Lecture Notes from Differential Geometry (Michaelmas 2021)

Isaac Martin

Last compiled March 11, 2022

Contents

§ *Lecture 1*

Recorded: 2022-03-09 Notes: 2022-03-09

Corollary 0.1. If $E[n] \subseteq K(K)$ then $\mu_n \subseteq K$, where μ_n is the set of nth roots of unity in $\overline{K}$.

> *Proof:* If e_n is nondegenerate then there exist $S,T \in E[n]$ such that $e_n(S,T)$ is a primitive n^{th} root of unit, say ζ_n. Then $\sigma(\zeta_n) = e_n(\sigma S, \sigma T) = e_n(S,T) = \zeta_n$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The first equality follows from Galois equivalence and the second since $S,T \in E(K)$. Therefore $\zeta_n \in K$. $\square$

Example 0.2. There exists no $E/\mathbb{Q}$ such that $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Remark 0.3. In fact, the Weil pairing is alternating, i.e. $e_n(T,T) = 1$ for all $T \in E[n]$. In particular, expanding $e_n(S+T,S+T)$ show $e_n(S,T) = e_n(T,S)^{-1}$.

1 Galois Cohomology

Throughout this section, G is a group and A is a G-module, i.e. and abelian group with an action of G via group homomorphisms. That is, we have a map $G \to \mathrm{Aut}(A)$ where $\mathrm{Aut}(A)$ is the group of abelian group homomorphisms of A, and $g \cdot a = g(a)$. To say that A is a G=module is equivalent to saying that A is a $\mathbb{Z}[G]$-module.

Definition 1.1. We set

$$H^0(G,A) = A^G = \{a \in A \mid \sigma(a) = a,\ \forall \sigma \in G\}.$$

We further set

$$\begin{aligned}
C^1(G,A) &= \{\text{maps } G \longrightarrow A\} && \text{“cochains”}\\
Z^1(G,A) &= \{(a_\sigma)_{\sigma\in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\} && \text{“}\textit{cocycles}\text{''}\\
B^1(G,A) &= \{(\sigma b - b)_{\sigma \in G} \mid b \in A\} && \text{“coboundaries”}
\end{aligned}$$

and we have inclusions $B^1(G,A) \subseteq Z^1(G,A) \subseteq C^1(G,A)$. We define $H^1(G,A) = Z^1(G,A)/B^1(G,A)$.

Remark 1.2. If G acts trivially on A, then $H^1(G,A) = \mathrm{Hom}(G,A)$.

Theorem 1.3. *A short exact sequence of G-modules*

$$0 \longrightarrow A \xrightarrow{\phi} B \xrightarrow{\psi} C \longrightarrow 0$$

gives rise to a long exact sequence of abelian groups

$$0 \longrightarrow A^G \xrightarrow[\phi]{} B^G \xrightarrow[\psi]{} C^G \xrightarrow[\delta]{} H^1(G,A) \xrightarrow[\phi_*]{} H^1(G,B) \xrightarrow[\psi_*]{} H^1(G,C) \longrightarrow \ldots$$

where we stop before $H^2(G,A)$ because we have yet to define it. The map δ arises from the snake lemma.

Definition 1.4. Let $c \in C^G$. Then there exists a $b \in B$ such that $\psi(b) = c$. Then

$$\psi(\sigma b - b) = \sigma(c) - c = 0$$

for all $\sigma \in G$. This means $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. One checks that $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$. We define $\delta(c) =$ chars of $(a_\sigma)_{\sigma \in G}$ in $H^1(G,A)$.

Theorem 1.5. *Let A be a G-module $H \subseteq G$ a normal subgroup. Then there is an inflation-restriction exact sequence*

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

Proof: Omitted. □

Let K be a perfect field. $\mathrm{Gal}(\overline{K}/K)$ is then a topological group with basis of open subgroups. The sets $\mathrm{Gal}(\overline{K}/L)$ for $[L:K] < \infty$.

If $G = \mathrm{Gal}(\overline{K}/K)$ then we modify the definition of $H^1(G,A)$ by insisting

1. The stabilizer of each $a \in A$ is an open subgroup of G.
2. All cochains $G \longrightarrow A$ are continuous where A is given by the discrete topology.

Then

$$H^1(\mathrm{Gal}(\overline{K}/K), A) = \varinjlim_{L,\ L/K \text{finite Galois}} H^1(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\overline{K}/L)}).$$

The direct limit is with respect to inflation maps (what are inflation maps?).

Theorem 1.6 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension. Then $H^1(\mathrm{Gal}(L/K), L^*) = 0$.*

Proof: Let $G = \mathrm{Gal}(L/K)$. Let $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^*)$. Distinct automorphisms are linearly independent, hence there exists some $y \in L$ such that

$$\underbrace{\sum_{\tau \in G} a_\tau^{-1} \tau(y)}_{x} \neq 0.$$

For $\sigma \in G$,

$$\sigma(x) = \sum_{\tau \in G} \sigma(a_\tau)^{-1} \sigma\tau(y) = a_\sigma \sum_{\tau \in G} a_\sigma^{-1} \sigma\tau(y) = a_\sigma \cdot x.$$

Therefore $a_\sigma = \sigma(x)/x \implies (a_\sigma)_{\sigma \in G} \in B^1(G, L^*)$. Hence $H^1(G, L^*)$. □

Corollary 1.7. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$.

Application: Assume $\mathrm{char}\, K \not| n$. There is an exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow[x \longmapsto x^n]{} \overline{K}^* \longrightarrow 0.$$

Have a long exact sequence

$$K^* \xrightarrow[x \mapsto x^n]{} K^* \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*),$$

but $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$ by Theorem (1.6). Therefore $H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If $\mu_n \subseteq K$ then $\mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n$.

If L/K is a finite Galois extension then $\mathrm{Gal}(\overline{K}/K) \xrightarrow{\pi} \mathrm{Gal}(L/K)$ and hence

$$\mathrm{Hom}(\mathrm{Gal}(L,K), \mu_n) \hookrightarrow \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n,$$

where the above map is given by $\chi \mapsto \chi \circ \pi$. The image is a finite subgroup $\Delta \subseteq K^*/(K^*)^n$.

If $\mathrm{Gal}(L/K)$ is abelian of exponent dividing n then

$$[L:K] = |\mathrm{Gal}(L/K)| = |\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)| = |\Delta|.$$

Compare to Theorem 11.2 from lectures Fix numbering.

Notation: We'll write $H^1(K, -) = H^1(\mathrm{Gal}(\overline{K}/K), -)$ to avoid writing Gal and $\overline{K}$ every time.

Lemma 1.8. Let $[K : \mathbb{Q}_p] < \infty$. Then

$$\ker(H^1(K, \mu_n) \longrightarrow H^1(K^{nr}, \mu_n)) \subseteq \{x \in K^*/(K^*) \mid v(x) \equiv 0 \pmod n\}.$$

remember that K^{nr} is the maximal unramified extension of K.

Proof: By Theorem (1.6), identify H^1 $\square$

§ *Lecture 2*

Recorded: 2022-03-11   Notes: 2022-03-11

Lemma 1.9. Let $K:\mathbb{Q}_p] < \infty$. Then

$$\ker(H^1(K,\mu_n) \longrightarrow H^1(K^{nr},\mu_n)) \subseteq \{x \in K^*/(K^*)^n \mid v(x) \equiv 0 \pmod n\}$$

Proof: (Continued). The discrete valuation $v : K^* \to \mathbb{Z}$ extends to $v : (K^{nr)^* \to \mathbb{Z}})$. Then $v(x) = nv(y) \equiv 0 \pmod n$. □

EXERCISE: (in local fields.) Show that if $p \nmid n$ then $\subseteq$ is actually $=$.

Let $\phi : E \longrightarrow E'$ be an isogeny of elliptic curves over K. Then there is a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \overset{\phi}{\longrightarrow}\!\!\!\!\rightarrow E' \longrightarrow 0.$$

Long-exact sequence:

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K,E[\phi]) \longrightarrow H^1(K,E) \xrightarrow{\phi_*} H^1(K,E').$$

We get a short exact sequence

$$0 \longrightarrow \frac{E'(K)}{\phi E(K)} \longrightarrow H^1(K,E[\phi]) \longrightarrow H^1(K,E)[\phi*] \longrightarrow 0.$$

Now take K to be a number field. For each place v fix an embedding $\overline{K} \subseteq \overline{K}_v$. Then $\mathrm{Gal}(\overline{K}_v/K_v) \subseteq \mathrm{Gal}(\overline{K}/K)$. This gives us a short exact sequence resembling the one above:

$$0 \longrightarrow \prod_v \frac{E'(K_v)}{\phi E(K_v)} \longrightarrow \prod_v H^1(K_v,E[\phi]) \longrightarrow \prod_v H^1(K_v,E)[\phi*] \longrightarrow 0.$$

These products just mean that we have an exact sequence

$$0 \longrightarrow \frac{E'(K_v)}{\phi E(K_v)} \longrightarrow H^1(K_v,E[\phi]) \longrightarrow H^1(K_v,E)[\phi*] \longrightarrow 0$$

for each place v. We also have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi E(K)} \arrow[r, "\delta"] \arrow[d] & H^1(K,E[\phi]) \arrow[r] \arrow[d, "res_v"] \arrow[dr] & H^1(K,E)[\phi*] \arrow[r] \arrow[d, "res_v"] & 0 \\
0 \arrow[r] & \prod_v \frac{E'(K_v)}{\phi E(K_v)} \arrow[r] & \prod_v H^1(K_v,E[\phi]) \arrow[r] & \prod_v H^1(K_v,E)[\phi*] \arrow[r] & 0.
\end{tikzcd}$$

This leads us to the definition of the *Selma group*.

Definition 1.10. The ϕ-Selma group is

$$\begin{aligned}
S^{(\phi)}(E/K) &= \ker(\text{downward diagonal map above}) \\
&= \ker\left(H^1(K,E[\phi]) \longrightarrow \prod_v H^1(K_v,E)\right) \\
&= \{\alpha \in H^1(K,E[\phi]) \mid \mathrm{res}_v(\alpha) \in \mathrm{img}(\delta_v)\ \forall v\}.
\end{aligned}$$

The *Tate Shaferevich group is*

$$\text{look at picture and fill in}, weird disjoint union looking symbol with three vertical strokes.$$

We get a short-exact sequence

$$0 \longrightarrow \frac{E'(K)}{\phi E(K)} \longrightarrow S^{(\phi)}(E/K) \longrightarrow (E/K)[\phi_*] \longrightarrow 0.$$

Taking $\phi = [n]$ gives

$$0 \longrightarrow \frac{E(K)}{nE(K)} \longrightarrow S^{(n)}(E/K) \longrightarrow (E/K)[n] \longrightarrow 0.$$

Rearranging the proof of weak Mordell-Weil gives

Theorem 1.11. *$S^{(n)}(E/K)$ is finite.*

Proof: For L/K a finite Galois extension there is an exact sequence

$$0 \longrightarrow H^1(\mathrm{Gal}(L/K), E(L)[n]) \xrightarrow{\text{inf}} H^1(K, E[n]) \xrightarrow{\text{res}} H^1(L, E[n]).$$

The first nonzero term above is finite, and $S^{(n)}(E/K) \to S^{(n)(E/L)}$ is induced by res since $S^{(n)}(E/K) \subseteq H^1(K,E[n])$ and $S^{(n)(E/L) \subseteq H^1(L,E[n])}$. Therefore, by extending our field, we may assume $E[n] \subseteq E(K)$ and hence $\mu_n \subseteq K$. This implies that $E[n] \cong \mu_n \times \mu_n$ as a $\mathrm{Gal}(\overline{K}/K)$-module.

Therefore $H^1(K,E[n]) \cong H^1(K,\mu_n) \times H^1(K,\mu_n) \cong K^*/(K^*)^n \times K^*/(K^*)^n$. Let

$$S = \text{primes of bad reduction for } E/K \cup \{v \mid n\infty\}.$$

N.B. This is a finite set of places. □

Definition 1.12. The subgroup of $\mathrm{H}^1(K,A) unramifiedoutside\mathrm{S}isThereisacommutativediagramwithexactrows$

<put commutative diagram here>

This map is surjective (the x_n map) for all $v \notin S$ (see Theorem 9.7 from class) therefore $(\delta_v) \subseteq \ker(\text{green downward map})$.

Lemma 1.13. Let $\ker\left(H^1(K,\mu_n) \to H^1(K^{nr},\mu_n)\right) \subseteq \{x \in K^*/(K^*)^n \mid v(x) \equiv 0 \pmod{n}\}$. Therefore

$$\begin{aligned} S^{(n)}(E/K) &= \left\{\alpha \in H^1(K,E[n]) \mid \mathrm{res}_v(\alpha) \in (\delta_v)\ \forall v\right\} \\ &\subseteq H^1(,E[n];S) \\ &\cong H^1(K,\mu;S) \times H^1(K,\mu_n;S) \\ &\cong K(S,n) \times K(S,n). \end{aligned}$$

But $K(S,n)$ is finite by Lemma 11.4, therefore $S^{(n)}(E/K)$ is finite.

Remark 1.14. $S^{(n)A}(E/K)$ is finite and effectively computable. If is conjectured that $|(E/K) < \infty$. This would imply that (K) is effectively computable.

2 Descent by cyclic isogeny

Let E and E' be elliptic curves over a number field K, and let $\phi : E \longrightarrow E'$ be an isogeny of degree n. Suppose $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ as a Galois module $S \mapsto e_\phi(S,T)$. Short-exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0.$$

Long exact sequence

... [r] E(K) [r,"ϕ"]$E'(K)[r,"\delta"][rd,"\alpha"]H^1(K,\mu_n)[r][d,"\cong"]$...
K$^*/(K^*)^n$

Theorem 2.1. *Let $f \in K(E')$ and $g \in K(E)$ with* $\mathrm{div}(f) = n(T) - n(P)$ *and* $\phi^* f = g^n$. *Then* $\alpha(P) = f(P) \mod (K^*)^n$ *for all* $P \in E'(K) \setminus \{0,T\}$.

Proof: Let $Q \in \phi^{-1}P$. Then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n$.

$$\begin{aligned} e_\phi(-Q,T) &= \frac{g(rQ - Q + X)}{gX)} && \text{for any } x \in E \setminus \text{zeros and poles} \\ &= \frac{g(\sigma Q)}{g(Q)} && x = Q \\ &= \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}} && \text{N.B.} f(P) = g(Q)^n \end{aligned}$$

Therefore $\delta(P)$ is represented by the cocycle $\sigma \mapsto \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}$. But $H^1(K,\mu_n) \cong K^*/(K^*)^n$, $big(\sigma \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}})x$. Therefore $\alpha(P) = f(P) \mod (K^*)^n$. □