is an injection from A to the co-induced module $\mathrm{Hom}(\mathbf{Z}[G], A_0)$.

1.2. Characterization of the cohomology groups.

For this section suppose that the group G is finite. For every G-module A, there are abelian (cohomology) groups $H^i(G, A)$ for $i \geq 0$. For an explicit definition using cocycles and coboundaries, see [**AW, Se2**]. We will omit the definition, and just make use of the following properties.

Theorem 1.2.1. *There is a unique collection of functors $H^i(G, \cdot)$ from G-modules to abelian groups, for $i \geq 0$, satisfying the following properties:*

(1) *$H^0(G, A) = A^G$ for every G-module A.*
(2) *If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then there is a (functorial) long exact sequence*

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \to H^1(G,A) \to H^1(G,B) \to \cdots$$
$$\cdots \to H^i(G,A) \to H^i(G,B) \to H^i(G,C) \to H^{i+1}(G,A) \to \cdots$$

(3) *If A is co-induced, then $H^i(G, A) = 0$ for all $i \geq 1$.*

Exercise 1.2.2. Show that the three properties above determine the cohomology groups $H^i(G, A)$ uniquely (assuming they exist). Hint: use induction and the fact (Exercise 1.1.4) that for every G-module A there is a short exact sequence $0 \to A \to B \to C \to 0$ with B co-induced.

In these lectures we will only make use of $H^i(G, A)$ for $i \leq 2$ (and mostly $i \leq 1$). When $i = 0$ the groups are described explicitly by condition (1) of Theorem 1.2.1; when $i = 1$ we have the following explicit description.

Define $C^1(G, A)$ (the 1-cochains) to be the group of (set) maps from G to A. Define subgroups of cocycles and coboundaries $B^1(G, A) \subset Z^1(G, A) \subset C^1(G, A)$ by

$$Z^1(G,A) = \{f \in C^1(G,A) : f(gh) = f(g) + g(f(h))\}$$
$$B^1(G,A) = \{f \in C^1(G,A) : \text{for some } a \in A,\ f(g) = ga - a \text{ for every } g \in G\}.$$

Proposition 1.2.3. $H^1(G, A) = Z^1(G, A)/B^1(G, A)$.

There is a similar definition of $H^i(G, A)$ for every i, where the cochains $C^i(G, A)$ (are) set maps from G^i to A, and $B^i(G, A) \subset Z^i(G, A) \subset C^i(G, A)$ are defined appropriately.

Example 1.2.4. Suppose that G acts trivially on A. Then $Z^1(G, A) = \mathrm{Hom}(G, A)$ and $B^1(G, A) = 0$, so in this case we conclude from Proposition 1.2.3 that

$$H^1(G,A) = \mathrm{Hom}(G,A).$$

Exercise 1.2.5. Suppose that G is a finite cyclic group. For every G-module A, let $A_N := \{a \in A : \sum_{g \in G} ga = 0\}$ (here "N" stands for "norm"; A_N is the kernel of the norm map $a \mapsto \sum_{g \in G} ga$).

Show that if g is a generator of G, then the map $f \mapsto f(g)$ is an injective homomorphism from $Z^1(G, A)$ to A with image A_N. Deduce that in this case

$$H^1(G,A) \cong A_N/(g-1)A.$$

(Warning: note that this isomorphism depends on the choice of generator g.)

Exercise 1.2.6. Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, and suppose $c \in C^G$. Fix an element $b \in B$ that maps to c.

Show that the map $g \mapsto gb - b$ defines a 1-cocycle $f_c \in Z^1(G, A)$ (that depends on the choice of b). Show that $c \mapsto f_c$ induces a well-defined homomorphism $H^0(G, C) \to H^1(G, A)$ and check that with this homomorphism, the beginning of the long exact sequence of Theorem 1.2.1(2) is in fact exact.

1.3. Continuous cohomology.

Now suppose that G is a *profinite group* (see for example [**Gr**]), i.e., there is an isomorphism

$$G = \varprojlim G/U \tag{1.1}$$

where U runs over open subgroups of G of finite index. This isomorphism gives G natural topology, where we view each finite quotient G/U as a discrete topological space, so the product $\prod(G/U)$ is a compact group with the product topology, and then (1.1) identifies G with a closed (and hence compact) subset of $\prod(G/U)$.

Note that a finite group G is profinite, with the discrete topology.

If A is a G-module, we will view A as a topological group with the discrete topology, and we call A a continuous G-module if the action of G on A (i.e., the map $G \times A \to A$) is continuous.

Exercise 1.3.1. Suppose A is a G-module. Show that the following are equivalent:

(1) A is a continuous G-module,
(2) for every $a \in A$, the stabilizer of a in G is open,
(3) $A = \cup A^U$, union over open subgroups $U \subset G$.

Example 1.3.2. If F/K is an infinite Galois extension of fields, and we put $G := \mathrm{Gal}(F/K)$, then there is a natural isomorphism

$$G = \varprojlim \mathrm{Gal}(L/K)$$

inverse limit over finite Galois extensions L of K in F. Thus G is a profinite group.

If $\mathcal{H}$ is an algebraic group over K as in Example 1.1.2, then

$$\mathcal{H}(F) = \cup \mathcal{H}(L) = \cup \mathcal{H}(F)^{\mathrm{Gal}(L/K)},$$

union over finite extensions L of K in F. Therefore G acts continuously on $\mathcal{H}(F)$ by Exercise 1.3.1.

It follows (for example) that when $F = K^{\mathrm{sep}}$ is a separable closure of K, the following G-modules are continuous: K^{sep}, $(K^{\mathrm{sep}})^\times$, $\boldsymbol{\mu}_{p^\infty}$ (the p-power roots of unity in K^{sep}), $E(K^{\mathrm{sep}})$ for an elliptic curve E, and $E[p^\infty]$ (the p-power torsion in $E(K^{\mathrm{sep}})$).

If A is a continuous G-module, we can define *continuous* cohomology groups $H^i(G, A)$, defined similarly to the case of finite groups G but with *continuous* cochains (that is, $C^i(G, A)$ consists of continuous maps from G^i to A). Theorem 1.2.1(1) and (2) also hold for continuous cohomology groups.

If G is finite, then all relevant maps are continuous and the continuous cohomology groups agree with the cohomology groups described in §1.2.

In the next section we will see (Proposition 1.4.7) how to describe the continuous cohomology groups in terms of the cohomology of finite groups.

Until further notice we will always assume that the group G is profinite, and G-module will mean continuous G-module, a discrete abelian group with a continuous action of G.

1.4. Change of group.

Suppose H is a closed subgroup of a profinite group G, and A is a G-module. Then A is an H-module, and $A^G \subset A^H$. For every i there is a restriction map on cochains

$\mathrm{Res} : C^i(G,A) \to C^i(H,A)$, and these maps induce *restriction maps*

$$\mathrm{Res} : H^i(G,A) \to H^i(H,A).$$

If $[G : H]$ is finite, then there is also a norm map $A^H \to A^G$, defined by $a \mapsto \sum_g ga$, summing over a set of left coset representatives of G/H. This map extends in a less obvious way to a *corestriction map*

$$\mathrm{Cor} : H^i(H,A) \to H^i(G,A)$$

for every i.

Proposition 1.4.1. *If $[G : H]$ is finite, then* $\mathrm{Cor} \circ \mathrm{Res} : H^i(G,A) \to H^i(G,A)$ *is multiplication by $[G : H]$.*

Corollary 1.4.2. *If G is finite, then for every G-module A and every $i \geq 1$, we have*

$$|G| \cdot H^i(G,A) = 0.$$

Proof. Take $H = \{1\}$ in Proposition 1.4.1. □

Exercise 1.4.3. Suppose $m \in \mathbf{Z}$. Show that if $mA = 0$, then $mH^i(G,A) = 0$ for every i. Show that if $m : A \to A$ is an isomorphism, then $mH^i(G,A) = H^i(G,A)$ for every i. Deduce that if $|G| : A \to A$ is an isomorphism, then $H^i(G,A) = 0$.

Exercise 1.4.4. Suppose G is finite. Using Exercise 1.1.4, show that for $i \geq 1$, $H^i(G,A)$ can be expressed in terms of $H^{i-1}(G,C)$ for some G-module C. Use this fact, the norm map on H^0, and induction to define the corestriction map on H^i.

Using this definition, prove Proposition 1.4.1.

Now suppose that H is a closed normal subgroup of G. Then A^H is a G/H-module, and for every i there is an inflation map on cochains $\mathrm{Inf} : C^i(G/H, A^H) \to C^i(G,A)$. These maps induce *inflation maps*

$$\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G,A).$$

Theorem 1.4.5. *If H is a normal subgroup of G and A is a G-module, then there is an natural exact sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A)^{G/H} \to H^2(G/H, A^H) \to H^2(G,A).$$

Corollary 1.4.6. *Suppose H acts trivially on A, and*

$$H^1(G/H, A) = H^2(G/H, A) = 0.$$

Then $H^1(G,A) \cong \mathrm{Hom}(H,A)^{G/H}$.

Proposition 1.4.7. *If A is a G-module, then*

$$H^i(G,A) = \varinjlim H^i(G/U, A^U)$$

direct limit over open subgroups $U \subset G$, with respect to the inflation maps.

Exercise 1.4.8. Prove Proposition 1.4.7 when $i = 1$, using the description (Proposition 1.2.3) of $H^1(G,A)$ in terms of cocycles.

Exercise 1.4.9. Use Proposition 1.4.7 to show that if A is a G-module, then $H^i(G,A)$ is a torsion group for $i \geq 1$.

Proposition 1.4.10. *Suppose $G \cong \hat{\mathbf{Z}} := \varprojlim \mathbf{Z}/n\mathbf{Z}$, and A is a torsion G-module.*

(1) *If γ is a topological generator of G, then evaluation of cocycles at γ induces an isomorphism $H^1(G, A) \cong A/(\gamma - 1)A$.*
(2) *$H^i(G, A) = 0$ for $i \geq 2$.*

Proof. See [**Se2**, §XIII.1]. Assertion (1) is the following exercise. □

Exercise 1.4.11. Prove Proposition 1.4.10(1) using Exercise 1.2.5 and Proposition 1.4.7.

From now on, if F/K is a Galois extension and A is a $\mathrm{Gal}(F/K)$-module, we will write $H^i(F/K, A)$ in place of $H^i(\mathrm{Gal}(F/K), A)$, and when F is a separable closure K^{sep} of K we write simply $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $H^i(K, A)$ in place of $H^i(K^{\mathrm{sep}}/K, A) = H^i(G_K, A)$.

Definition 1.4.12. Suppose K is a nonarchimedean local field K of characteristic zero, i.e., a finite extension of some $\mathbf{Q}_p$. Let $I_K \subset G_K$ denote the inertia group, $K^{\mathrm{ur}} = \bar{K}^{I_K}$ the maximal unramified extension of K, and $\varphi \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ the Frobenius automorphism. Then $\mathrm{Gal}(K^{\mathrm{ur}}/K) = G_K/I_K \cong \hat{\mathbf{Z}}$, generated by φ.

If A is a G_K-module, define the *unramified cohomology group* $H^1_{\mathrm{u}}(K, A) \subset H^1(K, A)$ by

$$H^1_{\mathrm{u}}(K, A) := \ker\bigl[H^1(K, A) \xrightarrow{\mathrm{Res}} H^1(K^{\mathrm{ur}}, A)\bigr].$$

The inflation-restriction exact sequence (Theorem 1.4.5) shows that

$$H^1_{\mathrm{u}}(K, A) = H^1(K^{\mathrm{ur}}/K, A^{I_K}). \tag{1.2}$$

If A is a G_K-module, we will say that A is *unramified* if I_K acts trivially on A.

Proposition 1.4.13. *If A is a finite unramified G_K-module, then:*

(1) *$H^1_{\mathrm{u}}(K, A) = H^1(K^{\mathrm{ur}}/K, A) = A/(\varphi - 1)A$,*
(2) *$H^1(K, A)/H^1_{\mathrm{u}}(K, A) \cong \mathrm{Hom}(I_K, A)^{G_K}$.*

Proof. This follows from Theorem 1.4.5 and Proposition 1.4.10. □

1.5. Selmer groups.

Suppose for this section that K is a number field, and A is a G_K-module. For every place v of K, we can view the decomposition group G_{K_v} as a subgroup of G_K, so we have restriction maps

$$\mathrm{Res}_v : H^i(K, A) \longrightarrow H^i(K_v, A).$$

Definition 1.5.1. A *Selmer structure* $\mathcal{F}$ for A is a collection of distinguished subgroups

$$H^1_{\mathcal{F}}(K_v, A) \subset H^1(K_v, A)$$

for every place v of K, such that $H^1_{\mathcal{F}}(K_v, A) = H^1_{\mathrm{u}}(K_v, A)$ for all but finitely many v.

If $\mathcal{F}$ is a Selmer structure for A, we define the *Selmer group* $H^1_{\mathcal{F}}(K, A)$ by

$$H^1_{\mathcal{F}}(K, A) = \ker\bigl[H^1(K, A) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v (H^1(K_v, A)/H^1_{\mathcal{F}}(K_v, A))\bigr].$$

In other words, $H^1_{\mathcal{F}}(K, A)$ is the subgroup of all classes in $H^1(K, A)$ whose localization lies in $H^1_{\mathcal{F}}(K_v, A)$ for every v.

Exercise 1.5.2. Suppose $\mathcal{F}$ is a Selmer structure, and suppose Σ is a finite set of places of K containing all archimedean places, all places where A is ramified, and all v such that $H^1_{\mathcal{F}}(K_v, A) \neq H^1_{\mathrm{u}}(K_v, A)$. Let K_Σ be the maximal extension of K unramified outside of Σ. Show that

$$H^1_{\mathcal{F}}(K, A) = \ker\Big[H^1(K_\Sigma/K, A) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_{v\in\Sigma} (H^1(K_v, A)/H^1_{\mathcal{F}}(K_v, A))\Big]$$

Proposition 1.5.3. *If A is finite and $\mathcal{F}$ is a Selmer structure for A, then $H^1_{\mathcal{F}}(K, A)$ is finite.*

Proof. With notation as in Exercise 1.5.2, a standard result (for example [**Mi**, Corollary I.4.15]) shows that $H^1(K_\Sigma/K, A)$ is finite. Thus $H^1_{\mathcal{F}}(K, A)$ is finite by Exercise 1.5.2. □

In what follows, Selmer groups will be arithmetically interesting objects (ideal class groups, Selmer groups of elliptic curves, ...) and their orders should be related to values of L-functions. We will see examples of Selmer groups in the next section.

Exercise 1.5.4. If B is a G_K-quotient of A, show that a Selmer structure $\mathcal{F}$ for A induces a Selmer structure for B (which we also denote by $\mathcal{F}$), where we define $H^1_{\mathcal{F}}(K_v, B)$ to be the image of $H^1_{\mathcal{F}}(K_v, A)$ under the canonical map $H^1(K_v, A) \to H^1(K_v, B)$.

Similarly, show that if C is a G_K-submodule of A, show that a Selmer structure $\mathcal{F}$ for A induces one for C, where $H^1_{\mathcal{F}}(K_v, C)$ is defined to be the inverse image of $H^1_{\mathcal{F}}(K_v, A)$ under the canonical map $H^1(K_v, C) \to H^1(K_v, A)$.

1.6. Kummer theory.

Proposition 1.6.1. *Suppose F/K is a Galois extension. Then*

$$H^i(F/K, F) = \begin{cases} K & \text{if } i = 0 \\ 0 & \text{if } i > 0, \end{cases} \qquad H^i(F/K, F^\times) = \begin{cases} K^\times & \text{if } i = 0 \\ 0 & \text{if } i = 1. \end{cases}$$

Exercise 1.6.2. Use Proposition 1.4.7 to reduce the proof of Proposition 1.6.1 to the case where F/K is finite.

Theorem 1.6.3. *For every $m > 0$ prime to the characteristic of K, there is a natural isomorphism*

$$K^\times/(K^\times)^m \cong H^1(K, \boldsymbol{\mu}_m).$$

Proof. The long exact cohomology sequence coming from the short exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_m \longrightarrow (K^{\mathrm{sep}})^\times \xrightarrow{m} (K^{\mathrm{sep}})^\times \longrightarrow 0$$

begins

$$0 \longrightarrow \boldsymbol{\mu}_m(K) \longrightarrow K^\times \xrightarrow{m} K^\times \longrightarrow H^1(K, \boldsymbol{\mu}_m) \longrightarrow H^1(K, (K^{\mathrm{sep}})^\times).$$

Now the theorem follows from Proposition 1.6.1. □

Exercise 1.6.4. Show using the description from Exercise 1.2.6 that the isomorphism of Theorem 1.6.3 is given by sending $x \in K^\times$ to the cocycle $g \mapsto g(\sqrt[m]{x})/\sqrt[m]{x}$ for $g \in G_K$.

Corollary 1.6.5. *If $\boldsymbol{\mu}_m \subset K$ then $K^\times/(K^\times)^m \cong \mathrm{Hom}(G_K, \boldsymbol{\mu}_m)$.*

Exercise 1.6.6. Suppose $\boldsymbol{\mu}_m \subset K$ and X is a finite subgroup of $K^\times/(K^\times)^m$. Show that the isomorphism of Corollary 1.6.5 identifies

$$X \cong \mathrm{Hom}(\mathrm{Gal}(K(\sqrt[m]{X})/K), \boldsymbol{\mu}_m),$$

where $K(\sqrt[m]{X})$ is the extension of K generated by m-th roots of all elements of X. Show that the isomorphism of Corollary 1.6.5 induces a bijection between finite subgroups of $K^\times/(K^\times)^m$ and finite abelian extensions of K of exponent dividing m.

Definition 1.6.7. If K is a nonarchimedean local field of characteristic zero, define

$$H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \subset H^1(K, \boldsymbol{\mu}_m)$$

to be the image under the Kummer map of Theorem 1.6.3

$$\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m \hookrightarrow K^\times/(K^\times)^m \cong H^1(K, \boldsymbol{\mu}_m)$$

where $\mathcal{O}_K$ is the ring of integers of K. If K is $\mathbf{R}$ or $\mathbf{C}$, let $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) = H^1(K, \boldsymbol{\mu}_m)$.

Exercise 1.6.8. Show that if K is a number field, then the collection of subgroups $\{H^1_{\mathrm{f}}(K_v, \boldsymbol{\mu}_m)\}$ is a Selmer structure (i.e., show that $H^1_{\mathrm{f}}(K_v, \boldsymbol{\mu}_m) = H^1_{\mathrm{u}}(K_v, \boldsymbol{\mu}_m)$ for all $v \nmid m\infty$).

Proposition 1.6.9. *The Selmer group $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m)$ defined with the Selmer structure above satisfies*

$$0 \longrightarrow \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m \longrightarrow H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \longrightarrow \mathcal{C}_K[m] \longrightarrow 0$$

where $\mathcal{C}_K[m]$ is the m-torsion subgroup of the ideal class group of K.

Exercise 1.6.10. Prove Proposition 1.6.9 as follows. Viewing $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \subset K^\times/(K^\times)^m$, show that if $x \in K^\times$ projects to an element of $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m)$, then the fractional principal ideal $x\mathcal{O}_K$ is $\mathfrak{a}^m$ for some fractional ideal $\mathfrak{a}$. Show that sending x to the class of $\mathfrak{a}$ induces a surjective map $H^1_{\mathrm{f}}(K, \boldsymbol{\mu}_m) \twoheadrightarrow \mathcal{C}_K[m]$ with kernel $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m$.

Theorem 1.6.3 has the following analogue for elliptic curves.

Theorem 1.6.11. *Suppose E is an elliptic curve defined over K and $m > 0$ is prime to the characteristic of K. There is an exact sequence*

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1(K, E[m]) \longrightarrow H^1(K, E(K^{\mathrm{sep}}))[m] \longrightarrow 0.$$

Exercise 1.6.12. Prove Theorem 1.6.11 using the short exact sequence

$$0 \longrightarrow E[m] \longrightarrow E(K^{\mathrm{sep}}) \xrightarrow{\ m\ } E(K^{\mathrm{sep}}) \longrightarrow 0.$$

Show that the injection $E(K)/mE(K) \hookrightarrow H^1(K, E[m])$ is given by sending $x \in E(K)$ to the cocycle $g \mapsto gy - y$, where $y \in E(K^{\mathrm{sep}})$ satisfies $my = x$ (and the same y is used for all g).

Definition 1.6.13. If K is a nonarchimedean local field of characteristic zero, E is an elliptic curve over K, and $m > 0$, define

$$H^1_{\mathrm{f}}(K, E[m]) \subset H^1(K, E[m])$$

to be the image of the Kummer map of Theorem 1.6.11

$$E(K)/mE(K) \hookrightarrow H^1(K, E[m]).$$

If K is $\mathbf{R}$ or $\mathbf{C}$, let $H^1_{\mathrm{f}}(K, E[m]) = H^1(K, E[m])$.

Suppose now that K is a number field and E is an elliptic curve over K. If $v \nmid m\infty$ and E has good reduction at v, then $H^1_{\mathrm{f}}(K_v, E[m]) = H^1_{\mathrm{u}}(K_v, E[m])$ by [**Ca**], so the collection of subgroups $\{H^1_{\mathrm{f}}(K_v, E[m])\}$ is a Selmer structure. The corresponding Selmer group is the classical m-Selmer group of E/K, sitting in an exact sequence

$$0 \longrightarrow E(K)/mE(K) \longrightarrow H^1_{\mathrm{f}}(K, E[m]) \longrightarrow Ш(E/K)[m] \longrightarrow 0$$

where $Ш(E/K)$ is the Shafarevich-Tate group of E/K.

1.7. The Brauer group.

If K is a field, $\boldsymbol{\mu}_\infty$ will denote the roots of unity in K^{sep}.

Exercise 1.7.1. Suppose K is a field. Show that for every $m > 0$ prime to the characteristic of K, there is a natural isomorphism $H^2(K, \boldsymbol{\mu}_m) \cong H^2(K, (K^{\mathrm{sep}})^\times)[m]$. Deduce that if K has characteristic zero, then $H^2(K, \boldsymbol{\mu}_\infty) \cong H^2(K, (K^{\mathrm{sep}})^\times)$.

Theorem 1.7.2. *If K is a nonarchimedean local field of characteristic zero (i.e., a finite extension of some $\mathbf{Q}_p$), then there is a canonical isomorphism*

$$\mathrm{inv}_K : H^2(K, \boldsymbol{\mu}_\infty) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

If $K = \mathbf{R}$, there is a canonical isomorphism

$$\mathrm{inv}_{\mathbf{R}} : H^2(\mathbf{R}, \boldsymbol{\mu}_\infty) \xrightarrow{\sim} \tfrac{1}{2}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}.$$

Proof. See [**Se2**, §XIII.3]. □

Theorem 1.7.3. *Suppose K is a number field. For every $m \leq \infty$ there is an exact sequence*

$$0 \longrightarrow H^2(K, \boldsymbol{\mu}_m) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^2(K_v, \boldsymbol{\mu}_m) \xrightarrow{\sum \mathrm{inv}_{K_v}} \mathbf{Q}/\mathbf{Z} \longrightarrow 0$$

where K_v is the completion of K at v, and Res_v is the restriction map with respect to the subgroup $G_{K_v} \subset G_K$.

Proof. See [**AT**, Chapter 7, Theorem 8]. □

1.8. Local fields and duality.

Suppose A and B are G-modules. There is a cup product homomorphism

$$H^i(G, A) \otimes H^j(G, B) \longrightarrow H^{i+j}(G, A \otimes B).$$

We view this as a bilinear pairing on $H^i(G, A) \times H^j(G, B)$, written $(a, b) \mapsto a \cup b$. The cup product pairing has numerous properties [**AW, Se2**]; here we mention only that it commutes with restriction maps: if $H \subset G$, then $\mathrm{Res}(a) \cup \mathrm{Res}(b) = \mathrm{Res}(a \cup b)$.

Suppose now that K is a field, A is a finite G_K module, and $\boldsymbol{\mu}_\infty$ is the G_K-module of roots of unity in K^{sep}. Define the Cartier dual $A^* = \mathrm{Hom}(A, \boldsymbol{\mu}_\infty)$. Then A^* is also a (continuous) G_K-module, and there is a natural pairing

$$A \otimes A^* \longrightarrow \boldsymbol{\mu}_\infty.$$

We can compose the cup product with this pairing to get a pairing

$$H^i(K, A) \otimes H^j(K, A^*) \longrightarrow H^{i+j}(K, \boldsymbol{\mu}_\infty). \tag{1.3}$$

If K is a local field of characteristic zero, and $i+j=2$, we can compose the pairing (1.3) with the isomorphism of Proposition 1.7.2 to get a new pairing

$$H^i(K,A)\times H^j(K,A^*) \xrightarrow{\cup} H^2(K,\boldsymbol{\mu}_\infty) \xrightarrow{\mathrm{inv}_K} \mathbf{Q}/\mathbf{Z}. \tag{1.4}$$

Theorem 1.8.1 (Tate local duality)**.** *Suppose K is a local field of characteristic zero, A is a finite G_K-module, and $0\le i\le 2$. Then* (1.4) *is a perfect pairing of finite groups.*

Proof. See [**Mi**, Corollary I.2.3]. □

In the following examples and exercise, K is a local field of characteristic zero and $\mathcal{O}_K$ is its ring of integers.

Example 1.8.2. Fix $m\ge 0$, and let $A=\boldsymbol{\mu}_m$. Then $A^*=\mathbf{Z}/m\mathbf{Z}$ (with trivial G_K-action), and we have

$$H^1(K,\boldsymbol{\mu}_m)\cong K^\times/(K^\times)^m,\quad H^1(K,\mathbf{Z}/m\mathbf{Z})=\mathrm{Hom}(G_K,\mathbf{Z}/m\mathbf{Z}).$$

By Theorem 1.8.1, the pairing (1.4) gives an isomorphism (for every m)

$$\begin{aligned}K^\times/(K^\times)^m \xrightarrow{\sim} H^1(K,\boldsymbol{\mu}_m) &\xrightarrow{\sim} \mathrm{Hom}(H^1(K,\mathbf{Z}/m\mathbf{Z}),\mathbf{Q}/\mathbf{Z})\\ &\xrightarrow{\sim} \mathrm{Hom}(\mathrm{Hom}(G_K,\mathbf{Z}/m\mathbf{Z}),\mathbf{Q}/\mathbf{Z}) \xrightarrow{\sim} G_K^{\mathrm{ab}}/(G_K^{\mathrm{ab}})^m.\end{aligned}$$

The inverse limit of these maps over m gives the Artin map $K^\times\to G_K^{\mathrm{ab}}$ of local class field theory.

Exercise 1.8.3. Recall that $H^1_{\mathrm{f}}(K,\boldsymbol{\mu}_m)\subset H^1(K,\boldsymbol{\mu}_m)$ is the image of the Kummer map $\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^m\hookrightarrow H^1(K,\boldsymbol{\mu}_m)$. Define

$$H^1_{\mathrm{f}}(K,\mathbf{Z}/m\mathbf{Z}):=H^1_{\mathrm{u}}(K,\mathbf{Z}/m\mathbf{Z})=\mathrm{Hom}(G_K/I_K,\mathbf{Z}/m\mathbf{Z})\subset H^1(K,\mathbf{Z}/m\mathbf{Z}),$$

where $I_K\subset G_K$ is the inertia group. Show, using the local class field theory description of the isomorphism in Example 1.8.2, that $H^1_{\mathrm{f}}(K,\boldsymbol{\mu}_m)$ and $H^1_{\mathrm{f}}(K,\mathbf{Z}/m\mathbf{Z})$ are orthogonal complements of each other under the Tate pairing

$$H^1(K,\boldsymbol{\mu}_m)\times H^1(K,\mathbf{Z}/m\mathbf{Z})\to\mathbf{Q}/\mathbf{Z}.$$

Example 1.8.4. Suppose E is an elliptic curve over K, $m>0$, and $A=E[m]$. The Weil pairing $E[m]\times E[m]\to\boldsymbol{\mu}_m$ gives a canonical isomorphism $A^*\cong E[m]$. By Theorem 1.8.1, the pairing (1.4) gives a perfect pairing

$$H^1(K,E[m])\times H^1(K,E[m])\longrightarrow\mathbf{Z}/m\mathbf{Z}.$$

The subgroup $H^1_{\mathrm{f}}(K,E[m])\subset H^1(K,E[m])$ given by Definition 1.6.13 is its own orthogonal complement under this pairing [**Ta1**].

1.9. Unramified and transverse cohomology groups.

Fix for this section a nonarchimedean local field K of characteristic zero, and let $\mathcal{O}_K$ be its ring of integers. As in Definition 1.4.12, we let $I_K\subset G_K$ denote the inertia group, $K^{\mathrm{ur}}=\bar{K}^{I_K}$ the maximal unramified extension of K, and $\varphi\in\mathrm{Gal}(K^{\mathrm{ur}}/K)$ the Frobenius automorphism. Then $\mathrm{Gal}(K^{\mathrm{ur}}/K)=G_K/I_K\cong\hat{\mathbf{Z}}$, generated by φ. Recall that a G_K-module A is *unramified* if I_K acts trivially on A.

Proposition 1.9.1. *Suppose A is a finite unramified G_K-module of order prime to the residue characteristic of K. Then $H^1_{\mathrm{u}}(K,A)$ and $H^1_{\mathrm{u}}(K,A^*)$ are orthogonal complements of each other under the pairing* (1.4).

PROOF. See for example [**Mi**, Theorem I.2.6], or combine the following two exercises. □

Exercise 1.9.2. Show using Proposition 1.4.13 that if A is a finite unramified G_K-module of order prime to the residue characteristic of K, then

$$|H^1_{\mathrm{u}}(K,A)| = [H^1(K,A^*) : H^1_{\mathrm{u}}(K,A^*)].$$

You will need to use that the tame quotient of I_K is isomorphic (as a G_K-module) to $\prod_{\ell\neq p} \boldsymbol{\mu}_{\ell^\infty}$, where p is the residue characteristic of K.

Exercise 1.9.3. Assuming that the cup product commutes with inflation, show that $H^1_{\mathrm{u}}(K,A)$ and $H^1_{\mathrm{u}}(K,A^*)$ are orthogonal because the following diagram commutes:

$$\begin{array}{ccc} H^1(K,A)\times H^1(K,A^*) & \xrightarrow{\cup} & H^2(K,\boldsymbol{\mu}_\infty) \\ \uparrow{\scriptstyle \mathrm{Inf}} & & \uparrow{\scriptstyle \mathrm{Inf}} \\ H^1_{\mathrm{u}}(K,A)\times H^1_{\mathrm{u}}(K,A^*) & \xrightarrow{\cup} & H^2(K^{\mathrm{ur}}/K,\boldsymbol{\mu}_\infty) \end{array}$$

and the lower right corner is zero by Proposition 1.4.10(2).

Let $\Bbbk$ denote the residue field of K, and $q := |\Bbbk|$.

Definition 1.9.4. Suppose L/K is a totally tamely ramified extension of degree $q-1$; then there is a canonical isomorphism $\mathrm{Gal}(L/K) \cong \Bbbk^\times$. (When $K = \mathbf{Q}_\ell$ we can take $L = \mathbf{Q}_\ell(\boldsymbol{\mu}_\ell)$.) We define the L-transverse subgroup $H^1_{\mathrm{t}}(K,A) \subset H^1(K,A)$ by

$$H^1_{\mathrm{t}}(K,A) := \ker\big[H^1(K,A) \to H^1(L,A)\big] = H^1(L/K, A^{G_L}).$$

Proposition 1.9.5. *Suppose A is a finite unramified G_K-module and $(q-1)A = 0$. Then:*

1. $H^1_{\mathrm{t}}(K,A) \cong \mathrm{Hom}(\mathrm{Gal}(L/K), A^{\varphi=1})$.
2. $H^1_{\mathrm{t}}(K,A) \otimes \mathrm{Gal}(L/K) \cong A^{\varphi=1}$.
3. *There is a direct sum decomposition* $H^1(K,A) = H^1_{\mathrm{u}}(K,A) \oplus H^1_{\mathrm{t}}(K,A)$.
4. $H^1_{\mathrm{t}}(K,A)$ *and* $H^1_{\mathrm{t}}(K,A^*)$ *are orthogonal complements of each other under the pairing* (1.4).

PROOF. See [**MR1**, Lemmas 1.2.1, 1.2.4 and Proposition 1.3.2]. Since A is unramified and I_K and G_L generate G_K, we have $A^{G_L} = A^{G_K} = A^{\varphi=1}$. This proves (1) and (2). By (1) and Proposition 1.4.13(2), $|H^1(K,A)| = |H^1_{\mathrm{u}}(K,A)|\cdot|H^1_{\mathrm{t}}(K,A)|$, so to prove (3) it is enough to show that $H^1_{\mathrm{u}}(K,A) \cap H^1_{\mathrm{t}}(K,A) = 0$, and then to prove (4) it is enough to show that $H^1_{\mathrm{t}}(K,A)$ and $H^1_{\mathrm{t}}(K,A^*)$ are orthogonal. These are left as an exercises, or see [**MR1**]. □

Definition 1.9.6. Suppose $m \mid q-1$, and let $R = \mathbf{Z}/m\mathbf{Z}$. Suppose that A is an unramified G-module that is free of finite rank over R, and that $\det(1-\varphi|A) = 0$. Consider the characteristic polynomial

$$P(x) := \det(1-\varphi x|A) \in R[x].$$

Since $P(1) = \det(1-\varphi|A) = 0$, we have $P(x) = (x-1)Q(x)$ for some $Q(x) \in R[x]$. By the Cayley-Hamilton theorem, $P(\varphi^{-1})$ annihilates A, so $Q(\varphi^{-1}) \subset A^{\varphi=1}$. Define the *unramified-transverse comparison map* ϕ^{ut} to be the composition

$$H^1_{\mathrm{u}}(K,A) \xrightarrow{\sim} A/(\varphi-1)A \xrightarrow{Q(\varphi^{-1})} A^{\varphi=1} \xrightarrow{\sim} H^1_{\mathrm{t}}(K,A)\otimes\mathrm{Gal}(L/K)$$

using the isomorphisms of Proposition 1.4.13(1) and 1.9.5(2).

Exercise 1.9.7 (Lemma 1.2.3 of [**MR1**])**.** Suppose $m \mid q-1$ and A is an unramified G-module that is free of finite rank over $\mathbf{Z}/m\mathbf{Z}$. Show that $A^{\varphi=1}$ is free of rank one over $\mathbf{Z}/m\mathbf{Z}$ if and only if $A/(\varphi-1)A$ is free of rank one over $\mathbf{Z}/m\mathbf{Z}$. If these conditions are satisfied, show that the map ϕ^{ut} of Definition 1.9.6 is an isomorphism and $H^1_{\mathrm{u}}(K,A)$, $H^1_{\mathrm{t}}(K,A)$, $H^1_{\mathrm{u}}(K,A^*)$, $H^1_{\mathrm{t}}(K,A^*)$, are all free of rank 1 over $\mathbf{Z}/m\mathbf{Z}$.

1.10. Comparing Selmer groups.

Suppose K is a number field and A is a finite G_K-module.

Definition 1.10.1. If $\mathcal{F}$ is a Selmer structure for A, define a Selmer structure $\mathcal{F}^*$ for the Cartier dual $A^* := \mathrm{Hom}(A, \boldsymbol{\mu}_\infty)$ by

$$H^1_{\mathcal{F}^*}(K_v, A^*) := H^1_{\mathcal{F}}(K_v, A)^\perp \subset H^1(K_v, A^*)$$

for every v, where $H^1_{\mathcal{F}}(K_v,A)^\perp$ is the orthogonal complement of $H^1_{\mathcal{F}}(K_v,A)$ in $H^1(K_v,A^*)$ under the local Tate pairing (1.4). By Proposition 1.9.1, $\mathcal{F}^*$ is a Selmer structure.

If $\mathcal{F},\mathcal{G}$ are Selmer structures for A, we will say $\mathcal{G} \subset \mathcal{F}$ if $H^1_{\mathcal{G}}(K_v,A) \subset H^1_{\mathcal{F}}(K_v,A)$ for every v. Note that if $\mathcal{G} \subset \mathcal{F}$, then

- $H^1_{\mathcal{G}}(K,A) \subset H^1_{\mathcal{F}}(K,A)$,
- $\mathcal{F}^* \subset \mathcal{G}^*$.

Theorem 1.10.2 (Global duality)**.** *Suppose $\mathcal{G}_1, \mathcal{G}_2$ are Selmer structures for A, and $\mathcal{G}_1 \subset \mathcal{G}_2$. There are exact sequences*

$$0 \longrightarrow H^1_{\mathcal{G}_1}(K,A) \longrightarrow H^1_{\mathcal{G}_2}(K,A) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^1_{\mathcal{G}_2}(K_v,A)/H^1_{\mathcal{G}_1}(K_v,A),$$

$$0 \longrightarrow H^1_{\mathcal{G}_2^*}(K,A^*) \longrightarrow H^1_{\mathcal{G}_1^*}(K,A^*) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^1_{\mathcal{G}_1^*}(K_v,A^*)/H^1_{\mathcal{G}_2^*}(K_v,A^*),$$

summing over v such that $H^1_{\mathcal{G}_1}(K_v,A) \neq H^1_{\mathcal{G}_2}(K_v,A)$. The images of the two right-hand maps are orthogonal complements of each other under the sum of the local Tate pairings (1.4)*.*

Proof. See [**Ru**, Theorem 1.7.3] to derive this statement from the usual statement of Poitou-Tate duality ([**Ta2**, Theorem 3.1] or [**Mi**, Theorem I.4.10]). □

Exercise 1.10.3. Show that the two sequences of Theorem 1.10.2 are exact. Show that the images of the two right-hand maps are orthogonal, using Theorem 1.7.3.

The following corollary of Theorem 1.10.2 will be used to bound the size of $H^1_{\mathcal{F}}(K,A)$. Note that given $\mathcal{F}$, there will exist $\mathcal{G} \subset \mathcal{F}$ "small enough" that $H^1_{\mathcal{G}}(K,A) = 0$.

Corollary 1.10.4. *Suppose $\mathcal{G} \subset \mathcal{F}$ are Selmer structures for A, and $H^1_{\mathcal{G}}(K,A) = 0$. Then*

$$|H^1_{\mathcal{F}}(K,A)| \le \Big|\mathrm{coker}\big[H^1_{\mathcal{G}^*}(K,A^*) \xrightarrow{\oplus \mathrm{Res}_v} \bigoplus_v H^1_{\mathcal{G}^*}(K_v,A^*)/H^1_{\mathcal{F}^*}(K_v,A^*)\big]\Big|.$$

Exercise 1.10.5. Prove Corollary 1.10.4.