Lecture Notes from Differential Geometry (Michaelmas 2021)

Isaac Martin

Last compiled March 16, 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 $\zeta_n \in K$. □

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

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

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

If $G = \text{Gal}(\overline{K}/K)$ 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

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

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

Proof: Let $G = \text{Gal}(L/K)$. 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. $H^1(\text{Gal}(\overline{K}/K), \overline{K}^*) = 0$.

Application: Assume $\text{char}\,K \nmid n$. There is an exact sequence of $\text{Gal}(\overline{K}/K)$-modules

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

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 □

§ ***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 $v : K^* \longrightarrow \mathbb{Z}$ extends to $v : (K^{nr})^{*\to\mathbb{Z}})$. Then $v(x) = nv(y) \equiv 0 \pmod{n}$. □

EXERCISE: (in local fields.) Show that if $p \not| n$ 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

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

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*

$$\text{look at picture and fill in}, weirddisjointunionlookingsymbolwiththreeverticalstrokes.$$

We get a short-exact sequence

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

Taking $\phi = [n]$ gives

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

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 $H^1(K, A)$ unramified outside S is

$$H^1(K, A; S) = \ker\left(H^1(K, A)\; to \prod_{v \notin S} H^1(K_v^{nr}, A)\right)$$

There is a commutative diagram with exact rows

<put commutative diagram here>

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

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

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

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 $|\text{Ш}(E/K) < \infty$. This would imply that $\mathrm{rank}\, E(K)$ 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

$$\begin{tikzcd}
\ldots \arrow[r] & E(K) \arrow[r, "\phi"] & E'(K) \arrow[r, "\delta"] \arrow[dr, "\alpha"] & H^1(K,\mu_n) \arrow[r] \arrow[d, "\cong"] & \ldots \\
& & & K^*/(K^*)^n &
\end{tikzcd}$$

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 $\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n$.

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

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

§ *Lecture 3*

Recorded: 2022-03-14   Notes: 2022-03-14

Theorem 2.2. *Let $f \in K(E')$ and $g \in K(E)$ with $\operatorname{div}(f) = n(T) - n(0)$ and $\phi^* f = g^n$. Then there exists a group homomorphism $\alpha : E'(K) \longrightarrow K^*/(K^*)^n$ with $\ker\alpha = \phi(E(K))$ and $\alpha(P) = f(P) \mod (K^*)^n$ for all $P \in E'(K) \setminus \{0, T\}$.*

2.1 Descent by 2-isogeny

$E:\ y^2 = x(x^2 ax + b)$

$E':\ y^2 = x(x^2 + a'x + b')$ where $b(a^2 - 4ab) \neq 0$, $a' = -2a$ $b' = a^2 - 4b$. Let $\phi : E \longrightarrow E'$, $(x,y) \mapsto \left(\left(\frac{x}{y}\right)^2, \frac{y(x^2-b)}{x^2}\right)$. Then

$$\hat{\phi} E' \longrightarrow E,\ (x,y) \mapsto \left(\frac{1}{4}\left(\frac{y}{x}\right), \frac{y(x^2 - b')}{8x^2}\right)^2.$$

Then $E[\phi] = \{0, T\}$, $T = (0,0) \in E(K)$ and $E'[\hat{\phi}] = \{0, T'\}$, $T' = (0,0) \in E'(K)$.

Proposition 2.3. There is a group homomorphism

$$E'(K) \longrightarrow K^*/(K^*)^2,\ (x,y) \mapsto \begin{cases} x(K^*)^2 & \text{if } x \neq 0 \\ b'(K^*)^2 & \text{if } x = 0 \end{cases}$$

with kernel $\phi E(K)$.

> *Proof:* **Either** Apply Theorem (2.2) with $f = x \in K(E')$ and $g = \frac{y}{x} \in K(E)$ **or** do direct calculation, see example sheet 4. □

Two maps

$$\alpha_E : \frac{E(K)}{\hat{\phi} E'(K)} \hookrightarrow K^*/(K^*)^2$$
$$\alpha_{E'} : \frac{E'(K)}{\phi E(K)} \hookrightarrow K^*/(K^*)^2.$$

Lemma 2.4.

$$2^{\operatorname{rank} E(K)} = \frac{|\operatorname{img}(\alpha_E)| \cdot |\operatorname{img} \alpha_{E'}}{4}.$$

> *Proof:* If
>
> $$A \xrightarrow{f} B \xrightarrow{g} C$$
>
> is a homomorphism of abelian groups then there is an exact sequence
>
> $$0 \longrightarrow \ker(f) \longrightarrow \ker(gf) \xrightarrow{f} \ker(g) \longrightarrow \operatorname{coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \longrightarrow \operatorname{coker}(g) \longrightarrow 0.$$

Since $\hat{\phi}\phi = [2]_E$ we get an exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[2] \xrightarrow{\phi} E'(K)[\hat{\phi}] \longrightarrow \frac{E'(K)}{\phi E(K)} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \longrightarrow \frac{E(K)}{\hat{\phi}E'(K)} \longrightarrow 0.$$

The leftmost nontrivial term above is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the third nontrivial term is also $\mathbb{Z}/2\mathbb{Z}$, the fourth is isomorphic to $\operatorname{img}\alpha_{E'}$, and the rightmost nontrivial term is $\operatorname{img}\alpha_E$.

Therefore

$$\frac{|E(K)/2E(K)|}{|E(K)[2]|} = \frac{|\operatorname{img}\alpha_E|\cdot|\operatorname{img}\alpha_{E'}|}{2\cdot 2}.$$

Mordell-Weil implies $E(K) \cong \Delta \times \mathbb{Z}^r$ where Δ is a finite group, $r = \operatorname{rank} E(K)$.

$$\frac{E(K)}{2E(K)} \cong \frac{\Delta}{2\Delta} \times (\mathbb{Z}/2\mathbb{Z})^r$$

and $E(K)[2] \cong \Delta[2]$. Therefore $\frac{|E(K)/2E(K)|}{|E(K)[2]|} = 2^r$. Taken with equation (**??**), this proves the result. □

Lemma 2.5. If K is a number field and $a, b \in \mathcal{O}_K$ then $\operatorname{img}(\alpha_E) \subseteq K(S,2)$ where $S = \{\text{primes dividing } b\}$.

Proof: Must show that if $x, y \in K$, $y^2 = x(x^2+ax+b)$ and $v_{\mathfrak{p}}(b)$, then $v_{\mathfrak{p}}(x) = 0 \ (\mod 2)$.

Case $v_{\mathfrak{p}}(x) < 0$, then Lemma 9.1 $\implies v_{\mathfrak{p}}(x) = -2r$ and $v_{\mathfrak{p}}(y) = -3r$ for some $r \geq 1$.

Case $v_{\mathfrak{p}}(x) < 0$, then $v_{\mathfrak{p}}(x^2+ax+b) = 0 \implies v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(y^2) = 2v_{\mathfrak{p}}(y)$. □

Lemma 2.6. If $b_1 b_2 = b$ then $b_1(K^*)^2 \in \operatorname{img}(\alpha_E)$ or equivalently $\omega^2 = b_1u^4 + au^2v^2 + b_2v^4$ is soluble for $u, v, w \in K$ not all zero.

Proof: If $b_1 \in (K^*)$ or $b_2 \in (K^*)^2$ then both conditions are satisfied. So we may assume $b_1, b_2 \notin (K^*)^2$. Have $b_1(K^*) \in \operatorname{img}(\alpha_E) \iff$ there exists some $(x,y) \in E(K)$ such that $x = b_1t^2$ for some $t \in K^*$. This implies $y^2 = b_1t^2\left((b_1)^2 + ab_1t^2 + b\right) \implies \left(\frac{y}{b_1t}\right)^2 = b_1t^4 + at^2 + b/b_1$. So the ω^2 equation above has a solution $u = t, v = 1, \omega = \frac{y}{b_1t}$.

Conversely (simply perform same calculation in reverse), if (u, v, ω) is a solution to the ω equation above, then $uv \neq 0$ and $\left(b_1\left(\frac{u}{v}\right)^2, b_1\frac{u\omega}{v^3}\right) \in E(K)$. □

Example 2.7. Take $K = \mathbb{Q}$ and $E :\ t^2 = x^3 - x$, $a = 0$ and $b = -1$. Then $\operatorname{img}(\alpha_E) = \langle -1 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$, $E' :\ y^2 = x^3 + 4x$. $\operatorname{img}(\alpha_E') \subseteq \langle -1, 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Have

$$\begin{aligned} b_1 &= -1 & \omega^2 &= -y^4 - 4v^4 \\ b_1 &= 2 & \omega^2 &= 2u^4 + 2v^4 \\ b_1 &= -2 & \omega &- 2u^4 - 2v^4. \end{aligned}$$

The first and third equations are insoluble over $\mathbb{R}$, while the second has solution $(u, v, \omega) = (1, 1, 2)$. Therefore $\operatorname{img}(\alpha_{E'}) = \langle 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$ and $2^{\operatorname{rank} E(\mathbb{Q})} = \frac{2\cdot 2}{4} \implies \operatorname{rank} E(\mathbb{Q}) = 0 \implies 1$ is not a congruent number.

Example 2.8. $E: y^2 = x^3 + px$ with p prime $p \equiv 5 \pmod 8$. Let $b_1 = -1$, $\omega^2 = -u^4 - pv^4$ insoluble over $\mathbb{R}$. Therefore $\mathrm{img}(\alpha_E) = \langle p \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

§ *Lecture 4*

Recorded: 2022-03-16 Notes: 2022-03-16

Last time had an elliptic curve $E: \; y^2 = x(x^2+ax+b)$, $\phi : E \longrightarrow E'$ a 2-isogeny. Set $b_2 = b/b_1$ and

$$w^2 = b_1u^4 + au^2v^2 + b_2v^4$$

$$w^2 = b_1u^4 + a'u^2v^2 + b_2v^4$$

with $b_2 = b'/b_1$. Here, we additionally had that $a' = -2a$ and $b' = a^2 - 4b$. We then get an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \arrow[r] \arrow[dr, "\alpha_{E'}"] & S^{(\phi)}(E/\mathbb{Q}) \arrow[r] \arrow[d, "\text{inc}"] & \text{Ш}(E/\mathbb{Q})[\phi^*] \arrow[r] & 0 \\
& & \mathbb{Q}^*/(\mathbb{Q}^*)^2 & &
\end{tikzcd}$$

Then $\operatorname{img}(\alpha_E) = \{b_1(\mathbb{Q}^*)^2 \mid (*) \text{ is soluble over } \mathbb{Q}\}$ is a subset of $S^{(\phi)}(E/\mathbb{Q}) = \{b_1(^*)^2 \mid (*') \text{ is soluble over } \mathbb{R} \text{ and over } \mathbb{Q}_p$ for a

Fact: (Uses Ex Sheet 3, Question 9 and Hensel's lemma) If $a, b_1, b_2 \in \mathbb{Z}$ and $p \not| 2b(a^2-4b)$ then $(*)$ is soluble over $\mathbb{Q}$.

Example 2.9 (Continued from last lecture)**.** $y^2 = x^3 + px$ with p prime and $p \equiv 5 \pmod 8$, then

(1) $w^2 = 2u^4 - 2pv^4$

(2) $w^2 = -2u^4 + 2pv^4$

(3) $w^2 = pu^4 - 4v^4$.

(1) and (2) are insoluble over $\mathbb{Q}_p$ since $\left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = -1$, e.g. if (2) had a solution with $u, v, w \in \mathbb{Q}_p$ (not all zero) then without loss of generality $u, v \in \mathbb{Z}_p$ are coprime.

If $p|u$ then $p|w$ and then $p|v$, contradiction. Therefore

$$\operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{if (3) is insoluble over } \mathbb{Q} \\ 1 & \text{if (3) is soluble over} \mathbb{Q} \end{cases}.$$

(3) is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = +1$, so by Hensel's lemma, $-1 \in (\mathbb{Z}_p^*)^2$. (3) is insoluble over $\mathbb{Q}_2$ since $p - 4 \equiv 4 \pmod 8$ so by Hensel's lemma $p - 4 \in (\mathbb{Z}_2^*)^2$. (3) is soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

It is an **open conjecture** that $\operatorname{rank} E(\mathbb{Q}) = 1$ for all primes $p \equiv 5 \pmod 8$.

Example 2.10 (Lind)**.** $E: \; y^2 = x^3 + 17x$. $\operatorname{img}(\alpha_E) = \langle 17 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)2$. Set $E': \; y^2 = x^3 - 68x$, then $b_1 = 2$ and $\omega^2 = 2u^4 - 34v^4$. Replace w by $2w$ and divide by 2 to get

$$C : 2w^2 = u^4 - 17v^4.$$

Notation:

$$C(K) = \left\{ (u,v,w) \in K^3 \setminus \{0\} \,\middle|\, \text{satisfying equation } (\textbf{??}) \right\}$$

where $(u,v,w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for all $\lambda \in K^*$.

- $C(\mathbb{Q}_2) \neq \emptyset$ since $7 \in (\mathbb{Q}_2^*)^2$
- $C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Q}_{17}^*)^2$
- $C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$.

Therefore $C(\mathbb{Q}_p) \neq \emptyset$ for all places v of $\mathbb{Q}$. Suppose $(u,v,w) \in C(\mathbb{Q})$ with (wlog) u,v,w $\in \mathbb{Z}$,gcd$(u,v) = 1$, $w > 0$. If $17|w$, then $17|u$ and then $17|v$. Contradiction since u and v assumed to by coprime. So if $p|w$ with p and odd prime, then $p \neq 17$ and $\left(\frac{17}{p}\right) = 1$ which implies $\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1$ by quadratic reciprocity. Also note: $\left(\frac{2}{17}\right) = 1$, therefore $\left(\frac{w}{17} = 1\right)$.

But $2w^2 \equiv u^4 \pmod{17}$, hence $2 \in (\mathbb{F}_{17}^*)^4 = \{\pm_1, \pm 4\}$. A contradiction. Therefore $C(\mathbb{Q}) = \emptyset$, i.e. C is a counterexample to the Hasse principle. It represents a nontrivial element of $\text{Ш}(E/\mathbb{Q})$.

Birch Swinterton-Dyer Conjecture Let $E/\mathbb{Q}$ be an elliptic curve.

Definition 2.11.

$$L(E,s) = \prod_p L_p(E,s)$$

where

$$L_p(E,s) = \begin{cases} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} & \text{if } E \text{ has good reduction at } p \\ (1 \pm p^{-s})^{-1} & \text{if } E \text{ has multiplicative reduction at } p \\ 1 & \text{if E has additive reduction at } p. \end{cases}$$

Here $\#\tilde{E}(\mathbb{F}_p) = p + 1 - a_p$.

Hasse's theorem implies $|a_p| \leq 2\sqrt{p}$ and so $L(E,s)$ converges for $\text{Re}(s) > 3/2$.

Theorem 2.12 (Wiles, Breil, Conrad, Diamond, Taylor)**.** *$L(E,s)$ is the L-function of a weight 2 modular form and hence has an analytic continuation to all of $\mathbb{C}$ (and a function equation $L(E,s) \leftrightarrow L(E,2-s)$).*

Wiles proved the special case of the modularity theorem for semi-simple (semi-stable?) elliptic curves, which was good enough for Fermat's last theorem.

The weak BSD: [Weak BSD] $\text{ord}_{s=1} L(E,s) = \text{rank}\, E(\mathbb{Q}) A$. [Strong BSD] This says

$$\lim_{s \to 1} \frac{1}{(s-1)^r} L(E,s) = \frac{\Omega_E \cdot E(\mathbb{Q}) \cdot |\text{Ш}(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}$$

where

- c_p is the Tamagawa number of $E/\mathbb{Q}_p$, i.e. $c_p = [E)\mathbb{Q}_p) : E_0(\mathbb{Q})_p]$

- $E(\mathbb{Q})/E(\mathbb{Q})_{tors} = \langle p_1, ..., p_r \rangle$,
- $E(\mathbb{Q}) = \det([P_i, P_j])_{i,j=1,...,r}$,
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y+a_1x+a_3}$,
- $[P,Q] = \hat{h}(P+Q) - \hat{P} - \hat{Q}$
- a_i = coefficient of a global minimal Weiestrauss equation for E/Q.