Ranks and Parity of Ranks of Curves and Abelian Surfaces

MA842 at BU Spring 2019

Céline Maistret

April 19, 2019

These are notes for Céline Maistret's course MA842 at BU Spring 2019.
The course webpage is https://sites.google.com/view/cmaistret/teaching#h.p_BYGoPzU848FJ.

Lecture 1 22/1/2018

Outline

1. Elliptic curves and their ranks
   (a) Background
      i. Mordell Weil theorem (state and prove) (ANT and cohomological proof)
      ii. Non-effectivity
      iii. Computing the rank (descent)
   (b) The Birch and Swinnerton-Dyer conjecture
      i. Heuristic via counting points omn the reduced curve
      ii. L-functions
      iii. BSD-1
      iv. Local arithmetic invariants and BSD-2
   (c) Parity of ranks
      i. Isogeny invariants of BSD 2
      ii. Galois representations and local root numbers
      iii. The parity conjecture
2. Abelian surfaces
   (a) Background on genus 2 curves and their Jacobians
   (b) BSD in this case
   (c) Computability of local arithmetic invariants
   (d) Parity conjecture

Evaluation, none, when not around will give exercise/project, if you come regularly and do a computation you pass.

Main references that we will be following:

1. Vladimir Dokchitser - Lecture course
2. Silverman - Arithmetic of Elliptic Curves
3. Milne - Abelian Varieties?

1 Elliptic curves and their ranks

Sources: Silverman I, V. Dokchitser's lectures.

1.1 Mordell-Weil

Let K be a number field and let E/K be an elliptic curve. The group $E(K)$ is finitely generated.

$$E(K) \simeq E(K)_{\text{tors}} \oplus \mathbf{Z}^r.$$

Where $E(K)_{\text{tors}}$ is a finite subgroup and r is the rank, a non-negative integer.

Assuming that we can compute the torsion subgroup, computing the rank would completely determine $E(K)$ and hence solve the associated diophantine problem.

Plan

1. Understand the proof of Mordell-Weil
2. See where it is non-effective.
3. From the proof, extract a strategy to sometimes compute the rank (define Selmer groups, Shafarevich-Tate group).

Outline proof of Mordell-Weil. Part 1: Prove that

$$E(K)/mE(K)$$

is finite for some $m \geq 2$.

Part 2: use a descent argument with heights of points. ∎

Of these two parts of the proof, part 1 is the challenging/interesting one.

For part 2: Assuming that

$$E(K)/mE(K)$$

is finite and that E has a "height function" then $E(K)$ is finitely generated.

Theorem 1.1 Descent theorem (see Thm. VIII 3.1). *Let A be an abelian group, suppose that there exists a function*

$$h\colon A \longrightarrow \mathbf{R}$$

with the following properties:

1. *Let $Q \in A$ then there is a constant c_1 depending on Q and A such that*
$$h(P+Q) = 2h(P) + c_1,\ \forall P \in A.$$
2. *There is an integer $m \geq 2$ and a constant c_2 depending on A s.t.*
$$h(mP) \geq m^2 h(P) - c_2,\ \forall P \in A.$$
3. *For every constant c_3, the set*
$$\{P \in A : h(P) \leq c_3\}$$
is finite.

suppose further that for the m in 2. we have A/mA is finite. Then A is finitely generated.

Proof. Choose elements $Q_1, \ldots, Q_r \in A$ to represent the finitely many cosets in A/mA. Let P be a point in A. We show that P can be generated by $Q_1, \ldots, Q_r$ plus a set of finitely many points of bounded height.

First write
$$P = mP_1 + Q_{i_1}$$
for some $1 \leq i \leq r$. Repeat this for
$$P_1 = mP_2 + Q_{i_2}$$
$$P_2 = mP_3 + Q_{i_3}$$
$$\vdots$$
$$P_{n-1} = mP_n + Q_{i_n}$$
by property 2. of h we have
$$h(P_j) \leq \frac{1}{m^2}(h(mP_j) + c_2)$$
$$\frac{1}{m^2}(h(P_{j-1}) - Q_{i_j}) + c_2)$$
$$\leq \frac{1}{m^2}(2h(P_{j-1}) + c_1' + c_2)$$
by 1. Where c_1' is the maximum of the constants from i for Q in $\{-Q_1, \ldots, -Q_r\}$. Note that c_1' and c_2 do not depend on P and that $h(P) \geq 0$. We repeat this inequality starting from P_n and working back to P.
$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right)(c_1' + c_2)$$
$$= \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right)(c_1' + c_2)$$
$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_1' + c_2}{m^2 - 2}$$
$$\leq \frac{1}{2^n} h(P) + \frac{c_1' + c_2}{2},$$
since $m \geq 2$. Hence for n sufficiently large (to make $\frac{1}{2^n} h(P) \leq 1$) we have
$$h(P_n) \leq 1 + \frac{1}{2}(c_1' + c_2).$$
Since P is a linear combination of P_n and Q_i
$$P = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j},$$
it follows that every $P \in A$ is a linear combination of points in
$$\{Q_1, \ldots, Q_r\} \cup \{Q \in A : h(Q) \leq 1 + \frac{1}{2}(c_1' + c_2)\}.$$
■

Remark 1.2 On $E/\mathbf{Q}$ the height function

$$h\colon E(\mathbf{Q}) \to \mathbf{Q}$$

$$P \mapsto \begin{cases} \log(\max\{|p|,|q|\}),\ x(P) = \frac{p}{q}, & P \neq 0, \\ 0, & P = 0. \end{cases}$$

satisfies the conditions of Theorem 1.1.

Remark 1.3 The above proof is effective. To find generators of $E(\mathbf{Q})$ first compute $c_1 = c_1(Q_i)$ for each i, then compute c_2. Find points of bounded height. Note that we need $Q_1, \ldots, Q_r$ to start with.

It remains to show part 1:

Theorem 1.4 Weak Mordell-Weil. *Let K be a number field E/K an elliptic curve, $m \geq 2$ then*

$$\# E(K)/mE(K) < \infty.$$

We will prove this under the assumption that $E[m] \subseteq E(K)$. This is WLOG since:

Lemma 1.5 *Let L/K be a finite Galois extension, if*

$$E(L)/mE(L)$$

is finite then so is

$$E(K)/mE(K).$$

Proof.

$$0 \to \phi \to E(K)/mE(K) \xrightarrow{\varphi} E(L)/mE(L) \to 0$$

induced by

$$E(K) \subseteq E(L),$$

and prove that ϕ is finite. Kernel ϕ is given by

$$\frac{E(K) \cap mE(L)}{mE(K)},$$

take $P \in \phi$. We can choose $Q_P \in E(L)$ such that $Q_P = P$. Define a map of sets

$$\lambda_P\colon G_{L/K} \to E[m]$$

$$\sigma \mapsto Q_P^\sigma - Q_P.$$

Note that

$$[m](Q_P^\sigma - Q_P) = ([m]Q_P)^\sigma - [m]Q_P = 0.$$

Now we show that the association

$$\phi \to \mathrm{Map}(G_{L/K}, E[m])$$

$$P \mapsto \lambda_P$$

is 1 to 1.

Suppose that $P, P' \in E(K) \cap mE(L)$ satisfying $\lambda_P = \lambda_{P'}$ then

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$$

for all $\sigma \in G_{L/K}$ so $Q_P - Q_{P'} \in E(K)$ and hence

$$P - P' = [m]Q_P - [m]Q_{P'} \in mE(K)$$

hence

$$P = P' \pmod{mE(K)}.$$

$G_{L/K}$ and $E[m]$ are both finite, hence so is ϕ. ∎

Lecture 2 29/1/2018

Now we will prove the weak Mordell-Weil theorem. Using the above lemma we can reduce to the case where $E[m] \subseteq E(K)$, so we assume this going forwards.

Definition 1.6 The Kummer pairing. The **Kummer pairing** is

$$\kappa\colon E(K) \times G_{\overline{K}/K} \to E[m]$$

$$P, \sigma \mapsto Q^\sigma - Q$$

where Q is a choice of point in $E(\overline{K})$ such that $mQ = P$. ◊

Proposition 1.7 *κ is well defined, bilinear, the kernel in the first argument is $mE(K)$ and in the second argument is $G_{\overline{K}/L}$ where $L = K([m]^{-1}E(K))$ is the compositum of all fields $\kappa(x(Q), y(Q))$ as Q ranges over all the points of $E(\overline{K})$ s.t. $mQ \in E(K)$.*

Hence the Kummer pairing induces a perfect bilinear pairing

$$E(K)/mE(K) \times G_{L/K} \to E[m]$$

i.e. the map

$$E(K)/mE(K) \to \mathrm{Hom}_K(G_{L/K}, E[m])$$

$$P \mapsto (\sigma \mapsto Q^\sigma - Q)$$

is an isomorphism.

Proof. Of part 4.

Take ■

Lecture 3 31/1/2018

Lecture 4 5/2/2018

Remark 1.8 A homomorphism $\phi\colon \mathrm{Gal}(\overline{K}/K) \to G$ for a finite group G is continuous if it comes from a finite Galois extension, i.e.

$$\exists F/K \text{ finite Galois },\ \tilde{\phi}\colon\ \mathrm{Gal}(F/K) \to G$$

s.t. ϕ is the composition $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(F/K) \xrightarrow{\tilde{\phi}} G$. So $\phi(g)$ only cares about what g does to F.

Proposition 1.9 *Let E/K be an elliptic curve*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

for $P \in E(K)$ have $\frac{1}{2}P \in E(\overline{K})$ s.t. $\frac{1}{2}P \oplus \frac{1}{2}P = P$.

1. *$K(\frac{1}{2}P)/K$ is a Galois extension and $\mathrm{Gal}(K(\frac{1}{2}P)/K) = C_2 \times C_2$ from Lemma 1.*
2. $$\phi_P\colon\ \mathrm{Gal}(\overline{K}/K) \to E(K)[2]$$ $$g \mapsto Q^\sigma - Q = g(\frac{1}{2}P) - \frac{1}{2}P$$ *is well defined and has kernel $\mathrm{Gal}(K/K(\frac{1}{2}P))$.*
3. $$\phi\colon E(K)/2E(K) \to \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), E(K)[2])$$ $$P \mapsto \phi_P$$

is well defined and injective. Now ϕ_P is continuous by 2. *and so*

$$\begin{aligned}\phi_{P\oplus Q}(g) &= g(\frac{1}{2}(P\oplus Q)) - (\frac{1}{2}P\oplus\frac{1}{2}Q)\\ &= g(\frac{1}{2}P)\oplus g(\frac{1}{2}Q) - \frac{1}{2}P\ominus\frac{1}{2}Q\\ &= \phi_P(g)\oplus\phi_Q(g)\end{aligned}$$

a homomorphism.

$$\phi_{2Q}(g) = g(\frac{1}{2}2Q)) - \frac{1}{2}2(Q) = g(Q) - Q = 0$$

for all $g \in \mathrm{Gal}(\overline{K}/K)$ if $Q \in E(K)$ so this is well defined. For injectivity:

$$\phi_P(g) = 0 \implies g(\frac{1}{2}P) = \frac{1}{2}P \forall g \in \mathrm{Gal}(\overline{K}/K)$$

$$\implies \frac{1}{2}P \in E(K) \implies P \in 2E(K)$$

which gives injectivity.

4.

$$\eta\colon\ \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), E(K)[2]) \longrightarrow K^\times/K^{\times 2}\times K^\times/K^{\times 2}\times K^\times/K^{\times 2}$$

$$\psi \mapsto \psi_\alpha, \psi_\beta, \psi_\gamma$$

$$\psi(g) \in \{0,(\alpha,0)\} \subseteq E(K) \iff g \in \mathrm{Gal}(\overline{K}/K(\sqrt{\psi_\alpha}))$$

then η is an injective homomorphism. It is an isomorphism to the subgroup of triples a, b, c s.t. $abc \in K^{\times 2}$. Proof:

$$\mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), C_2) \simeq K^\times/K^{\times 2}$$

with ψ s.t. $\ker\psi = \mathrm{Gal}(\overline{K}/K\sqrt{d}) \leftrightarrow d$. It is an isomorphism:

$$\ker\psi_i = \mathrm{Gal}(\overline{K}/K(\sqrt{d_i})),\ i = 1,2$$

$$\ker\psi_1\psi_2 = \mathrm{Gal}(\overline{K}/K(\sqrt{d_1 d_2}))$$

Now apply this to $E(K)[2] = C_2\times C_2$ to get an isomorphism to $K^\times/K^{\times 2}\times K^\times/K^{\times 2}$. Record this third homomorphism to get η.

5. *If $P = (x_0, y_0) \in E(K)$ then*

$$\eta(\phi_P) = (x_0-\alpha, x_0-\beta, x_0-\gamma).$$

Proof sketch: If

$$E\colon\ y^2 = x^3 + Ax^2 + Bx$$

then for $Q = (x_0, y_0) \in E(K)$.

$$2Q = \left(\left(\frac{x_0 - B}{2y_0}\right)^2, \ldots\right)$$

Hence if $2Q = P = (x_1, y_1)$ then $\sqrt{x_1} \in K(\frac{1}{2}P)$. So if

$$E\colon\ y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

then

$$P = (x_2, y_2)$$

then

$$\sqrt{x_2-\alpha}, \sqrt{x_2-\beta}, \sqrt{x_2-\gamma} \in K(\frac{1}{2}P)$$

$$K(\sqrt{x_2-\alpha}), K(\sqrt{x_2-\beta}), K(\sqrt{x_2-\gamma}) \subseteq K(\frac{1}{2}P)$$

$$\implies K(\frac{1}{2}P) = K(\sqrt{x_2-\alpha}, \sqrt{x_2-\beta}, \sqrt{x_2-\gamma})$$

Example 1.10 Let

$$E\colon y^2 = x(x-1)(x+1)$$

for $P \in E(\mathbf{Q})$, $\mathbf{Q}(\frac{1}{2}P)/\mathbf{Q}$ can only ramify at 2.

$$\mathbf{Q}(\frac{1}{2}P) \subseteq \mathbf{Q}(i, \sqrt{2})$$

$$P = (x_0, y_0) \mapsto x_0, x_0 - 1, x_0 + 1 \in \mathbf{Q}^\times/\mathbf{Q}^{\times 2}$$

is a homomorphism so x_0, x_0-1, x_0+1 are $\pm 1, \pm 2$ up to square.

x_0	$x_0 - 1$	$x_0 + 1$	rat?
1	1	1	1) rat
1	-1	-1	2) non-rat
1	2	2	1) rat
1	-2	-2	2) non-rat
-1	1	-1	2) non-rat
-1	-1	1	1) rat
-1	2	-1	2) non-rat
-1	-2	2	1) rat
2	1	2	3) non-rat
2	-1	-2	2) non-rat
2	2	1	4) rat
2	-2	-1	2) non-rat
-2	1	-2	?
-2	-1	2	?
-2	2	-1	?
-2	-2	1	?

Table 1.11: Images

1) The 2-torsion points $P = 0, (0,0), (1,0), (-1,0) \in E(\mathbf{Q})$ give us some rows. 2) As we have $x_0 > -1$ we get $x_0 + 1 > 0$ so $x_0(x_0-1) > 0$ for the product to be a square (and hence > 0). 3) $x_0 = 2A^2$, $x_0 - 1 = B^2$, $x_0 + 1 = 2C^2$ with $A, B, C \in \mathbf{Q} \setminus \{0\}$. Let $A = m/n$ so $2m^2/n^2 - 1 = B^2$

$$2m^2 - n^2 = (Bn)^2$$

and

$$2m^2 + n^2 = 2(Cn)^2$$

if $m \equiv 0(2) \implies -1 = \square \pmod 8$ a contradiction.

$$m \equiv 1 \pmod 2 \implies m^2 \equiv 1 \pmod 8.$$

So $2 - n^2 = \square \pmod 8 \implies n^2 \equiv 1 \pmod 8$

$$2 + n^2 = 2\square \pmod 8 \implies n^2 \equiv 0 \pmod 8$$

$$|E(\mathbf{Q})/2E(\mathbf{Q})| = 4$$

$$|E(\mathbf{Q})[2]| = 4 \implies \mathrm{rk} = 0$$

$$E(\mathbf{Q}) \cong E(\mathbf{Q})[2].$$

4) Use the group structure! $\square$

Theorem 1.12 Complete 2-decent. *Let K be a field of characteristic 0 and*

$$E\colon y^2 = (x-\alpha)(x-\beta)(x-\gamma),\ \alpha, \beta, \gamma \text{ distinct.}$$

The map

$$P \mapsto (x_0 - \alpha, x_0 - \beta, x_0 - \gamma)$$

replacing $x_0 - \alpha$ with $(x_0 - \beta)(x_0 - \gamma)$ if 0.

$$E(K)/2E(K) \to (K^\times / K^{\times 2})^3$$

Triples (a, b, c) that lie in the image satisfy $abc \in K^{\times 2}$. A triple a, b, c with $abc \in K^{\times 2}$ lies in the image iff it is in the image of $E(K)[2]$ or

$$cz_3^2 - \alpha + \gamma = az_1^2$$

$$cz_3^2 - \beta + \gamma = bz_1^2$$

is soluble with $z_i \in K^\times$. In which case

$$P = (az_1^2 + \alpha, \sqrt{abc}, z_1 z_2 z_3) \mapsto (a, b, c)$$

iii) If K is a number field and (a, b, c) is in the image then

$$K(\sqrt{a}, \sqrt{b}, \sqrt{c})/K$$

only ramifies at primes dividing $2(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$.

Exercise 1.13

$$E\colon y^2 = x(x-5)(x+5).$$

Lecture 5 7/2/2018

Recall:

$$\phi\colon E(K)/2E(K) \to \mathrm{Hom}_{cts}(G_K, E(K)[2])$$

$$P \mapsto \phi_P$$

where $\phi_P\colon \sigma \mapsto Q^\sigma - Q$ where $Q = 2P$. Which is well-defined and injective.

Elements of

$$\mathrm{Hom}_{cts}(G_K, E[2]) \leftrightarrow a, b, c \in (K^\times / K^{\times 2}) \text{ s.t. } abc \in K^{\times 2}$$

$$(x_0, y_0) \mapsto (x_0 - \alpha, x_0 - \beta, x_0 - \gamma).$$

Lemma 1.14 *Let $n \geq 1$*

1.

$$\psi\colon E(K)/nE(K) \to \{K \subseteq F \subseteq \overline{K}\}$$

$$P \mapsto K(\frac{1}{n}P, E[n])$$

is well defined.

2. $K(\frac{1}{n}P, E[n])/K$ *only ramifies at* $\mathfrak{p}|n\Delta_E$.

3. $$\mathrm{Gal}(K(\frac{1}{n}P, E[n])/K) \le \mathbf{Z}/n \times \mathbf{Z}/n$$

4. *There are only finitely many fields satisfying 2. and 3. so* $\mathrm{im}\,\psi$ *is finite.*

To do descent, need more than ψ (i.e. injection).

Definition 1.15 Let G be a group and M a G-module then let

$$H^0(G, M) = M^G = \{m \in M : gm = m \forall g \in G\}$$

$H^1(G, M) = \{\text{skew homs } G \to M\}/\{\text{skew homs } G \to M \text{ of the form } g \mapsto g(t) - t,\ t \in M\}$.

◊

Remark 1.16 If G acts trivially on M then

$$H^0(G, M) = M$$

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

When G is profinite then we want that the skew homomorphisms factor through finite Galois groups. We will prove that

$$E(K)/nE(K) \hookrightarrow H^1(G_K, E[n]).$$

Theorem 1.17 *If*

$$0 \to A \to B \to C \to 0$$

is an exact sequence of G-modules then

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

Lemma 1.18

1. ψ *is finite-to-one (gives Mordell-Weil)*

2. *Let*
$$\phi_P \colon G_K \to E[n]$$
$$\phi_P(gh) = \phi_P(g) + g\phi_P(h)$$
is a skew (or crossed) homomorphism. If $(\frac{1}{n}P)'$ is another choice of $\frac{1}{n}P$ and ϕ'_P is the corresponding skew homomorphism, then
$$\phi_P - \phi'_P$$
is of the form
$$g \mapsto T \ominus gT$$
where $T \in E[n]$.

3. ϕ_P *factors through*
$$\mathrm{Gal}(K(\frac{1}{n}P, E[n])/K).$$

4. $$\phi \colon E(K)/nE(K) \to Z/B$$
$$P \mapsto \phi_P$$

is an injective homomorphism. Where

$$Z = \{\textit{skew homs } G_K \to E[n]\}$$

$$B = \{\textit{skew homs } G_K \to E[n] \textit{ of the form } g \mapsto T \ominus gT,\ T \in E[n]\}.$$

Proof.

1. There are finitely many skew homomorphisms

$$\mathrm{Gal}(K(\frac{1}{n}P, E[n])/K) \to E[n]$$

and by 4.

$$P \mapsto \{\phi_P, K(\frac{1}{n}P, E[n])\}$$

is injective. So $\psi\colon P \mapsto K(\frac{1}{n}P, E[n])$ is finite to one by 3.

2.

$$\phi_P(gh) = \frac{1}{n}P \ominus gh\frac{1}{n}P$$

$$= \left((\frac{1}{n}P) \ominus g(\frac{1}{n}P)\right) \oplus \left(g(\frac{1}{n}P) \ominus g(h(\frac{1}{n}P))\right)$$

$$= \phi_P \oplus g(\phi_P(h)).$$

Remark: If $E[n] \subseteq E(K)$ then ϕ_P is a homomorphism. Recall for $n = 2$

$$\phi_P(gh) = \frac{1}{2}P \ominus gh(\frac{1}{2}P)$$

$$= \frac{1}{2}P \ominus h(\frac{1}{2}P) \oplus h(\frac{1}{2}P) \ominus g(h(\frac{1}{2}P))$$

$$= \phi_P(h) \oplus \phi_P(g)$$

since $2h(\frac{1}{2}P) = h(P) = P$. Consider now

$$\frac{1}{n}P = \frac{1}{n}P' \oplus T$$

for some $T \in E[n]$

$$(\phi_P \ominus \phi'_P)(g) = \phi_P(g) - \phi'_P(g) = \frac{1}{n}P \ominus g(\frac{1}{n}P) - [(\frac{1}{n}P) \oplus T \ominus g(\frac{1}{n}P) \oplus gT]$$

$$= T \ominus gT.$$

■

Take $G = G_K$

$$B = E(\overline{K}), A = E[n], C = E(\overline{K})$$

to get

$$0 \to E[n] \to E(\overline{K}) \xrightarrow{\cdot n} E(\overline{K}) \to 0$$

which gives the long exact sequence

$$0 \to E(K)[n] \to E(K) \xrightarrow{\cdot n} E(K) \xrightarrow{\delta} H^1(G_K, E[n]) \to H^1(G_K, E(\overline{K})) \to$$

$$\implies E(K)/nE(K) \hookrightarrow H^1(G_K, E[n]).$$

Problem:

$$H^1(G_K, E[n])$$

is infinite. What subgroup of

$$H^1(G_K, E[n])$$

do we land in?

Notation: When v is a place of K we have $G_{K_v} \subseteq G_K$, for any module M have $M^{G_K} \leq M^{G_{K_v}}$ and

$$\mathrm{Res}\colon H^1(G_K, E[n]) \to H^1(G_{K_v}, E[n]).$$

We have from the theorem

$$\begin{tikzcd}
0 \arrow[r] & E(K)/nE(K) \arrow[r, "\delta"] \arrow[d] & H^1(G_K, E[n]) \arrow[r] \arrow[d, "\mathrm{Res}"] & H^1(G_K, E(\overline{K}))[n] \arrow[r] \arrow[d, "\mathrm{Res}"] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/nE(K_v) \arrow[r, "\delta"] & \prod_v H^1(G_{K_v}, E[n]) \arrow[r] & \prod_v H^1(G_{K_v}, E(\overline{K}))[n] \arrow[r] & 0
\end{tikzcd}$$

we want to understand $\operatorname{im}\delta$ i.e. the subgroup

$$\ker\{H^1(G_K, E[n]) \to H^1(G_K, E(\overline{K}))\}$$

this is as hard as finding $E(K)$, here is why:

Claim 1.19

$$H^1(G_K, E(\overline{K}))$$

corresponding to principal homogeneous spaces for E (genus 1 curves whose jacobian is E)

Finding

$$\ker\{H^1(G_K, E[n]) \to H^1(G_K, E(\overline{K}))\}$$

is equivalent to finding which PHS coming from H^1 have a rational point. ??? Hensel's lemma.

Let C be a curve

$$\mathrm{Isom}(C) \leftrightarrow C(\overline{K}) \times \mathrm{Aut}(C)$$

$$\tau_p \circ \alpha \leftrightarrow (P, \sigma)$$

$$\mathrm{Twist}(E/K) \leftrightarrow H^1(G_K, \mathrm{Isom}(C))$$

$$C \simeq_{\overline{K}} E$$

$$PHS \leftrightarrow H^1(G_K, E(\overline{K}))$$

C is a PHS for E iff E is the jacobian of C.

Lecture 6 14/2/2018

$$\begin{tikzcd}
0 \arrow[r] & E(K)/nE(K) \arrow[r, "\delta"] \arrow[d] & H^1(G_K, E[n]) \arrow[r] \arrow[d, "\mathrm{Res}"] & H^1(G_K, E(\overline{K}))[n] \arrow[r] \arrow[d, "\mathrm{Res}"] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/nE(K_v) \arrow[r, "\delta"] & \prod_v H^1(G_{K_v}, E[n]) \arrow[r] & \prod_v H^1(G_{K_v}, E(\overline{K}))[n] \arrow[r] & 0
\end{tikzcd}$$

Definition 1.20 Twists of curves. A **twist** of C/K is a smooth curve C'/K that is isomorphic to C over $\overline{K}$. $\Diamond$

If C_1, C_2 are twists of C/K and $C_1 \simeq_K C_2$ then we say that C_1 and C_2 are equivalent modulo K-isomorphism.

We denote $\mathrm{Twist}(C/K)$ - the set of twists of C/K modulo K-isomorphism.

Theorem 1.21 *The twists of C/K up to K-isomorphism are in 1-1 correspondence with elements of*

$$H^1(G_K, \mathrm{Isom}(C))$$

where

$$\mathrm{Isom}(C) = \{\overline{K}\text{-}\textit{isomorphisms } C \to C\}.$$

Proof. Let C'/K be a twist of C/K then there exists an isomorphism $/\overline{K}$

$$\phi \colon C' \to C$$

associate the following map

$$\xi \colon G_K \to \mathrm{Isom}(C)$$

$$\sigma \mapsto \phi^\sigma \phi^{-1}.$$

Check that ξ is a cocycle

$$\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau$$

for all $\sigma, \tau \in G_K$. Denote $\{\xi\}$ the associated class in H^1. $\{\xi\}$ is determined by the K-isomorphism class of C' independent of the choice ϕ.

The map

$$\mathrm{Twist}(C/K) \leftrightarrow H^1(G_K, \mathrm{Isom}(C))$$

$$C' \mapsto \{\xi\}$$

is a bijection.

Injective, trace through.

Surjectivity, define the function field using the curve. ■

Remark 1.22 If C is an elliptic curve then $\mathrm{Isom}(C)$ is generated by

$$\mathrm{Aut}(C)(\text{fixing } 0)$$

and translations

$$\tau_P \colon C \to C$$

$$Q \mapsto Q + P.$$

Example 1.23 E/K elliptic, consider

$$K(\sqrt{d})$$

a quadratic extension and χ the associated character

$$\chi \colon G_K \to \{\pm 1\}$$

$$\sigma \mapsto \sigma(\sqrt{d})/\sqrt{d}.$$

The group ± 1 can be viewed as automorphisms of C. So use χ to define the cocycle

$$\xi \colon G_K \to \mathrm{Isom}(C)$$

$$\sigma \mapsto [\chi(\sigma)].$$

Let C/K be the corresponding twist of E/K, we find an equation for C/K. Choose

$$y^2 = f(x) \text{ for } E/K$$

and write

$$\overline{K}(E) = \overline{K}(x, y)$$

$$\overline{K}(C) = \overline{K}(x, y)_\xi$$

since $[-1](x, y) = (x, -y)$ the action of $\sigma \in G_K$ on

$$\overline{K}(x, y)_\xi \text{ is given by } \sqrt{d}^\sigma = \chi(\sigma)\sqrt{d}$$

$$x^\sigma = x,\ y = \chi(\sigma)y$$

note that the function $x' = x$ and $y' = y/\sqrt{d}$ are in $\overline{K}(x, y)_\xi$ and are fixed by G_K. Now x', y' satisfy

$$dy'^2 = f(x')/K$$

is defined over K and defines an elliptic curve. Moreover

$$(x, y) \mapsto (x', y'\sqrt{d})$$

is an isomorphism over $K(\sqrt{d})$. □

Note C/K is not a principal homogeneous space for E/K.

Definition 1.24 Homogenous spaces. Let E/K be an elliptic curve, a principal homogeneous space for E/K is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over K.

$$\mu\colon C \times E \to C$$

morphism defined over K satisfying

1. $$\mu(P, 0) = P\ \forall P \in C$$

2. $$\mu(\mu(p, P), Q) = \mu(p, P + Q)\ \forall P \in C$$

3. $$\forall p, q \in C,\ \exists! P \in E \text{ s.t.}$$
   $$\mu(p, P) = q$$
   so we may define a subtraction map
   $$\nu\colon C \times C \to E$$
   $$p, q \mapsto P$$
   as above.

◊

Proposition 1.25 *Let E/K and C/K be a principal homogeneous space for E/K. Fix a point $p_0 \in C$ and define a map*

$$\theta\colon E \to C$$

$$P \mapsto \underbrace{p_0 + P}_{\mu(p_0,P)}.$$

1. *θ is an isomorphism over $K(p_0)$. In particular C/K is a twist of E/K.*
2. *$\forall p, q \in C$*
$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$
3. *θ is a morphism over K.*

Definition 1.26 Two homogeneous space C/K and C'/K for E/K are equivalent if there is an isomorphism
$$\phi\colon C \to C'$$
defined over K and is compatible with the action of E on C and C'.

$$\begin{tikzcd} C \arrow[r, "\theta"] \arrow[d, "\phi"'] & E \arrow[d] \\ C' \arrow[r] & E' \end{tikzcd}$$

◊

The equivalence class of PHS for E/K containing E/K acting on itself via translation is called the trivial class.

The collection of equivalence classes of PHS for E/K is called the Weil-Châtelet group, denoted
$$WC(E/K).$$
Proposition 1.27 *Let C/K be a PHS for E/K then C/K is in the trivial class $\iff C(K) \neq \emptyset$.*

Theorem 1.28 *Let E/K then there is a natural bijection after fixing $p_0 \in C$*

$$WC(E/K) \to H^1(G_K, \underbrace{E(\overline{K})}_{\subseteq \mathrm{Isom}(E)})$$

$$\{C/K\} \mapsto \{\sigma \mapsto p_0^\sigma - p_0\}$$

Proof. Well-definedness:
$$\sigma \mapsto p_0^\sigma - p_0$$
is a cocycle. Suppose that C'/K and C/K are two equivalent PHS then
$$p_0^\sigma - p_0$$
and
$${p'_0}^\sigma - p'_0$$
are cohomologous.

Injective, suppose that $p_0^\sigma - p_0$ and ${p'_0}^\sigma - p'_0$ corresponding to C/K and C'/K that are cohomologous and prove that $C \simeq_K C'$.

Surjective: let $\xi\colon G_K \to E(\overline{K})$ be a cocycle representing an element in $H^1(G_K, E)$. Embed
$$E(\overline{K}) \hookrightarrow \mathrm{Isom}(E)$$
$$P \mapsto \tau_P$$
and view
$$\xi \in H^1(G_K, \mathrm{Isom}\, E).$$

From the theorem on

$$\mathrm{Twist}(E/K) \leftrightarrow H^1(G_K, \mathrm{Isom}(E))$$

there exists a curve C/K and a $\overline{K}$-isomorphism

$$\phi \colon C \to E$$

s.t.

$$\forall \sigma \in G_K : \phi^\sigma \phi^{-1} = \text{translation by } -\xi_\sigma.$$

Define a map $\mu \colon C \times E \to C$

$$(p, Q) \mapsto \phi^{-1}(\phi(p) + Q).$$

Show that μ is simply transitive.

Show μ defined over K. Compute the cohomology class associated to C/K and show it is ξ. ■

Remark 1.29 For a given C/K of genus 1 one can define several structures of PHS.

$$\{C/K, \mu\}^\alpha = \{C/K, \mu \circ (1 \times \alpha)\}$$

$$\mu^\alpha(p, Q) = \mu(p, \alpha Q)$$

for $\alpha \in \mathrm{Aut}(E)$.

$$\begin{tikzcd} C \arrow[r, "\mu"] & E \arrow[d, "P"] \\ C' \arrow[r, "\mu^\alpha"] & E' \end{tikzcd}$$

Lecture 7 21/2/2018

Example 1.30 E/K and $K(\sqrt{d})/K$ a quadratic extension. Let $T \in E(K)$ be a non-trivial point of order 2. Then $\xi \colon G_K \to E$

$$\sigma \mapsto \begin{cases} 0 & \text{if } (\sqrt{d})^\sigma = \sqrt{d}, \\ T & \text{if } (\sqrt{d})^\sigma = -\sqrt{d}. \end{cases}.$$

We construct the PHS corresponding to $\{\xi\} \in H^1(G_K, E(\overline{K}))$. Since $T \in E(K)$ can choose a Weierstraß equation for E/K

$$E \colon y^2 = x^3 + ax^2 + bx \text{ with } T = (0, 0)$$

then the translation by T map is given by

$$\tau_T(P) = (x, y) + (0, 0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$$

for

$$P = (x, y).$$

Thus if $\sigma \in G_K$ is non-trivial, σ acts on $\overline{K}(E)_\xi$, which is isomorphic to $\overline{K}(E)$ but $\mathrm{Gal}(\overline{K}/K)$ action is twisted by ξ, i.e. $x^{\mathrm{id}} \mapsto (x^{\mathrm{id}})^\sigma$.

$$(\sqrt{d})^\sigma = -\sqrt{d}$$

$$x^\sigma = \frac{b}{x}, \; y^\sigma = -\frac{by}{x^2}$$

need to find the subfield of $K(\sqrt{d})(x,y)_\xi$ fixed by σ. Note:

$$\frac{\sqrt{d}x}{y},\ \sqrt{d}\left(x-\frac{b}{x}\right)$$

are invariant, take

$$z=\frac{\sqrt{d}x}{y},\ w=\sqrt{d}\left(x-\frac{b}{x}\right)\left(\frac{x}{y}\right)^2$$

and find relations between z and w to get

$$C\colon dw^2=d^2-2adz^2+(a^2-4b)z^4.$$

Claim: C/K is the PHS of E/K corresponding to $\{\xi\}$. There is a natural map

$$\phi\colon E\to C$$

$$(x,y)\mapsto(z,w)$$

$$(x,y)\mapsto\left(\frac{\sqrt{d}y}{x^2+ax+b},\frac{\sqrt{d}(x^2-b)}{x^2+ax+b}\right)$$

so that

$$\phi(0,0)=(0,-\sqrt{d})$$

$$\phi(0)=(0,\sqrt{d})$$

- Prove that ϕ is an isomorphism so C is a twist.
- C is the PHS corresponding to $\{\xi\}$. Take $p\in C$ and compute

  $$\sigma\mapsto p^\sigma-p=\phi^{-1}(p^\sigma)-\phi^{-1}(p)$$

  for example let $p=(0,\sqrt{d})\in C$, if $\sigma=\text{id}$ then $p^\sigma-p=0-0=0$. If $\sigma=-\text{id}$ then $p^\sigma-p=T-0=T$.

□

Back to Selmer, we want to have the image of our weak Mordell-Weil land in something finite.

$$\begin{tikzcd}
0 \arrow[r] & E(K)/mE(K) \arrow[r, "\delta"] \arrow[d] & H^1(G_K,E[m]) \arrow[r] \arrow[d, "\mathrm{Res}"] & WC(E/K)[m] \arrow[r] \arrow[d, "\mathrm{Res}"] & 0 \\
0 \arrow[r] & \prod_v E(K_v)/nE(K_v) \arrow[r, "\delta"] & \prod_v H^1(G_{K_v},E[n]) \arrow[r] & \prod_v WC(E/K_v)[m] \arrow[r] & 0
\end{tikzcd}$$

Definition 1.31 *m***-Selmer groups.** The m-Selmer group of E/K is the subgroup of

$$H^1(G_K,E[m])$$

defined by

$$\mathrm{Sel}^m(E/K)=\ker\left\{H^1(G_K,E[m])\to\prod_v WC(E/K_v)\right\}.$$

◊

Definition 1.32 The Shafarevich-Tate group. The **Shafarevich-Tate** group of E/K is the subgroup of

$$WC(E/K)$$

defined by

$$\text{III}(E/K) = \ker\left\{WC(E/K) \to \prod_v WC(E/K_v)\right\}.$$

◊

Theorem 1.33 *There is an exact sequence*

1. $$0 \to E(K)/mE(K) \to \mathrm{Sel}^m(E/K) \to \text{III}(E/K)[m] \to 0$$

2. $\mathrm{Sel}^m(E/K)$ *is finite.*

1.2 p^∞-Selmer and the structure of III

$H^1(G_K, E(\overline{K}))$ is torsion for general galois cohomological reasons. So

$$\text{III}(E/K) \subseteq H^1(G_K, E(\overline{K}))$$

is torsion.

So we may write

$$\text{III}(E/K) = \bigoplus_p \text{III}_{p^\infty}(E/K)$$

where for each prime p

$$\text{III}_{p^\infty}(E/K)$$

denotes the p-primary part of $\text{III}(E/K)$. (i.e. the subgroup of elements whose order is a power of p.) By descent

$$\text{III}(E/K)[m] \text{ is finite for all } m \geq 1.$$

So

$$\text{III}_{p^\infty}(E/K) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p} \oplus T_p,\ \delta_p \in \mathbf{Z}_{\geq 0}$$

where T_p is a finite abelian p-group.

$$T_p \cong \mathbf{Z}/p^{s_1}\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/p^{s_l}\mathbf{Z},\ s_i \in \mathbf{Z}_{\geq 0}.$$

The group

$$\bigoplus_p (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p} \subseteq \text{III}(E/K)$$

is called the infinitely divisible subgroup of III denoted III_{div}.

The conjecture that III is finite implies $\delta_p = 0$ for all p. And $T_p \neq 0$ for only finitely many p.

There is a pairing called the Cassels-Tate pairing

$$\text{III}(E/K) \times \text{III}(E/K) \to \mathbf{Q}/\mathbf{Z}$$

which is bilinear and alternating, and the kernel on either side is the infinitely divisible group. If $\text{III}(E/K)$ is finite then the pairing is non-degenerate and hence

$$|\,\text{III}(E/K)| = \square \in \mathbf{Z}.$$

Definition 1.34 **p^∞-Selmer group.** Consider $\mathrm{Sel}_{p^n}(E/K)$ and take the direct limit

$$\varinjlim_n \mathrm{Sel}_{p^n}(E/K)$$

to define the p^∞-Selmer group. ◊

One shows that

$$X_p(E/K) = \mathrm{Hom}_{\mathbf{Z}_p}(\varinjlim_n \mathrm{Sel}_{p^n}(E/K), \mathbf{Q}_p/\mathbf{Z}_p)$$

called the Pontyragin dual of the p^∞ Selmer group is a finitely generated $\mathbf{Z}_p$-module. The associated $\mathbf{Q}_p$-vector space, denoted $\mathcal{X}_p(E/K) = X_p(E/K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ has dimension rk_p.

Definition 1.35 rk_p is called the p^∞-Selmer rank of E/K and satisfies

$$\mathrm{rk}_p = \mathrm{rk}(E/K) + \delta_p.$$

◊

So if Ш is finite then $\delta_p = 0$ for all p. Use BSD to compute parity of rk_p.

Lecture ? 19/3/2018

1.3 Consequences of BSD

Consider $E/\mathbf{Q}$: Mordell-Weil implies that

$$E(\mathbf{Q}) \simeq \mathbf{Z}^{\mathrm{rk}} \oplus \text{torsion}$$

then BSD 1 says that

$$\underbrace{\mathrm{ord}_{s=1} L(E,s)}_{\mathrm{rk}_{\mathrm{an}}} = \mathrm{rk}\,,$$

functional equation for $L(E,s)$.

$$L^*(E,s) = wL^*(E, 2-s)$$

with $w \in \{\pm 1\}$ the sign of the functional equation. If $w = 1$ then $L(E,s)$ is (essentially) symmetric at $s = 1$. So $\mathrm{ord}_{s=1} L(E,s)$ is even. If $w = -1$ then $\mathrm{ord}_{s=1} L(E,s)$ is odd.

We get BSD mod 2:

$$(-1)^{\mathrm{rk}} = w(\text{sign of f.e.})$$

a conjecture based on conjecture is bad so we go one step further.

Theorem 1.36 *The sign in the functional equation of $L(E,s)$ is equal to the global root number of E.*

This is defined by

$$w_\infty \prod_p w_p,$$

the local root numbers defined in terms of the local galois representations. Non-trivial to understand, but manageable.

Conjecture 1.37 **Parity conjecture.**

$$(-1)^{\mathrm{rk}} = \prod_v w_v = w.$$

Example 1.38
$$E/\mathbf{Q}\colon y^2 + y = x^3 + x^2 - 7x + 5$$
$$\Delta_E = -7 \cdot 13$$
$w_v = 1$ if $v \nmid \infty 7 \cdot 13$
$$w_\infty = -1$$
(in general -1^g where g is dimension of the abelian variety).
$$w_7 = -1$$
$$w_{13} = -1$$
so $w = -1$ and the rank is odd, hence there is a point of infinite order on this curve. □

Problem. On the one hand $\prod_v w_v$ is computable. On the other hand $(-1)^{\mathrm{rk}}$ is precisely unknown.
$$(-1)^{\mathrm{rk}} = \prod_v w_v.$$
Theorem 1.39 *Assume* Ш *is finite, let* $\phi\colon E \to E'$ *be an isogeny whose degree is not divisible by* char(K)*, then*
$$\frac{|\,Ш_E\,| \mathrm{Reg}_E \prod_p c_p \Omega_E}{|E_{\mathrm{tors}}|^2} = \frac{|\,Ш_{E'}\,| \mathrm{Reg}_{E'} \prod_p c'_p \Omega_{E'}}{|E'_{\mathrm{tors}}|^2}.$$
Remark 1.40 In fact this is true for all abelian varieties over K.

Example 1.41 Let
$$E/\mathbf{Q}\colon y^2 + xy = x^3 - x$$
http://www.lmfdb.org/EllipticCurve/Q/65/a/1. $\Delta_E = 5 \cdot 13$, it has a 2-isogenous curve E'.

Compute
$$c_5 = c_{13} = 1$$
$$c'_5 = c'_{13} = 2$$
$$\Omega_E = 2\Omega_{E'}$$
then
$$\frac{\mathrm{Reg}_{E'}}{\mathrm{Reg}_E} = \frac{|\,Ш_E\,||E'_{\mathrm{tors}}|^2 \prod_p c_p \Omega_E}{|\,Ш_{E'}\,||E_{\mathrm{tors}}|^2 \prod_p c'_p \Omega_{E'}} \equiv \square \frac{2}{4} \neq 1 \square.$$
So $\mathrm{Reg}_E \neq 1$, $\mathrm{Reg}_{E'} \neq 1$ so E has at least one rational point of infinite order, so rk ≥ 1. □

Lemma 1.42 *Assume* Ш *is finite, let*
$$\phi\colon E/K \to E'/K$$
be a K-rational isogeny of degree d.

Write $n = \mathrm{rk}_E = \mathrm{rk}_{E'}$. *Pick a basis* $\Lambda = \langle P_1, \ldots, P_n \rangle$ *for*
$$E(K)/\mathrm{tors}$$
write Λ' *for a basis of* $E'(K)/\mathrm{tors}$. *Write* $\phi^\vee\colon E' \to E$ *for the dual isogeny s.t.* $\phi\phi^\vee = [d]$.

using the following fact
$$\left\langle \phi(P), Q \right\rangle_{E'} = \left\langle P, \phi^\vee(Q) \right\rangle_E$$

Then

$$\begin{aligned} d^n \operatorname{Reg}_E &= \det(\langle dP_i, P_j\rangle_E)_{i,j} \\ &= \det(\langle \phi^\vee \phi P_i, P_j\rangle_E) = \det(\langle \phi P_i, \phi P_j\rangle_{E'}) \\ &= \operatorname{Reg}_{E'}[\Lambda' : \phi(\Lambda)]^2. \end{aligned}$$

Back to the example

$$\frac{\operatorname{Reg}_E}{\operatorname{Reg}_{E'}} \equiv \frac{1}{2}\square$$

so by the lemma rk is odd. Here we assumed that Ш is finite for elliptic curves, one can drop the assumption of finiteness of Ш to get unconditional results on the parity of rk_p for all p.

Conjecture 1.43 ***p*-parity.**

$$(-1)^{\mathrm{rk}_p} = w.$$

This is known over $\mathbf{Q}$ and totally real fields.

How to compute the parity of $\mathrm{rk}_p(E/K)$? Need BSD-invariance for Selmer groups. (Details T. and V. Dokchitser "On the BSD quotients modulo squares", and Milne "Arithmetic duality theorems")

Definition 1.44 For an isogeny

$$\Psi \colon A \to B$$

of abelian varieties over K. Let

$$Q(\Psi) = |\operatorname{coker}(\Psi \colon A(K)/A(K)_{\mathrm{tors}} \to B(K)/B(K)_{\mathrm{tors}})| \cdot |\ker(\psi \colon Ш(A)_{\mathrm{div}} \to Ш(B)_{\mathrm{div}})|.$$

◊

Recall $\mathrm{rk}_p = \mathrm{rk} + \delta_p$ where

$$Ш = \bigoplus Ш_{p^\infty}$$

and

$$\begin{aligned} Ш_{p^\infty} &\simeq (\mathbf{Q}_p/\mathbf{Z}_p)_p^\delta \oplus T_p \\ Ш_{\mathrm{div}} &= \bigoplus (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p}. \end{aligned}$$

Strategy, we show that for Ψ an isogeny s.t. $\Psi\Psi^\vee = [p]$. Then

$$p^{\mathrm{rk}_p(E/K)} \equiv \frac{Q(\Psi^\vee)}{Q(\Psi)} \equiv \frac{\prod_v c_p}{\prod_v c'_v}\frac{\Omega_E}{\Omega_{E'}} \pmod{K^{\times 2}}.$$

Remark 1.45 Let $A^\vee$ be the dual of A. $A^\vee = \operatorname{Pic}^0(A)$.

So

$$(-1)^{\mathrm{rk}_p(E/K)} = (-1)^{\operatorname{ord}_p\left(\frac{\prod_v c_v \Omega_E}{\prod_v c'_v \Omega_{E'}}\right)}$$

the parity of $\mathrm{rk}_p(E/K)$ is computable from local invariants of E and E'.

To prove the p-parity conjecture it remains to prove

$$(-1)^{\operatorname{ord}_p\left(\frac{\prod_v c_v \Omega_E}{\prod_v c'_v \Omega_{E'}}\right)} = \prod_v w_v.$$

Lecture ? 21/3/2018

Aside: Generalisation of the definition of $\mathrm{Sel}^n(E/\mathbf{Q})$**.** Consider

$$\Psi\colon A \to B$$

an isogeny of abelian varieties. We have

$$0 \to A(K)[\Psi] \to A(K) \xrightarrow{\Psi} B(K) \xrightarrow{\delta} H^1(G_K, A[\Psi]) \to H^1(G_K, A) \xrightarrow{\Psi} H^1(G_K, B)$$

from which we extract

$$0 \to B(K)/\Psi(A(K)) \xrightarrow{\delta} H^1(G_K, A[\Psi]) \to H^1(G_K, A)[\Psi] \to 0$$

$$0 \to \prod_v B(K_v)/\Psi(A(K_v)) \xrightarrow{\delta} H^1(G_{K_v}, A[\Psi]) \to \prod_v H^1(G_K, A)[\Psi] \to 0$$

we then define

$$\mathrm{Sel}^{(\Psi)}(A/K) = \ker\left\{H^1(G_K, A[\Psi] \to \prod_v H^1(G_{K_v}, A)\right\}$$

$$\text{Ш}(A/K) = \ker\left\{H^1(G_K, A) \to \prod_v H^1(G_{K_v}, A)\right\}$$

so

$$0 \to \underbrace{B(K)/\Psi(A(K))}_{\mathrm{coker}(\Psi\colon A(K) \xrightarrow{\Psi} B(K))} \to \mathrm{Sel}^{(\Psi)}(A/K) \to \text{Ш}(A/K) \to 0.$$

We want to show:

Theorem 1.46 *Let E/K be an elliptic curve, K a number field, if Ψ is s.t. $\Psi\Psi^\vee = [p]$ then*

$$p^{\mathrm{rk}_p(E/K)} \equiv \frac{Q(\Psi)}{Q(\Psi^\vee)} \equiv \frac{\prod_v c_p}{\prod_v c'_v} \frac{\Omega_E}{\Omega_{E'}} \pmod{K^{\times 2}}$$

We will show this in 3 parts, first the left, then the right, then the equality with the global root number.

Step 1. Proposition 1.47

$$p^{\mathrm{rk}_p(E/K)} \equiv \frac{Q(\Psi)}{Q(\Psi^\vee)} \pmod{K^{\times 2}}$$

Proof. Note that

$$Q(\Psi \circ \Psi^\vee) = Q(\Psi)Q(\Psi^\vee)$$

hence

$$\frac{Q(\Psi)}{Q(\Psi^\vee)} \equiv \underbrace{Q(\Psi)Q(\Psi^\vee)}_{=Q([p])} \pmod{K^{\times 2}}$$

now

$$|\,\mathrm{coker}([p]\colon E(K)/E(K)_{\mathrm{tors}} \to E'(K)/E'(K)_{\mathrm{tors}})| = p^{\mathrm{rk}(E/K)}$$

Proof of this: For each generator R of $E(K)/E(K)_{\mathrm{tors}}$ then

$$\frac{1}{p}R, \frac{2}{p}R, \ldots, \frac{p-1}{p}R, R$$

are not in the image of $[p]$ which implies the size is $p^{\mathrm{rk}(E/K)}$. Also

$$|\ker([p]\colon\ \text{Ш}(E/K)_{\mathrm{div}} \to \text{Ш}(E'/K)_{\mathrm{div}})| = p^{\delta_p}$$

since

$$\text{III}(E/K)_{\text{div}} = \bigoplus_p (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p}$$

and since $[p]$ is trivial on all

$$(\mathbf{Q}_l/\mathbf{Q}_l)^{\delta_l},\ l \neq p$$

then look at $[p]\colon (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p} \to (\mathbf{Q}_p/\mathbf{Z}_p)^{\delta_p}$ if $x \in \mathbf{Q}_p/\mathbf{Z}_p$ and $\ker[p]$ then $px \in \mathbf{Z}_p \implies x = a/p$ for $a \in \mathbf{F}_p$. so

$$p^{\delta_p}.$$

■

Step 2. We show that

$$\frac{Q(\Psi)}{Q(\Psi^\vee)} \equiv \frac{\prod_v c_p}{\prod_v c_v'} \frac{\Omega_E}{\Omega_{E'}} \pmod{K^{\times 2}}.$$

Theorem 1.48 *Let $A, B/K$ be abelian varieties given with a non-zero global exterior form ω_A, ω_B. Suppose*

$$\Psi\colon A \to B$$

is an isogeny and

$$\Psi^\vee\colon B^\vee \to A^\vee$$

its dual.

Let $\text{III}_0(A/K)$ denote $\text{III}(A/K)$ mod its divisible part. And

$$\Omega_A = \prod_{v|\infty,\ real} \int_{A(K_v)} |\omega_A| \prod_{v|\infty,\ complex} 2^{\dim A} \int_{A(K_v)} \omega_A \wedge \overline{\omega_A}.$$

Then

$$\frac{Q(\Psi^\vee)}{Q(\Psi)} = \frac{|B(K)_{\text{tors}}||B^\vee(K)_{\text{tors}}|}{|A(K)_{\text{tors}}||A^\vee(K)_{\text{tors}}|} \frac{\prod_v c_p(A/K)}{\prod_v c_v(B/K)} \frac{\Omega_A}{\Omega_B} \prod_{p|\deg\Psi} \frac{|\text{III}_0(A)[p^\infty]|}{|\text{III}_0(B)[p^\infty]|}.$$

Remark 1.49 If $A = E$, $B = E'$ with Ψ s.t. $\Psi\Psi^\vee = [p]$ then

$$E \simeq E^\vee,\ E' \simeq E'^\vee$$

and $|\text{III}_0| = \square$.

$$\frac{Q(\Psi^\vee)}{Q(\Psi)} \equiv \frac{\prod_v c_p}{\prod_v c_v'} \frac{\Omega_E}{\Omega_{E'}} \pmod{K^{\times 2}}.$$

Sketch proof of theorem. We show how to obtain the quotient of Tamagawa numbers, for a sufficiently large set of places S of K

$$\frac{Q(\Psi^\vee)}{Q(\Psi)} \frac{|\text{III}[\Psi^\vee]|}{|\text{III}[\Psi]|} = \prod_{v\in S} \frac{|\ker\Psi_v|}{|\ker\Psi_v^\vee|}$$

where Ψ_v is the induced map on $E(K_v) \to E'(K_v)$. If $v \nmid \infty$ and $v \in S$ what is

$$\frac{|\ker\Psi_v|}{|\operatorname{coker}\Psi_v|}?$$

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & 0 \arrow[d] & \ker\Psi_v \arrow[d] & H_1 \arrow[d] & \\
0 \arrow[r] & E_1(K_v) \arrow[r] \arrow[d] & E(K_V) \arrow[r] \arrow[d] & E(K_v)/E_1(K_v) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E_1'(K_v) \arrow[r] \arrow[d] & E'(K_V) \arrow[r] \arrow[d] & E'(K_v)/E_1'(K_v) \arrow[r] \arrow[d] & 0 \\
 & 0 & \operatorname{coker}\Psi_v & H_2 &
\end{tikzcd}$$

Snake lemma gives

$$0 \to \ker\Psi_v \to H_1 \to 0 \to \operatorname{coker}\Psi_v \to H_2 \to 0$$

$$\implies |\ker\Psi_v| = |H_1|$$

and

$$|\operatorname{coker}\Psi_v| = |H_2|.$$

Also

$$\left|\frac{E(K_v)/E_1(K_v)}{H_1}\right| = \left|\frac{E'(K_v)/E_1'(K_v)}{H_2}\right|.$$

Moreover since E, E' are isogenous we have

$$|\widetilde{E}_{\mathrm{ns}}(\bar{k})| = |\widetilde{E}'_{\mathrm{ns}}(\bar{k})|$$

hence since

$$0 \to E_1(K_v) \to E_0(K_v) \to \widetilde{E}_{\mathrm{ns}}(\bar{k}) \to 0$$

similarly for E'. We have

$$|E_0(K_v)/E_1(K_v)| = |E_0'(K_v)/E_1'(K_v)|$$

$$\implies \left|\frac{E'(K_v)/E_1'(K_v)}{E(K_v)/E_1(K_v)}\right| = \left|\frac{E'(K_v)/E_0'(K_v)}{E(K_v)/E_0(K_v)}\right| = \frac{c_v}{c_v'}.$$

■

Hence

$$(-1)^{\mathrm{rk}_p(E/K)} = (-1)^{\mathrm{ord}_p\left(\prod_v \left|\frac{\operatorname{coker}\Psi_v}{\ker\Psi_v}\right|\right)}$$

$$= (-1)^{\mathrm{ord}_p\left(\frac{\prod_v c_v'}{\prod_v c_v} \underbrace{\prod_{v|\infty}\left|\frac{\operatorname{coker}\Psi_v}{\ker\Psi_v}\right|}_{\Omega_E/\Omega_{E'}}\right)}.$$

Step 3. We need to show that

$$(-1)^{\mathrm{rk}_p(E/K)} = w_E \text{ (p-parity)}$$

i.e. we need to show that

$$(-1)^{\mathrm{ord}_p\left(\frac{\prod_v c'_v}{\prod_v c_v}\frac{\Omega_E}{\Omega_{E'}}\right)} = w_E$$

Strategy:

$$(-1)^{\mathrm{ord}_p\left(\frac{\prod_v c'_v}{\prod_v c_v}\frac{\Omega_E}{\Omega_{E'}}\right)} = \prod_{v\nmid\infty}(-1)^{\mathrm{ord}_p\frac{c'_v}{c_v}}\prod_{v|\infty}(-1)^{\mathrm{ord}_p\left|\frac{\ker\Psi_v}{\operatorname{coker}\Psi_v}\right|}$$

and relate

$$(-1)^{\mathrm{ord}_p\frac{c'_v}{c_v}}$$

to w_v for $v\nmid\infty$ and

$$(-1)^{\mathrm{ord}_p\left|\frac{\ker\Psi_v}{\operatorname{coker}\Psi_v}\right|}$$

to w_v for $v \mid \infty$.

Then take product over all places.

Lecture ? 26/3/2018

Let E/K be an elliptic curve admitting an isogeny Ψ of degree p (defined over K). Recall that we proved

$$p^{\mathrm{rk}_p(E/K)} = \prod_v \frac{c_v}{c'_v}\frac{\Omega_E}{\Omega_{E'}}$$

v missing p. More precisely

$$p^{\mathrm{rk}_p(E/K)} \equiv \prod_{v|p\infty}\frac{c_v}{c'_v}\prod_{v|\infty}\left|\frac{\ker\psi_v}{\operatorname{coker}\psi_v}\right|$$

where ψ_v is the map induced by ψ on $E(K_v)$.

What about $v|p$ to extract

$$\frac{c_v}{c'_v}$$

from

$$\left|\frac{\ker\psi_v}{\operatorname{coker}\psi_v}\right|$$

at finite places we can use a diagram involving

$$0 \to E_1(K_v) \to E'_1(K_v) \to \operatorname{coker} \to 0.$$

If $v \nmid p$ then $|\operatorname{coker}| = 1$ since then on the level of the formal group ψ induces a map

$$\begin{aligned}\hat{\psi}\colon \hat{E}(\mathfrak{m}_K) &\to \hat{E}'(\mathfrak{m}_K)\\ T &\mapsto aT + \cdots\end{aligned}$$

power series rep of ψ $\psi(x,y) = (x',y')$ Silverman IV cor 4.3/ $\omega'\circ\psi = \psi'\circ\omega$. with leading $a = \psi^*\omega'/\omega\times$ unit $\in \mathcal{O}_K$.

$$\implies aa' = p \in \mathcal{O}_K^\times \implies \hat{\psi} \text{ isom.}$$

If $v|p$ then coker contributes to the snake lemma and at that place

$$\frac{c_v}{c'_v}\left|\frac{\psi^*\omega'}{\omega}\right|_v = \frac{c_E}{c'_E}\left|\frac{\omega}{\omega_v^0}\right|_v$$

for a particular choice of ω.

Proving p-parity. To prove the p-parity conjecture

$$(-1)^{\mathrm{rk}_p(E/K)} = w_E.$$

We will show that

$$(-1)^{\mathrm{ord}_p \prod_v \frac{c_v}{c'_v} \frac{\Omega}{\Omega_{E'}}} = w_E$$

by relating

$$(-1)^{\mathrm{ord}_p \frac{c_v}{c'_v}}$$

and w_v at some place $v \nmid p\infty$

$$(-1)^{\mathrm{ord}_p \frac{\Omega_E}{\Omega_{E'}}} = (-1)^{\mathrm{ord}_p \left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|}$$

and w_v at $v|\infty$.

We only sketch these steps for $v \nmid p$ and E is semistable at v.

The proofs of p-parity for p odd and $p = 2$ are different.

p odd. The p-parity conjecture is proven for principally polarized abelian varieties with a p-cyclic isogeny with $p \geq 2g + 2$ or $p \geq 2$ and semistable reduction and some local constraints at $v|p$. see Root numbers selmer groups and non-commutative Iwasawa theory, Coates, Fukaya, Kato, Sujatha

Sketch, for an elliptic curve with a p-isogeny ψ we look at $v|\infty$ where $w_v = -1$, and

$$(-1)^{\mathrm{ord}_p \left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|}$$

if v is complex $|\ker \psi_v| = p$ $|\operatorname{coker} \psi_v| = 1$. so

$$(-1)^{\mathrm{ord}_p \left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|} = -1 = w_v.$$

If $v|\infty$ is real what does $E(\mathbf{R})$ look like? Either there is a real period and so two real components, and all real p-torsion (if any) is on the identity component. Or there is no real period and only 1 real component that contains all real p-tors if any.

1. $|\ker \psi_v| = p$ (the p-tors in $\ker \psi$ are real)
2. $|\ker \psi_v| = 1$ (the p-tors in $\ker \psi$ are not real)

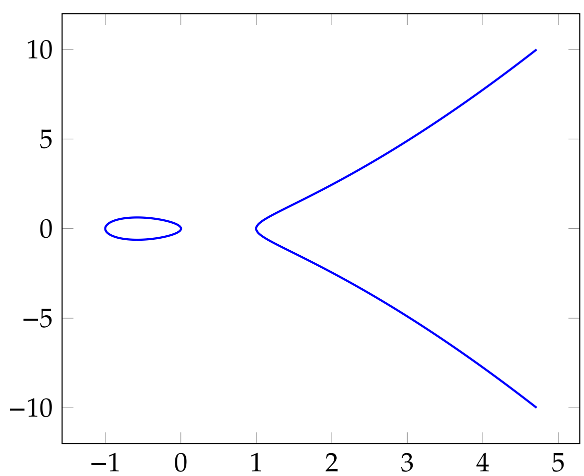

Figure 1.50

Moreover $|\operatorname{coker}\psi| = 1$ always, $\operatorname{sgn}(\Delta_E) = \operatorname{sgn}(\Delta_{E'})$

More generally if $\deg \Psi$ is odd then

$$E'(\mathbf{R})/\psi(E(\mathbf{R})) \hookrightarrow H^1(\mathrm{Gal}(\mathbf{C}/\mathbf{R}), E[\psi]) = 0$$

since $[\mathbf{C}:\mathbf{R}] = 2$ is coprime to $E[\psi]$ (see Atiyah's book).

In the first case

$$(-1)^{\operatorname{ord}_p\left|\frac{\ker\psi_v}{\operatorname{coker}\psi_v}\right|} = -1 = w_v$$

In the second case

$$(-1)^{\operatorname{ord}_p\left|\frac{\ker\psi_v}{\operatorname{coker}\psi_v}\right|} = 1 \neq w_v$$

For K a local field let $F = K(\ker\psi_v)$ noting that

$$\mathrm{Gal}(F/K) \hookrightarrow (\mathbf{Z}/p\mathbf{Z})^\times$$

from its action on points in $\ker\psi = F/K$ is cyclic.

Consider the composition

$$F^\times \xrightarrow{\text{local rec.}} \mathrm{Gal}(F/K) \hookrightarrow (\mathbf{Z}/p)^\times.$$

and denote

$$(-1, F/K)$$

the image of -1 under the above map.

$$(-1, F/K) = \begin{cases} 1 & \text{if } -1 \text{ is a norm from } F \text{ to } K, \\ -1 & \text{otw} \end{cases}$$

this is the Artin symbol.

This is perfect as they cancel out globally.

If v is complex then $F = \mathbf{C}$, $K = \mathbf{C}$ and $(-1, F/K) = 1$

If v is real and $|\ker\psi_v| = p$ then $F = \mathbf{R}$, $K = \mathbf{R}$ and $(-1, F/K) = 1$

If v is real and $|\ker\psi_v| = 1$ then $F = \mathbf{R}$, $K = \mathbf{R}$ and $(-1, F/K) = -1$

$p = 2$. Note that $(-1, F/K) = 1$ for all places of K since if E admits a 2-isogeny ψ/K then is admits a 2-torsion point over K.

Hence $F = K(\ker\psi_v) = K$

set -up

$$E/K$$

with a 2-isogeny ψ/K

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

by translating 2-torsion to (0,0)

$$\psi\colon E \to E' : y^2 = x(x^2 - 2ax + \delta)$$

where $\delta = a^2 - 4b = \mathrm{disc}(x^2 + ax + b)$ if $\delta > 0$ then $E(\mathbf{R})$ has two connected components. $\delta < 0$ only 1. Have $16b = \mathrm{disc}(x^2 - 2ax + \delta)$ likewise for E'

$$\begin{tikzcd}
 & & 0 \arrow[d] & & \\
 & \ker \psi_v^0 0 \arrow[d] & \ker \psi_v \arrow[d] & \ker \psi_/ \arrow[d] & \\
0 \arrow[r] & E^0(\mathbf{R}) \arrow[r] \arrow[d] & E(\mathbf{R}) \arrow[r] \arrow[d] & E(\mathbf{R})/E^0(\mathbf{R}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E'^0(\mathbf{R}) \arrow[r] \arrow[d] & E'(\mathbf{R}) \arrow[r] \arrow[d] & E'(\mathbf{R})/E'^0(\mathbf{R}) \arrow[r] \arrow[d] & 0 \\
 & \operatorname{coker} \psi_v^0 & \operatorname{coker} \Psi_v & \operatorname{coker} \psi_/ &
\end{tikzcd}$$

by snakey

$$\frac{|\ker \psi_v^0||\ker \psi_/||\ker \psi|}{|\ker \psi_v||\operatorname{coker} \psi_v^0||\operatorname{coker} \psi_/|} = 1$$

$$\implies \left|\frac{\operatorname{coker} \psi_v}{\ker \psi_v}\right| = \frac{|\operatorname{coker} \psi_v^)||\operatorname{coker} \psi_/|}{|\ker \psi_v^0||\ker \psi_/|}$$

let $n(E), n(E')$ be the number of real connected components $n = E(\mathbf{R})/E^0(\mathbf{R})$

By the third column

$$\frac{n(E')}{n(E)} \frac{|\ker \psi_/|}{\operatorname{coker} \psi_/|} = 1$$

now $|\operatorname{coker} \psi_v^0| = 1$ as the map on identity component is surjective. hence

$$\left|\frac{\operatorname{coker} \psi_v}{\ker \psi_v}\right| = \frac{n(E')}{n(E)|\ker \psi_v^0|}$$

Lecture ? 28/3/2018

Recall: to prove the 2-parity conjecture for E/K

$$(-1)^{\mathrm{rk}_2(E)} = w????????????????????$$

missed

Notation

$$E\colon y^2 = x(x^2 + ax + b) = xq_1(x)$$

$$E'\colon y^2 = x(x^2 - 2ax + \delta) = xq_2(x),\ \delta = a^2 - 4b$$

$\mathrm{disc}(q_1(x)) = \delta$ $\mathrm{disc}(q_2(x)) = 16b$

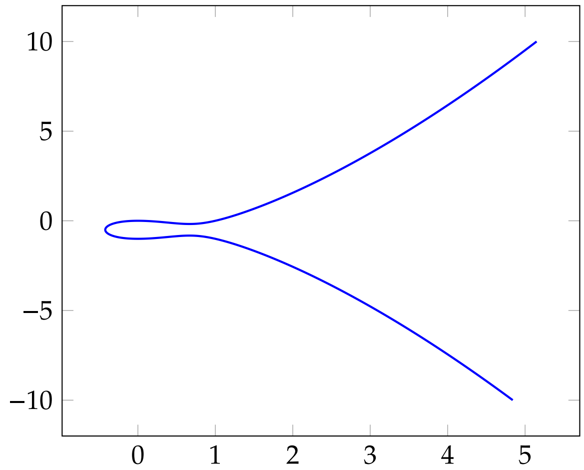

Figure 1.51

a) If $\delta > 0, b > 0$ then E, E' both have two real components, $n(E) = n(E') = 2$.

$$|\ker \psi_v^0| = \begin{cases} 1 & \text{if } (0,0) \text{ is not on } E^0(\mathbf{R}) \\ 2 & \text{if } (0,0) \text{ is on } E^0(\mathbf{R}) \end{cases} = \begin{cases} 1 & \text{if } a < 0 \\ 2 & \text{if } a > 0 \end{cases}$$

write $q_1(x) = x^2 + ax + b = (x-\alpha)(x-\beta)$ then if $(0,0) \in E^0(\mathbf{R})$, $\alpha, \beta < 0$ but $a = -\alpha - \beta$ hence in this case $a > 0$.

$$(-1)^{\operatorname{ord}_2\left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|} = \begin{cases} 1 & \text{if } a < 0 \\ -1 & \text{if } a > 0 \end{cases}$$

so we need some correction if $\delta > 0, b > 0, a < 0$.

b) If $\delta > 0, b < 0$ E has two real components and E' only 1 $n(E) = 2, n(E') = 1$.

$$|\ker \psi_v^0| = 1$$

since $b < 0$ and $b = \alpha\beta$.

$$(-1)^{\operatorname{ord}_2\left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|} = -1$$

so no correction if $\delta > 0, b < 0$.

c) If $\delta < 0, b > 0$, $n(E) = 1, n(E') = 2$.

$$|\ker \psi_v^0| = 2$$

and

$$(-1)^{\operatorname{ord}_2\left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|} = 1$$

need correction if $\delta < 0, b > 0$.

d) $b < 0, \delta < 0$ contradiction, $\delta = a^2 - 4b$.

So in summary if $\delta > 0, b > 0, a < 0$ or $\delta < 0, b > 0$ need a correction, if $\delta > 0, b > 0, a > 0$ or $\delta > 0, b < 0$ no correction.

$$(-1)^{\operatorname{ord}_2\left|\frac{\ker \psi_v}{\operatorname{coker} \psi_v}\right|} =? w_v$$

First guess

$$(a, -b)(-a, \delta)$$

Recall: let K be a local field

$$K^\times \times K^\times \to \{\pm 1\}$$

$$(a,b) \mapsto \begin{cases} 1 & \text{if } a \text{ is a norm from } K(\sqrt{b}) \to K, \\ -1 & \text{otw} \end{cases}$$

If K is archimidean $(a,b) = -1 \iff a < 0, b < 0$. If K is non-archimidean with odd residue characteristic then

$$(\text{unit}, \text{unit}) = 1$$

$$(\text{unit}, \pi^n) = -1$$

if n odd and unit is not a square.

$$(a, bc) = (a,b)(a,c).$$

So guess

$$(a,-b)(-a,\delta)$$

works over **R**.

$v \nmid 2\infty$ need to show that

$$(-1)^{\operatorname{ord}_2 \frac{c_v}{c'_v}} = (a,-b)(-a,\delta) w_v$$

if E has good reduction at v.

$$c_v = c'_v = 1.$$

Need to show that

$$(a,-b)(-a,\delta) = 1.$$

Since E, E' have good reduction at v. then b, δ are units in K. If $a \in \mathcal{O}_K^\times$ then $(a,-b)(-a,b) = 1$ if $a \equiv 0 \pmod{\pi_K}$ then since $a^2 - 4b = \delta$ then $\delta \equiv -4b \pmod{\pi_K}$.

If E has split multiplicative reduction, (multiplicative reduction is when $y^2 = f(x)$ and $f(x)$ has a double root mod π_K, any two distinct tangents at the node, both defined over k (fixed by frob)). so E' also has split multiplicative reduction as ψ commutes with frobenius.

Need to compute

$$\frac{c_v}{c'_v}$$

by Tates algorithm

$$c_E = v(\Delta_E) = n$$

we show that

$$c_{E'} = v(\Delta_{E'}) = \begin{cases} 2n, \\ \frac{1}{2} n \end{cases}$$

Recall

$$E\colon y^2 = \overbrace{x(x^2 + ax + b)}^{f_E(x)} = x(x-\alpha)(x-\beta) = xq_1(x)$$

$$\Delta_{f_E} = \alpha^2\beta^2(\alpha-\beta)^2 = b^2(\alpha-\beta)^2 = b^2\delta$$

$$E'\colon y^2 = \overbrace{x(x^2 - 2ax + \delta)}^{f_{E'}(x)} = x(x-A)(x-B) = xq_2(x)$$

$$\Delta_{f_{E'}} = A^2B^2(A-B)^2 = \delta^2(A-A)^2 = \delta^2 16b$$

if $v(\delta) = n$ then $v(\Delta_{f_E}) = n$ so $c_E = -n$ and $v(\Delta_{f_{E'}}) = 2n$ so $c_{E'} = 2n$ in general if E admits a p-isogeny and E has split multiplicative reduction then

$$\frac{c_E}{c_{E'}} = p^{\pm 1}.$$

here $w_v = -1$ and

$$(-1)^{\mathrm{ord}_2 \frac{c_E}{c_{E'}}} = -1$$

need to show that

$$(a, -b)(-a, \delta) = 1$$

if E has a double root at $(0,0)$ wlog $\alpha \equiv 0 \pmod{\pi}_K$ then $v(\delta) = 0$, $v(b) > 0$ and both slopes of tangent at $(0,0)$ are defined over k.

Taylor expansion at $(0,0)$

$$\begin{aligned} f(x,y) &= y^2 - x^3 - ax^2 - bx \\ &= (y - s_1x)(y - s_2x) + h.o.t. \\ &= y^2 - xy(s_1+s_2) + s_1s_2x^2 + h.o.t. \end{aligned}$$

so $s_1 = -s_2$ and $s_1s_2 = -a$ implies $s_1^2 = a$.

so $s_1 \in k^\times$ then $a \in k^{\times 2}$

$$(a, -b) = 1 \implies (-a, \delta) = 1$$

as both are units.

Now $b = \alpha\beta \equiv 0 \pmod{\pi_K}$ so

$$x^2 - 2ax + \delta \equiv (a - A)^2 \pmod{\pi_K}$$

same Taylor expansion gives

$$\begin{aligned} f(x,y) &= y^2 - x^3 + 2ax^2 - \delta x \\ = f(x,y) - f(A,0) &= (y - s_3(x-A))(y - s_4(x-A)) + h.o.t. \end{aligned}$$

so $s_3 = -s_4$ and $s_3s_4 = 2a$, $s_3^2 = -2a$ hence

$$(a, -b)(-2a, \delta)$$

split multiplicative

$$-2a \in K^{\times 2},$$

So we should use this Hilbert symbol instead, it doesn't change the real case.

If E has non-split multiplicative reduction

$$\frac{c_E}{c_{E'}} = \begin{cases} 1, & \text{if } v(\Delta_E), v(\Delta_{E'}) \text{ even} \\ 2, & \text{if } v(\Delta_{E'}) \text{ odd} \\ \frac{1}{2} & \text{if } v(\Delta_E) \text{ odd} \end{cases}$$

$$\implies (-1)^{\mathrm{ord}_2 \frac{c_E}{c_{E'}}} = \begin{cases} 1, \\ -1, \\ -1, \end{cases}$$

done since $a, -2a$ precisely not squares.

What are these invariants purely in theory?

2 Abelian varieties

Lecture ? 2/4/2018

What about generalising this method to abelian varieties?

For p odd Coates et. al. (ppav with p-cyclic isogenies and local constraints)

For $p = 2$.

Recall let $X, Y/K$ be abelian varieties over a number field and suppose that $\Psi\colon X \to Y$ is an isogeny, then $\Psi^\vee\colon Y^\vee \to X^\vee$ its dual. Then

$$\frac{Q(\Psi^\vee)}{Q(\Psi)} = \frac{|Y(K)_{\text{tors}}|}{|X(K)_{\text{tors}}|}\frac{|Y^\vee(K)_{\text{tors}}|}{|X^\vee(K)_{\text{tors}}|}\frac{\prod_v c(X/K_v)}{\prod_v c(Y/K_v)}\frac{\Omega_X}{\Omega_Y}\prod_{p\mid\deg\Psi}\frac{|Ш_0(X)[p^\infty]|}{|Ш_0(Y)[p^\infty]|} \tag{2.1}$$

on the other hand we showed that if $\Psi\Psi^\vee = [p]$ then

$$\frac{Q(\Psi^\vee)}{Q(\Psi)} \equiv p^{\text{rk}_p(X/K)} \pmod{K^{\times 2}}$$

note that in this case $\deg\psi = p^{\dim(X)}$.

To be able to use the same method we need to compute the RHS of (2.1).

For E since $E \simeq E^\vee$ and $|Ш_0(E)| = \square$, this only meant computing

$$\prod_v \frac{c(E/k)}{c(E'/k)}\frac{\Omega_E}{\Omega_{E'}}.$$

First consider a ppav X/K s.t.

$$\text{(2.1)} \equiv \frac{\prod_v c(X/K_v)}{\prod_v c(Y/K_v)}\frac{\Omega_X}{\Omega_Y}\frac{|Ш_0(X)[p^\infty]|}{|Ш_0(Y)[p^\infty]|} \pmod{K^{\times\vee}} \tag{2.2}$$

1. Can we compute
$$\frac{\prod_v c(X/K_v)}{\prod_v c(Y/K_v)}\frac{\Omega_X}{\Omega_Y}? \tag{2.3}$$
Leads us to Jacobians of hyperelliptic curves of genus g

2. Can we compute
$$\frac{|Ш_0(X)[p^\infty]|}{|Ш_0(Y)[p^\infty]|}? \tag{2.4}$$
Leads us to Jacobians of hyperelliptic curves of genus g

3. Need an isogeny Ψ of degree 2^g s.t.
$$\Psi\colon J \to J'$$
i.e. the codomain must be a Jacobian of a hyperelliptic curve otherwise we cannot compute 1. or 2.

To satisfy 1., 2. and 3. we take $g = 2$ because of the following:

Theorem 2.1 González, Josep, Jordi Guardia, and Victor Rotger. Abelian surfaces of GL2-type as Jacobians of curves. arXiv preprint math/0409352 (2004). *Let A/K be a principally polarized abelian surface defined over a number field. Then A is one of the following types*

- $$A/K \simeq_K J(C)$$
  where C/K is a smooth genus 2 curve.

- $$A/K \simeq_K C_1 \times C_2$$

  where $C_1, C_2/K$ are elliptic curves defined over K.

- $$A/K \simeq_K \mathrm{Res}_{F/K} C$$

  where $\mathrm{Res}_{F/K} C$ is the Weil restriction of an elliptic curve defined over a quadratic extension F/K.

Remark 2.2 The parity of the rank of A/K in the last two cases can be computed from that of the underlying elliptic curves.

We will concentrate on $A \simeq_K J(C)$,

$$C\colon y^2 = f(x)$$

for $\deg(f) = 6$.

The generalisation of a 2-isogeny is called a Richelot isogeny.

Plan:

1. Review of hyperelliptic curves and their Jacobians.
2. Richelot isogeny
3. Compute contribution of the real places
4. Compute Tamagawa numbers/local root numbers
5. Compute $|\text{Ш}_0(J)[2^\infty]|$ up to squares
6. Find and prove the right error term

2.1 Review of hyperelliptic curves and Jacobians

See Stoll's notes.

By a hyperelliptic curve C over a number field K given my

$$C/K\colon y^2 = f(x)$$

of genus g where $f(x) \in K[x]$ of degree $2g+1$ or $2g+2$ with no multiple roots, we mean the pair of affine patches

$$U_x\colon y^2 = f(x)$$

$$U_t\colon v^2 = t^{2g+2} f\left(\frac{1}{t}\right)$$

glued together along the maps

$$x = \frac{1}{t},\ y = \frac{v}{t^{g+1}}.$$

We refer to as the points at ∞ (i.e. $C \setminus U_x$) the points with $t = 0$ on U_t.

Explicitly denote by c the leading term of $f(x)$.

If $f(x)$ is of degree $2g+1$ then

$$U_x\colon y^2 = c \prod_{i=1}^{2g+1} (x - r_i)$$

$$U_t\colon v^2 = tc\prod_{i=1}^{2g+1}(tr_i - 1)$$

we denote $P_\infty = (0,1)$ the only point at infinity with $t = 0$.

Otherwise if $f(x)$ is of degree $2g+2$ then

$$U_x\colon y^2 = c\prod_{i=1}^{2g+2}(x - r_i)$$

$$U_t\colon v^2 = c\prod_{i=1}^{2g+2}(tr_i - 1)$$

we denote $P_\infty^\pm = (0, \pm\sqrt{c})$ the two points on U_t with $t = 0$.

Divisors and the picard group. Let G_K be the absolute galois group of K, recall that G_K acts on

$$C(K^{\text{sep}})$$

via its action on coordinates.

Definition 2.3 A divisor D on C is a formal sum

$$\sum_{P\in C(K^{\text{sep}})} n_P P$$

where $n_P \in \mathbf{Z}$ and $n_P = 0$ for all but finitely many $P \in C(K^{\text{sep}})$. The integer n_P is called the multiplicity of P in D and $\deg(D) = \sum_P n_P$ is the degree of D.

Divisors on C are elements of the free abelian group on the set of points $P \in C(K^{\text{sep}})$. Denote by $\operatorname{Div}(C)$ the group of divisors on C. ◊

Definition 2.4 A divisor

$$D = \sum_{P\in C(F)} n_P P$$

for some Galois extension $F|K$. We say it is K-rational, or defined over K if

$$D^\sigma = D\ \forall\sigma \in \operatorname{Gal}(F/K).$$

◊

Example 2.5

$$C\colon y^2 = f(x)$$

$$\alpha \in K$$

$$P = (\alpha, \sqrt{f(\alpha)})$$

$$\bar{P} = (\alpha, -\sqrt{f(\alpha)})$$

then

$$D = P + \bar{P}$$

is a K-rational divisor. □

Definition 2.6 Let f be a non-zero rational function on C. Define

$$[f] = \sum_{P\in C}\operatorname{ord}_P(f)P$$

where the multiplicity of P in $[f]$ is given by the order of vanishing of f at

P. These divisors are called principal divisors, the group of such is denote $\mathrm{Princ}(P)$. Note that these are all of degree 0. ◊

Definition 2.7 The picard group of C is defined to be

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Princ}(P).$$

Note that this inherits a notion of degree from $\mathrm{Div}(C)$. ◊

Theorem 2.8 *Let C be a smooth, projective, absolutely irreducible curve of genus g over some field K. Then there exists an abelian variety J of dimension g over K s.t. for each field*

$$K \subseteq L \subseteq K^{\mathrm{sep}}$$

$$J(L) = \mathrm{Pic}^0_C(L)$$

Definition 2.9 J is called the Jacobian variety of C. ◊

Remark 2.10 J is a projective variety (abelian), thus it can be embedded in some projective space $\mathbf{P}^N$ over K. One can show that

$$N = 4^g - 1$$

always works for hyperelliptic curves.

This is too large to work with an explicit model for J instead we will work with the curve C.

Lecture ? 4/4/2018

Jacobians of genus 2 curves. Let C be a hyperelliptic curve of genus 2 defined over K.

$$C\colon y^2 = f(x)$$

with $f(x) \in K[x]$ of degree 6.

Points on $C(\overline{K})$ and $J(\overline{K})$:

A point D on $J(\overline{K})$ is given by a divisor on C of the form

$$D = P + Q - P_\infty^+ - P_\infty^-$$

for some $P, Q \in C(\overline{K})$. For D to be defined over K either $P, Q \in C(K)$ or $P = Q^\sigma$ for $\sigma \in \mathrm{Gal}(F/K)$ where $[F : K] = 2$.

Remark 2.11 If $P = (x, y)$ and $P' = (x, -y)$ then

$$D = P + Q - P_\infty^+ - P_\infty^-$$

is zero in $J(\overline{K})$.

Addition:

Choose 4 points $P, P', Q, Q' \in C(\overline{K})$ (in general position to make it easier).

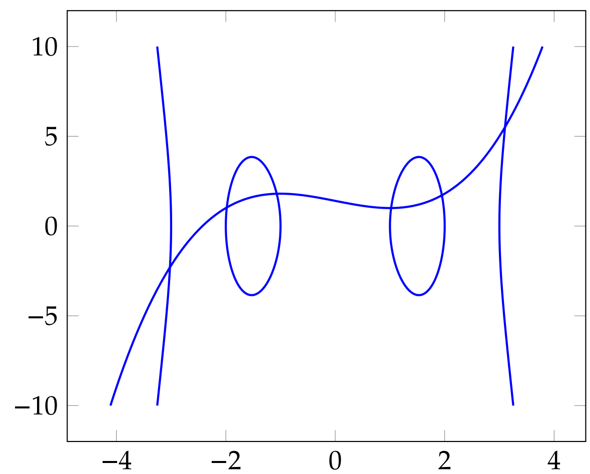

Figure 2.12

We can find a cubic polynomial $y = p(x)$ through the four points. It also intersects at two additional points S, S' so that

$$[y - p(x)] = P + P' + Q + Q' + S + S' - 3P_\infty^+ - 3P_\infty^-$$

$$(P + P' - P_\infty^+ - P_\infty^-) + (Q + Q' - P_\infty^+ - P_\infty^-) = -(S + S' - P_\infty^+ - P_\infty^-)$$

hence

$$\underbrace{[P, P']}_{=P+P'-P_\infty^+-P_\infty^-} + [Q, Q'] = [R, R']$$

where $[R, R'] = -[S, S']$. Where negation is taking negative of all y-coordinates.

So what is 2-torsion?

Lemma 2.13 *Each non-zero element of $J(\overline{K})[2]$ may be uniquely represented by the following pairs of points on $C(\overline{K})$, let $x_1, \ldots, x_6$ be the roots of $f(x)$ then*

$$J(\overline{2})[2] = \{[T_i, T_k], i \neq k\},\ T_i = (x_i, 0) \in C(\overline{K}).$$

Remark 2.14 For the Richelot isogeny ϕ:

$$\begin{tikzcd} J \arrow[r, "\phi"] & J' \arrow[r, "\phi^\vee"] & J \\ C \arrow[u, hook] \arrow[r, "\Gamma"'] & C' \arrow[u, hook] & \end{tikzcd}$$

where $\phi^\vee \circ \phi = [2]$ and Γ is a correspondence.

2.2 Richelot isogenies and the Richelot construction

Richelot isogenies are defined for Jacobians of genus 2 curves, they split multiplication by 2. Their codomain is the Jacobian of a curve, a model of which is explicitly given by the Richelot construction.

Definition 2.15 The Richelot operator. Given two polynomials $P(x), Q(x) \in K[x]$ of degree at most 2 we define the **Richelot operator** $[-,-]$ by

$$[P(x), Q(x)] = P'(x)Q(x) - Q'(x)P(x).$$

◊

Definition 2.16 Richelot polynomials. We say that a polynomial $G(x) \in K[x]$ of degree 5 or 6 is a **Richelot polynomial** over K if we can fix a factorisation

$$G(x) = G_0(x)G_1(x)G_2(x)$$

where each G_i is of degree at most 2, defined over $\overline{K}$ and defined over K as a set.

Write

$$G_i(x) = g_{i2}x^2 + g_{i1}x + g_{i0} = g_i(x - \alpha_i)(x - \beta_i)$$

for its factorisation over $\overline{K}$ and define

$$\Delta_G = \det((g_{ij})_{0\le i,j\le 2}).$$

◊

Definition 2.17 Richelot dual polynomials. To a Richelot polynomial $G(x)$ with a fixed factorisation

$$G(x) = G_0(x)G_1(x)G_2(x)$$

such that $\Delta_G \neq 0$. We associate its **Richelot dual polynomial** $F(x)$ given by

$$F(x) = \prod_{i=1}^{3} F_i(x),\ F_i(x) = \frac{1}{\Delta_G}[G_{i+1}(x), G_{i+2}(x)]$$

where we take indices mod 3. Write $F_i(x) = f_i(x - A_i)(x - B_i)$ ◊

Δ_G may not be defined over K but Δ_G^2 is.

Definition 2.18 Richelot (dual) curves. We say that a hyperelliptic curve C/K of genus 2 is a **Richelot curve** over K if it is given by $y^2 = G(x)$ together with the factorisation

$$G(x) = G_0(x)G_1(x)G_2(x)$$

as a Richelot polynomial over K such that $\Delta_G \neq 0$.

To a Richelot curve C/K we associate its **Richelot dual curve** $\widehat{C}$ given by

$$\widehat{C}\colon\ y^2 = F(x)$$

where $F(x)$ is the Richelot dual polynomial of $G(x)$ with respect to the given factorisation. ◊

Remark 2.19 Let $G(x) \in K[x]$ be a polynomial of degree 5 or 6. Denote by K_G its splitting field. Then the conditions for $G(x)$ to be a Richelot polynomial can be rephrased as

$$\mathrm{Gal}(K_G/K) \subseteq C_2^3 \rtimes S_3 \subseteq S_6$$
$$G(x) = G_0(x)G_1(x)G_2(x)$$

Richelot isogenies. **Definition 2.20 Richelot isogenies.** Let C/K be a Richelot curve with fixed factorisation

$$G(x) = G_0(x)G_1(x)G_2(x).$$

Let J be its Jacobian, consider the 2-torsion points of $J(\overline{K})$ defined by the quadratic factorisation of $G(x)$.

$$D_i = [P_i, Q_i]$$

where $P_i = (\alpha_i, 0)$, $Q_i = (\beta_i, 0)$. Then the isogeny over K for J whose kernel is $\{0, D_1, D_2, D_3\}$ is called a **Richelot isogeny**. ◊

We say that a Jacobian admits a Richelot isogeny over K if its underlying curve is a Richelot curve $/K$.

Theorem 2.21 *Let C/K be a Richelot curve with fixed factorisation*

$$G(x) = G_0(x)G_1(x)G_2(x).$$

Let $\widehat{C}/K$ be its Richelot dual curve and let ϕ denote the associated Richelot isogeny on J. Then $\phi\colon J \to \widehat{J}$ where $\widehat{J}$ is the Jacobian of $\widehat{C}$ and moreover $\hat{\phi}\phi = [2]$.

Lecture ? 9/4/2018

Brauer groups Galois cohomology and local invariants (Angus). Reference Milne's CFT.

Central simple algebras:

We will consider finite dimensional k-algebra for k a field.

Definition 2.22 A k-algebra A is central if the center $Z(A) = k$. A k-algebra is simple if the only two sided ideals are A and (0). ◊

Example 2.23 The matrix algebra $M_n(k)$ is central simple for k. □

Example 2.24 A quaternion algebra like $\mathbf{H} = \mathbf{R}\{i, j, k\}$ is central simple for k. □

Example 2.25 A division algebra is simple. □

Definition 2.26 Two central simple k-algebras A, B are similar, if there exists $m, n \in \mathbf{Z}_{>0}$ s.t. $A \otimes_k M_m(k) \simeq B \otimes_k M_n(k)$. Denote this by $A \sim B$. ◊

Definition 2.27 Brauer groups. The **Brauer group** of a field k denoted $\mathrm{Br}(k)$ is the set of similarity classes of central simple algebras $[A]$ with operation

$$[A][B] = [A \otimes B].$$

◊

Remark 2.28

1. The class $[M_n(k)]$ is the identity for all n.
2. The operation is well defined.
3. Given A let A^{op} be the algebra with order of multiplication reversed. Then
$$A \otimes_k A^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_k(A) \simeq M_{\dim_k(A)}(k)$$
$$(a \otimes a') \mapsto (v \mapsto ava').$$
So
$$[A]^{-1} = [A^{\mathrm{op}}].$$

Galois cohomology:

Theorem 2.29 Noether-Skolem. *Let A, B be central simple k-algebras and $f, g\colon A \longrightarrow B$ a k-algebra morphism. Then there exists*

$$b \in B^\times$$

such that

$$f(a) = bg(a)b^{-1}, \ \forall a \in A.$$

Let A be a central simple k-algebra with maximal subfield L/k.

Let $\sigma \in \mathrm{Gal}(\overline{k}/k)$, it induces a map

$$\sigma\colon A \longrightarrow A,$$

comparing this to the identity Noether-Skolem gives an element

$$e_\sigma \text{ s.t. } \sigma a = e_\sigma a e_\sigma^{-1}, \ \forall a \in L$$

defined up to multiplication by $L^\times$.

Given another $\tau \in \mathrm{Gal}(\overline{k}/k)$ I have

$$e_{\sigma\tau} a e_{\sigma\tau}^{-1} = \sigma(\tau a) = e_\sigma e_\tau a e_\tau^{-1} e_\sigma^{-1}$$

thus there exists

$$\phi(\sigma, \tau) \in L^\times$$

s.t.

$$e_{\sigma\tau} = \phi(\sigma, \tau) e_\sigma e_\tau$$

this gives a map

$$\{\text{central simple algebras}/k\} \longrightarrow H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^\times).$$

Theorem 2.30 *This descends to*

$$\mathrm{Br}(k) \simeq H^2(\mathrm{Gal}(\overline{k}/k), \overline{k}^\times).$$

Some special k.

Theorem 2.31 Wedderburn. *Every central simple k-algebra is isomorphic to $M_n(D)$ for D a division k-algebra.*

Proposition 2.32 *If $k = \overline{k}$ then any division k-algebra D is isomorphic to k. Thus* $\mathrm{Br}(k) = 0$*.*

Theorem 2.33 Wedderburn. *Every finite division ring is a field. So if k is a finite field then* $\mathrm{Br}(k) = 0$*.*

Theorem 2.34 Frobenius. *Every central division* $\mathbf{R}$*-algebra is isomorphic to either* $\mathbf{R}$ *or* $\mathbf{H}$*. Thus* $\mathrm{Br}(\mathbf{R}) \simeq \mathbf{Z}/2$*.*

Let k be a non-archimidean local field with valuation

$$v\colon k^\times \longrightarrow \mathbf{Z}$$

for a central division algebra D there exists $n \in \mathbf{Z}$ s.t.

$$v\colon D^\times \longrightarrow \frac{1}{n}\mathbf{Z}.$$

Consider a maximal unramified subfield

$$K \subseteq L \subseteq D$$

with $\sigma \in \mathrm{Gal}(L/K)$ lifting frobenius.

Noether-Skolem gives $\alpha \in D^\times$ s.t.

$$\sigma x = \alpha x \alpha^{-1},\ \forall x \in L$$

up to $L^\times$.

If we take $\alpha' = c\alpha$ for $c \in L^\times$ we can compute

$$v(\alpha') = v(c) + v(\alpha) \equiv v(\alpha) \pmod{\mathbf{Z}}.$$

We get a map

$$\{\text{central division algebras}/k\} \to \mathbf{Q}/\mathbf{Z}.$$

Theorem 2.35 *This descends to an isomorphism*

$$\mathrm{Br}(k) \simeq \mathbf{Q}/\mathbf{Z}.$$

If F is a number field with a place $v \in |F|$ get a map

$$\mathrm{inv}_v \colon \mathrm{Br}(F) \to \mathrm{Br}(F_v) \simeq \begin{cases} 0, & F_v = \mathbf{C}, \\ \mathbf{Z}/2, & F_v = \mathbf{R}, \\ \mathbf{Q}/\mathbf{Z}, & F_v \text{ nonarch.} \end{cases}.$$

Global CFT gives an exact seq

$$0 \to \mathrm{Br}(F) \to \bigoplus_v \mathrm{Br}(F_v) \to \mathbf{Q}/\mathbf{Z} \to 0.$$

Root numbers of elliptic curves (Ricky). Based on Rohrlich's article elliptic curves and the Weil-Deligne group

K non-archimidean local field, $\overline{K}$ is its separable closure.

$$\phi = (x \mapsto x^q)^{-1} \in \mathrm{Gal}(\overline{k}/k),\ q = |k|$$

Φ some lift of ϕ in $\mathrm{Gal}(\overline{K}/K)$.

$W(\overline{K}/K)$ = Weil group, the preimage of $\langle\phi\rangle$ in $\mathrm{Gal}(\overline{k}/k)$ under $G_K \twoheadrightarrow G_k$.

We consider $\sigma \colon W(\overline{K}/K) \to \mathrm{GL}(V)$, representations over $V/\mathbf{C}$ (always cts.)

Say σ is of Galois type if it factors through a finite quotient.

Another source of examples is

$$\omega \colon W \to \mathbf{C}^\times$$

given by

$$\omega(I) = \{1\}$$

where

$$I = \ker(G_K \to G_k)$$

and $\omega(\Phi) = q^{-1}$.

Fact, all irreducible $\sigma \cong \rho \otimes \omega^s$ for some $s \in \mathbf{C}$ and ρ of Galois type.

Definition 2.36 The Weil-Deligne group. The **Weil-Deligne group** is

$$W'(\overline{K}/K) = W(\overline{K}/K) \ltimes \mathbf{C}$$

where W acts on $\mathbf{C}$ via ω

$$gzg^{-1} = \omega(g)z,\ g \in W(\overline{K}/K), z \in \mathbf{C}.$$

◊

Upshot: Representations σ' of W' are the same as (σ, N) where

$$\sigma\colon W \to \mathrm{GL}(V)$$

a representation and N is a nilpotent linear operator on V. Satisfying

$$\sigma(g)N\sigma(g)^{-1} = \omega(g)N.$$

One motivation for studying those is a general construction of Grothendieck and Deligne which turn an l-adic representation of G_K into a representation of W' (given $i\colon \mathbf{Q}_l \hookrightarrow \mathbf{C}$).

Example 2.37

$$\mathrm{sp}(n) = \mathbf{C}^n$$

with action of W' given by

$$\sigma(g)e_j = \omega(g)^j e_j,\ \forall g \in W$$

$$Ne_j = e_{j+1},\ Ne_n = 0$$

check relation $\sigma N\sigma^{-1} = \omega N$. □

We want to define ϵ-factors for representations of W'. We need two choices:

$$\psi\colon K \to \mathbf{C}^\times$$

an additive character of K. And

$$\mathrm{d}x$$

a Haar measure on K.

Then

$$\epsilon(\sigma', \psi, \mathrm{d}x) = \epsilon(\sigma, \psi, \mathrm{d}x)\delta(\sigma')$$

where

$$\delta(\sigma') = \det(-N|V^I/V_N^I)$$

and $\epsilon(\sigma, \psi, \mathrm{d}x)$ is defined by the following proposition.

Proposition 2.38 Deligne-Langlands. *There exists a unique function $\epsilon(\sigma, \psi\,\mathrm{d}x)$ satisfying*

1. $\epsilon(*, \psi, \mathrm{d}x)$ *is multiplicative in short exact sequences.*
2. *If L/K is finite then*

   $$\epsilon(\mathrm{Ind}_{L/K}\,\rho, \psi, \mathrm{d}x) = \epsilon(\rho, \psi\circ\mathrm{Tr}_{L/K}, \mathrm{d}x_L)\cdot\big(\epsilon(\mathrm{Ind}_{L/K}\,1_L, \psi, \mathrm{d}x)/\epsilon(1_L, \psi\circ\mathrm{Tr}_{L/K}, \mathrm{d}x_L)\big)^{\dim\rho}$$

3. *For χ a character*

   $$\epsilon(, \chi, \psi, \mathrm{d}x)$$

   agrees with the ones defined in Tate's thesis. They're both given by an integral formula.

Definition 2.39 Root numbers. The **root number** of σ' is defined to be

$$w(\sigma', \psi) = \frac{\epsilon(\sigma',' y, \mathrm{d}x)}{|\epsilon(\sigma',' y, \mathrm{d}x)|}.$$

◊

For E/K an elliptic curve we have a representation on V_l^* $(l \neq p)$.

Using the Grothendieck-Deligne construction, let $\sigma_{E/K}$ be a representation of W' it has the following property

- E pot. good reduction then

  $$N_{E/K} = 0$$

  and $\sigma_{E/K}$ is semisimple. E has good reduction iff $\sigma_{E/K}$ is unramified.

- E has potential multiplicative reduction implies that we can take χ a character of W with $\chi^2 = 1$, so that

  $$E^\chi$$

  has split multiplicative reduction. Then

  $$\sigma'_{E/K} \simeq \chi\omega^{-1} \otimes \mathrm{sp}(2)$$

  χ is trivial / unramified and non-trivial / ramified according to E having split / non-split / additive reduction.

- $\sigma'_{E/K}$ is essentially symplectic. $W(E/K) = W(\sigma'_{E/K})$ is independent of ψ and must be ± 1.

Proposition 2.40

1. *E has good reduction implies $W(E/K) = 1$.*
2. *E potentially multiplicative reduction implies*

   $$W(E/K) = \begin{cases} -1 & \textit{split} \\ 1 & \textit{nonsplit} \end{cases}.$$

   If additive reduction take ξ quadratic character s.t.

   $$E^\xi$$

   has split multiplicative reduction and $W(E/K) = \xi(-1)$.

III **(Sachi).** Lecture ? 11/4/2018

Suppose G is a finite abelian group with a non-degenerate alternating, bilinear paring

$$\Gamma \colon G \times G \to \mathbf{Q}/\mathbf{Z}$$

then there exists H s.t. $G \cong H \times H$.

Nondegeneracy is the property that: If $\Gamma(v, w) = 0$ for all $w \in G$ then $w = 0$.

Alternating: For all $v \in G$, $\Gamma(v, v) = 0$. (this implies skew-symmetry).

Analogous theorem:

Symplectic space if V a vector space with non-degenerate alternating bilinear pairing, ω has a decomposition.

$$V = W \oplus W^*$$

where W is Lagrangian.

Proof is via induction on the dimension of V. Fix $v \in V$. $\exists W$ s.t. $\omega(v, w) = 1$, scalar nondegeneracy.

Define $W = \{z \in V : \omega(z, w) = 0, \omega(v, z) = 0\}$.

$$(W, V) \cap W = 0$$

so restrict ω to W, induct.

Proof of the theorem. Trivial group ✓.

Reduce to the case of a p-group, G a p-group. Fix x of maximal order in G, p^n. There exists y such that $\Gamma(x, y) = \frac{1}{p^n}$. If not then $\Gamma(p^{n-1}x, y) = 0$ for all $y \in G$ so this contradicts non-degeneracy. Any y has maximal order also since

$$0 \neq p^{n-1}\Gamma(x, y) = \Gamma(x, p^{n-1}y).$$

Next we want to show $\langle x \rangle \cap \langle y \rangle = 0$. If $mx = ny$ for some $0 < m, n < p^n$ then

$$0 = m\Gamma(x, y) = \Gamma(x, mx) = n\Gamma(x, y) \neq 0.$$

Define

$$H = \{z : \Gamma(x, z) = \Gamma(y, z) = 0\}$$

claim:

$$G \cong (\langle x \rangle \oplus \langle y \rangle) \oplus H.$$

Proof of claim: If $g \in G$

$$\gamma := g - p^n\Gamma(y, g)x - p^n\Gamma(x, g)y$$

so

$$\Gamma(x, \gamma) = \Gamma(x, g) - p^n\Gamma(y, g)\cancelto{0}{\Gamma(x, x)} - p^n\Gamma(x, g)\underbrace{\Gamma(x, y)}_{1/p^n} = 0$$

here we used alternating.

Then Γ restricts to a non-degenerate alternating bilinear pairing on H. ■

Remark 2.41 For a PPAV we do not always have an alternating pairing, sometimes just skew-symmetric, or nothing! So Sha can be square, twice a square, or arbitrary. See Poonen-Stoll, Stein?

Complete 2-descent (Oana). Let

$$y^2 = x(x - 5)(x + 5)$$

http://www.lmfdb.org/EllipticCurve/Q/800/d/3, then

$$\Delta = 10^6$$

so the bad primes are $2, 5$.

$\#\tilde{E}(\mathbf{F}_3) = 4$.

$$E_{\text{tors}}(\mathbf{Q}) \hookrightarrow \tilde{E}(\mathbf{F}_3)$$

so

$$E_{\text{tors}}(\mathbf{Q})[2] = \{0, (0, 0), (5, 0), (-5, 0)\}.$$

$$E[2] \subseteq E(\mathbf{Q}).$$

$S = \{2, 5, \infty\} \subseteq M_{\mathbf{Q}}$.

$$\mathbf{Q}(S,2) = \{b \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^2 : \mathrm{ord}_p(b) \equiv 0 \pmod 2,\ \forall p \notin S\}$$

a complete set of coset representatives is

$$\{\pm 1, \pm 2, \pm 5, \pm 10\}$$

which has 8 elements. Consider

$$E(\mathbf{Q})/2E(\mathbf{Q}) \to \mathbf{Q}(S,2) \times \mathbf{Q}(S,2)$$

$$e_0 = 0, e_1 = 5, e_2 = -5.$$

$$0 \mapsto (1,1)$$
$$(0,0) \mapsto (-1,-5)$$
$$(0,5) \mapsto (5,2)$$
$$(0,-5) \mapsto (-5,10)$$

does the system

$$b_1 z_1^2 - b_2 z_2^2 = 5$$
$$b_1 z_1^2 - b_1 b_2 z_3^2 = -5$$

have a solution for pairs $(b_1, b_2) \in \mathbf{Q}(S,2)^2$ and $z_1, z_2, z_3 \in \mathbf{Q}$?

If $b_1 < 0, b_2 > 0$ or $b_1 > 0, b_2 < 0$ then we have no solution.

b_1	b_2	reason/point?
1	1	point 0
1	2	
1	5	
5	2	point (0,5)
-1	-1	point (-4,6)
-5	-2	point (0,5) + (-4,6)

Table 2.42: Images

Reason if $\left(\frac{a}{p}\right) = -1$ and $x^2 = ay^2 \pmod p$ then

$$x \equiv 0 \equiv y \pmod p$$

then

$$b_1(z_1^2 - b_2 z_3^2) = -5$$

If $5 \nmid b_1$ and $\left(\frac{b_2}{5}\right) = -1$ then

$$5 | z_3$$

we have $z_3 \in 5\mathbf{Z}_3 \cap \mathbf{Q}$

$$|z_3|_5 \le \frac{1}{5}.$$

We reverse engineer $(-4, 6) \in E(\mathbf{Q})$.

Weil-Châtelet groups (Aash, Asra). I have an elliptic curve E/K, then C/K a smooth curve is a PHS if

$$\exists\mu\colon E(\overline{K})\times C(\overline{K})\to C(\overline{K})$$

$$(P,p)\mapsto p+P.$$

Such that μ is defined over K and $(P+Q)+p=P+(Q+p)$ and for all $p,q\in C(\overline{K})$ there exists a unique $P\in E(\overline{K})$ s.t. $\mu(P,p)=q$.

We say two PHS C,C' are equivalent if

$$\phi/K\colon C\to C'$$

which respects the action of E.

$\forall P\in E, p\in C$

$$\phi(P+p)=P+\phi(p)$$

$$\phi(\mu_C(P,p))=\mu_{C'}(P,\phi(P)).$$

WC(E) is set of the equivalence classes of PHS's.

$$WC(E/K)\leftrightarrow H^1(G_{\overline{K}/K},E).$$

Proposition 2.43 Weil. *Let H_1,H_2 be homogeneous spaces for an algebraic group G/K. There exists H a PHS over K and*

$$f\colon H_1\times H_2\to G$$

$$f(P+p,Q+q)=P+Q+f(p,q)$$

where $P,Q\in Q$, $p\in H_1$, $q\in H_2$ this H is unique up to PHS isomorphism. If $\mathcal{H}_1,\mathcal{H}_2$ are the classes of H_1,H_2 we call $\mathcal{H}_1+\mathcal{H}_2$ the class of H (above). This defines a group structure.

1. *Well defined binary operation*
2. *Identity: call class of G, $\mathcal{H}_0$.*

$$G\times H\to H$$

$$(P,p)\mapsto P+p$$

$$\mathcal{H}_0+\mathcal{H}=\mathcal{H}'$$

for any $\mathcal{H}$. Inverse: Say H is a PHS, consider H^-

$$\mu\colon H\times E\to H$$

$$p,P\mapsto p+P$$

$$\mu_-\colon H^-\times E'\to H^-$$

$$p,P\to p+(-P)$$

$$\phi\colon H\times H^-\to E$$

$$(a,b)\mapsto v(a,b)$$

$P=v(a,b)\in E$ s.t. $P+b=a$. Associativity: H_1,H_2,H_3

$$H_1,H_2\to H_{12}$$

Lecture ? 18/4/2018

$$C\colon y^2 = f(x) = p_1(x)p_2(x)p_3(x) \to C'\colon y^2 = \frac{1}{\Delta}g_1(x)g_2(x)g_3(x)$$

$$J(C) \xrightarrow{\text{Richelot isogeny}} J'(C')$$

We showed

$$(-1)^{\mathrm{rk}_2(J)} = (-1)^{\mathrm{ord}_2\left(\prod_v \frac{c_v(J)}{c(J')}\frac{\Omega_J}{\Omega_{J'}}\right)}$$

Missed ????????

Take $a \in Ш(A/K)$ then a can be represented by a locally trivial PHS X over K. Let $K^{\mathrm{sep}}(X)$ be the function field of $X \otimes_K K^{\mathrm{sep}}$. Have an exact sequence

$$0 \to (K^{\mathrm{sep}})^\times \to (K^{\mathrm{sep}}(X))^\times \to K^{\mathrm{sep}}(X)^\times/(K^{\mathrm{sep}})^\times \to 0$$

which yields

$$\mathrm{Br}(K) = H^2(G_K, (K^{\mathrm{sep}})^\times) \to H^2(G_K, K^{\mathrm{sep}}(X)^\times) \twoheadrightarrow H^2(G_K, K^{\mathrm{sep}}(X)^\times/(K^{\mathrm{sep}})^\times) \to 0$$

the last 0 is as $H^3(G_K, (K^{\mathrm{sep}})^\times) = 0$ as X is locally trivial (c.f. Mlne Arithmetic duality theory rmk. 6.11) we have

$$0 \to \prod_v \mathrm{Br}(K_v) \to \prod_v H^2(G_{K_v}, K^{\mathrm{sep}}(X)^\times) \to H^2(G_{K_v}, K^{\mathrm{sep}}(X)^\times/(K^{\mathrm{sep}})^\times) \to \cdots$$

On the other hand from the exact sequence

$$0 \to K^{\mathrm{sep}}(X)^\times/(K^{\mathrm{sep}})^\times \to \mathrm{Div}^0(X \otimes_K K^{\mathrm{sep}}) \to \mathrm{Pic}^0(X \otimes_K K^{\mathrm{sep}}) \to 0$$

we have

$$H^1(G_K, \mathrm{Div}^0(X\otimes_K K^{\mathrm{sep}})) \to H^1(G_K, \mathrm{Pic}^0(X\otimes_K K^{\mathrm{sep}})) \to H^2(G_k, K^{\mathrm{sep}}(X)^\times/(K^{\mathrm{sep}})^\times) \to \cdots$$

now over K^{sep}, $A \otimes_K K^{\mathrm{sep}} \simeq X \otimes_K K^{\mathrm{sep}}$ hence

$$\mathrm{Pic}^0(X \otimes K^{\mathrm{sep}}) \simeq \mathrm{Pic}^0(A \otimes K^{\mathrm{sep}})$$

hence one gets a map

$$H^1(G_K, \mathrm{Pic}^0(A \otimes K^{\mathrm{sep}})) \to H^2(G_K, (K^{\mathrm{sep}}(X))^\times/(K^{\mathrm{sep}})^\times)$$

Fact 2.44 *For Jacobians of curves if the principal polarization on J is given by a rational divisor then $\langle\cdot,\cdot\rangle$ is alternating, hence $|Ш_0(A/K)| = \square$ otherwise $|Ш_0(A/K)| = 2\square$.*

Noted by Poonen and Stoll.

Theorem 2.45 *C is deficient at an odd number of place iff*

$$|Ш_0(J)| = 2\square.$$

Definition 2.46 Deficient places. We say that C is **deficient** at a place v if C doesn't have a K_v rational divisor of degree $g-1$. ◊

Hence for genus g curves this says that C has no K_v rational divisor of degree 1. Equivalently C has no K_v-rational point over any odd degree extension of K_v.

E.g. if $K_v = \mathbf{R}$ we have C deficient iff $C(\mathbf{R}) \neq \emptyset$.

$$y^2 = cq_1(x)q_2(x)q_3(x),\ c > 0 \text{ and } q_i \text{ irred over } \mathbf{R}$$

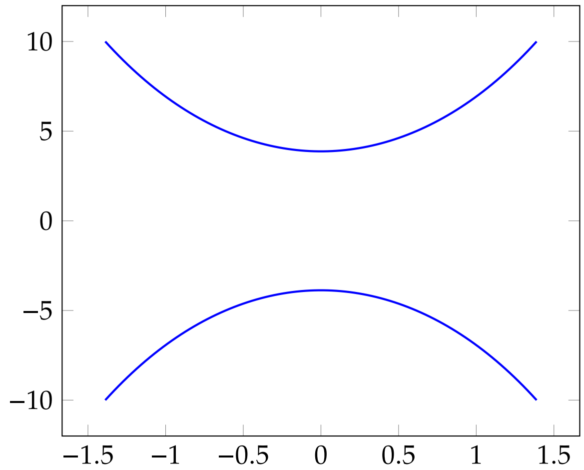

Figure 2.47

Here $c > 0$ and $C(\mathbf{R}) \neq \emptyset$ and C is not deficient over $\mathbf{R}$.
Alternatively $c < 0$ and $C(\mathbf{R}) = \emptyset$ and C is deficient over $\mathbf{R}$.

Infinite places. **Definition 2.48** Let J/K be a jacobian admitting a Richelot isogeny ϕ over K for a place of K such that $v|\infty$, we denote ϕ_v the map induced by ϕ on $J(K_v)$ and define

$$\varphi\colon J(K_v)^0 \to J(K_v)^0$$

the restriction of ϕ_v to the identity component. ◊

Lemma 2.49
$$\frac{\Omega_J}{\Omega_{J'}} = \prod_{v|\infty} \frac{n(J'(K_v))}{|\ker(\varphi)| n(J(K_v))}$$

where $n(J(K_v))$ denotes the number of connected components of $J(K_v)$.

Proof. Same as the elliptic curve case. ■

Case $K_v = \mathbf{C}$ here $n(J(\mathbf{C})) = 1 = n(J'(\mathbf{C}))$ and $|\ker\varphi| = 4$

Proposition 2.50

$$n(J(\mathbf{R})) = \begin{cases} 2^{n(C(\mathbf{R}))-1} & \text{if } n(C(\mathbf{R})) > 0, \\ 1 & \text{if } n(C(\mathbf{R})) = 0. \end{cases}$$

Proposition 2.51 *A divisor $D_i = [P_i, Q_i] \in \ker(\phi)$ is in $\ker\varphi$ iff the points P_i, Q_i satisfy either*

1. *$P_i = \overline{Q}_i$, or*
2. *P_i and Q_i lie on the same connected component of $C(\mathbf{R})$.*

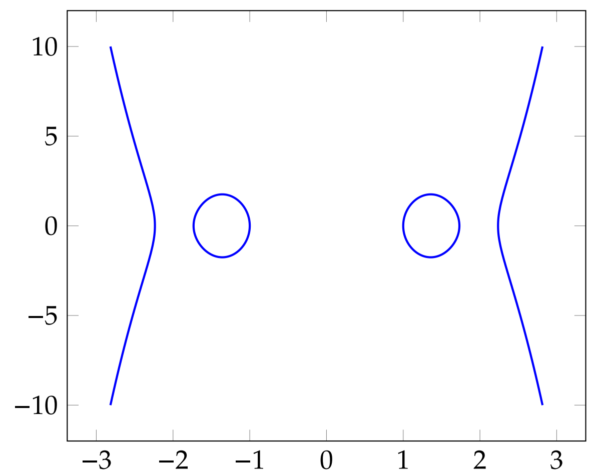

Figure 2.52

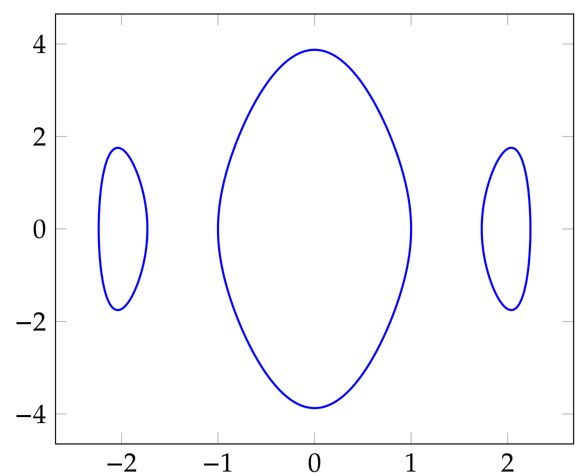

Figure 2.53

$D_1 = [(r_1, 0), (r_2)]$ with r_1, r_2 the smallest roots. Then $D_1 \in \ker\varphi$.
$D_2 = [(r_1, 0), (r_3)]$ with r_3 the next smallest root. Then $D_2 \notin \ker\varphi$.