Ranks and Parity of Ranks of Curves and Abelian Surfaces

MA842 at BU Spring 2019

Céline Maistret

March 7, 2019

1 Mordell-Weil groups

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?

1.1 Elliptic curves and their ranks

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

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

First write

$$P = mP_1 + Q_{i_1}$$

for some $1 \le i \le r$. 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

$$h(P_j) \le \frac{1}{m^2}(h(mP_j) + c_2)$$

$$\frac{1}{m^2}(h(P_{j-1}) - Q_{i_j}) + c_2)$$

$$\le \frac{1}{m^2}(2h(P_{j-1}) + c_1' + c_2)$$

by 1. Where c_1' is the maximum of the constants from i for Q in $\{-Q_1, \dots, -Q_r\}$. Note that c_1' and c_2 do not depend on P and that $h(P) \ge 0$. We repeat this inequality starting from P_n and working back to P.

$$h(P_n) \le \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right))(c_1' + c_2)$$

$$= \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{m^2}\left(1 + \frac{2}{m^2} + \left(\frac{2}{m^2}\right)^2 + \cdots + \left(\frac{2}{m^2}\right)^{n-1}\right))(c_1' + c_2)$$

$$< \left(\frac{2}{m^2}\right)^n h(P) + \frac{c_1' + c_2}{m^2 - 2}$$

$$\le \frac{1}{2^n} h(P) + \frac{c_1' + c_2}{2},$$

since $m \ge 2$. Hence for n sufficiently large (to make $\frac{1}{2^n} h(P) \le 1$) we have

$$h(P_n) \le 1 + \frac{1}{2}(c_1' + c_2).$$

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

$$\{Q_1, \dots, Q_r\} \cup \{Q \in A : h(Q) \le 1 + \frac{1}{2}(c_1' + c_2)\}.$$

■

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

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

Lecture 2 29/1/2018

Lecture 3 31/1/2018

Lecture 4 5/2/2018

Remark 1.6 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 1.7 *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

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

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

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

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.

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

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

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

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 1.8 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 1.9: 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 1.10 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

$$P = (az_1^2 + \alpha, \sqrt{abc}, z_1z_2z_3) \mapsto (a, b, c)$$

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 1.11

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

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

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 1.13 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 1.14 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 1.15 *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 1.16

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 1.17

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

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 1.18 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 Twist(C/K) - the set of twists of C/K modulo K-isomorphism.

Theorem 1.19 *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 1.20 If C is an elliptic curve then Isom(C) is generated by

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

and translations

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

$$Q \mapsto Q + P.$$

Example 1.21 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 1.22 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.

$\lozenge$

Proposition 1.23 *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 1.24 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'.

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

$\lozenge$

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 1.25 *Let C/K be a PHS for E/K then C/K is in the trivial class $\iff C(K) \neq \emptyset$.*

Theorem 1.26 *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 1.27 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 $\alpha \in \mathrm{Aut}(E)$.

$$\begin{array}{ccc} C & \xrightarrow{\mu} & E \\ & & \downarrow{\scriptstyle P} \\ C' & \xrightarrow{\mu^\alpha} & E' \end{array}$$

Lecture 7 21/2/2018

Example 1.28 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 $\sigma = \mathrm{id}$ then $p^\sigma - p = 0 - 0 = 0$. If $\sigma = -\mathrm{id}$ then $p^\sigma - p = T - 0 = T$.

$\square$

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

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

defined by

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

$\Diamond$

Definition 1.30 The Shafarevich-Tate group. The **Shafarevich-Tate** group of E/K is the subgroup of

$$WC(E/K)$$

defined by

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

$\Diamond$

Theorem 1.31 *There is an exact sequence*

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

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

1.2 p^∞-Selmer and the structure of Ш

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

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

is torsion.

So we may write

$$Ш(E/K) = \bigoplus_p Ш_{p^\infty}(E/K)$$

where for each prime p

$$Ш_{p^\infty}(E/K)$$

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

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

So

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

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

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

is called the infinitely divisible subgroup of Ш denoted $Ш_{div}$.

The conjecture that Ш 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

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

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

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

Definition 1.32 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 1.33 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.