

# Ranks and Parity of Ranks of Curves and Abelian Surfaces

MA842 at BU Spring 2019

Céline Maistret

February 21, 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](https://sites.google.com/view/cmaistret/teaching#h.p_BYGoPzU848FJ).

Course overview:

Main references that we will be following:

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

### 1.1 Mordell-Weil

Lecture 4 5/2/2018

**Remark 1.1** A homomorphism  $\phi: \text{Gal}(\bar{K}/K) \rightarrow G$  for a finite group  $G$  is continuous if it comes from a finite Galois extension, i.e.

$$\exists F/K \text{ finite Galois, } \tilde{\phi}: \text{Gal}(F/K) \rightarrow G$$

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

**Proposition 1.2** Let  $E/K$  be an elliptic curve

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

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

1.  $K(\frac{1}{2}P)/K$  is a Galois extension and  $\text{Gal}(K(\frac{1}{2}P)/K) = C_2 \times C_2$  from Lemma 1.

2.

$$\phi_P: \text{Gal}(\bar{K}/K) \rightarrow E(K)[2]$$

$$g \mapsto Q^\sigma - Q = g(\frac{1}{2}P) - \frac{1}{2}P$$

is well defined and has kernel  $\text{Gal}(K/K(\frac{1}{2}P))$ .

3.

$$\phi: E(K)/2E(K) \rightarrow \text{Hom}_{cts}(\text{Gal}(\bar{K}/K), E(K)[2])$$

$$P \mapsto \phi_P$$

is well defined and injective. Now  $\phi_P$  is continuous by 2. and so

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

a homomorphism.

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

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

$$\begin{aligned}\phi_P(g) = 0 &\implies g\left(\frac{1}{2}P\right) = \frac{1}{2}P \forall g \in \text{Gal}(\bar{K}/K) \\ &\implies \frac{1}{2}P \in E(K) \implies P \in 2E(K)\end{aligned}$$

which gives injectivity.

4.

$$\eta: \text{Hom}_{cts}(\text{Gal}(\bar{K}/K), E(K)[2]) \rightarrow K^\times/K^{\times 2} \times K^\times/K^{\times 2} \times K^\times/K^{\times 2}$$

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

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

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

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

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

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

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

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  $\eta$ .

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

$$E: y^2 = x^3 + Ax^2 + Bx$$

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

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

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

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

then

$$P = (x_2, y_2)$$

then

$$\begin{aligned} \sqrt{x_2 - \alpha}, \sqrt{x_2 - \beta}, \sqrt{x_2 - \gamma} &\in K(\frac{1}{2}P) \\ K(\sqrt{x_2 - \alpha}), K(\sqrt{x_2 - \beta}), K(\sqrt{x_2 - \gamma}) &\subseteq K(\frac{1}{2}P) \\ \implies K(\frac{1}{2}P) &= K(\sqrt{x_2 - \alpha}, \sqrt{x_2 - \beta}, \sqrt{x_2 - \gamma}) \end{aligned}$$

**Example 1.3** Let

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

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 1.4:** 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  $2 - n^2 = \square \pmod{8} \implies n^2 \equiv 1 \pmod{8}$

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

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

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

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

4) Use the group structure!

□

**Theorem 1.5 Complete 2-decent.** Let  $K$  be a field of characteristic 0 and

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

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.

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

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 1.6**

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

Lecture 5 7/2/2018

Recall:

$$\phi: E(K)/2E(K) \rightarrow \text{Hom}_{cts}(G_K, E(K)[2])$$

$$P \mapsto \phi_P$$

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

Elements of

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

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

**Lemma 1.7** Let  $n \geq 1$

1.

$$\psi: E(K)/nE(K) \rightarrow \{K \subseteq F \subseteq \overline{K}\}$$

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

is well defined.

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

3.

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

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

To do descent, need more than  $\psi$  (i.e. injection).

**Definition 1.8** Let  $G$  be a group and  $M$  a  $G$ -module then let

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

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

◇

**Remark 1.9** If  $G$  acts trivially on  $M$  then

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

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

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 1.10** If

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

is an exact sequence of  $G$ -modules then

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

**Lemma 1.11**

1.  $\psi$  is finite-to-one (gives Mordell-Weil)

2. Let

$$\phi_P: G_K \rightarrow E[n]$$

$$\phi_P(gh) = \phi_P(g) + g\phi_P(h)$$

is a skew (or crossed) homomorphism. If  $(\frac{1}{n}P)'$  is another choice of  $\frac{1}{n}P$  and  $\phi'_P$  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.  $\phi_P$  factors through

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

4.

$$\phi: E(K)/nE(K) \rightarrow Z/B$$

$$P \mapsto \phi_P$$

is an injective homomorphism. Where

$$Z = \{\text{skew homs } G_K \rightarrow E[n]\}$$

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

*Proof.*

1. There are finitely many skew homomorphisms

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

and by 4.

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

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

2.

$$\begin{aligned} \phi_P(gh) &= \frac{1}{n}P \ominus gh \frac{1}{n}P \\ &= \left( \left( \frac{1}{n}P \right) \ominus g \left( \frac{1}{n}P \right) \right) \oplus \left( g \left( \frac{1}{n}P \right) \ominus g(h \left( \frac{1}{n}P \right)) \right) \\ &= \phi_P \oplus g(\phi_P(h)). \end{aligned}$$

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

$$\begin{aligned} \phi_P(gh) &= \frac{1}{2}P \ominus gh \left( \frac{1}{2}P \right) \\ &= \frac{1}{2}P \ominus h \left( \frac{1}{2}P \right) \oplus h \left( \frac{1}{2}P \right) \ominus g(h \left( \frac{1}{2}P \right)) \\ &= \phi_P(h) \oplus \phi_P(g) \end{aligned}$$

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

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

for some  $T \in E[n]$

$$\begin{aligned} (\phi_P \ominus \phi'_P)(g) &= \phi_P(g) - \phi'_P(g) = \frac{1}{n}P \ominus g \left( \frac{1}{n}P \right) - \left[ \left( \frac{1}{n}P \right) \oplus T \ominus g \left( \frac{1}{n}P \right) \oplus gT \right] \\ &= T \ominus gT. \end{aligned}$$

■

Take  $G = G_K$

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

to get

$$0 \rightarrow E[n] \rightarrow E(\bar{K}) \xrightarrow{\cdot n} E(\bar{K}) \rightarrow 0$$

which gives the long exact sequence

$$\begin{aligned} 0 \rightarrow E(K)[n] \rightarrow E(K) \xrightarrow{\cdot n} E(K) \xrightarrow{\delta} H^1(G_K, E[n]) \rightarrow H^1(G_K, E(\bar{K})) \rightarrow \\ \implies E(K)/nE(K) \hookrightarrow H^1(G_K, E[n]). \end{aligned}$$

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

$$\text{Res}: H^1(G_K, E[n]) \rightarrow H^1(G_{K_v}, E[n]).$$

We have from the theorem

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E(\bar{K}))[n] \longrightarrow 0 \\ & & \downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} \\ 0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\delta} & \prod_v H^1(G_{K_v}, E[n]) & \longrightarrow & \prod_v H^1(G_{K_v}, E(\bar{K}))[n] \longrightarrow 0 \end{array}$$

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

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

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

**Claim 1.12**

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

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

Finding

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

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

Let  $C$  be a curve

$$\text{Isom}(C) \hookrightarrow C(\bar{K}) \times \text{Aut}(C)$$

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

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

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

$$\text{PHS} \hookrightarrow H^1(G_K, E(\bar{K}))$$

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

Lecture 6 14/2/2018

$$\begin{array}{ccccccc}
0 & \longrightarrow & E(K)/nE(K) & \xrightarrow{\delta} & H^1(G_K, E[n]) & \longrightarrow & H^1(G_K, E(\bar{K}))[m] \longrightarrow 0 \\
& & \downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} \\
0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\delta} & \prod_v H^1(G_{K_v}, E[n]) & \longrightarrow & \prod_v H^1(G_{K_v}, E(\bar{K}))[m] \longrightarrow 0
\end{array}$$

**Definition 1.13 Twists of curves.** A **twist** of  $C/K$  is a smooth curve  $C'/K$  that is isomorphic to  $C$  over  $\bar{K}$ .  $\diamond$

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

**Theorem 1.14** *The twists of  $C/K$  up to  $K$ -isomorphism are in 1-1 correspondence with elements of*

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

where

$$\text{Isom}(C) = \{\bar{K}\text{-isomorphisms } C \rightarrow C\}.$$

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

$$\phi: C' \rightarrow C$$

associate the following map

$$\xi: G_K \rightarrow \text{Isom}(C)$$

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

Check that  $\xi$  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  $\phi$ .

The map

$$\begin{aligned}
\text{Twist}(C/K) &\leftrightarrow H^1(G_K, \text{Isom}(C)) \\
C' &\mapsto \{\xi\}
\end{aligned}$$

is a bijection.

Injective, trace through.

Surjectivity, define the function field using the curve.  $\blacksquare$

**Remark 1.15** If  $C$  is an elliptic curve then  $\text{Isom}(C)$  is generated by

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

and translations

$$\tau_P: C \rightarrow C$$

$$Q \mapsto Q + P.$$

**Example 1.16**  $E/K$  elliptic, consider

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



a quadratic extension and  $\chi$  the associated character

$$\chi: G_K \rightarrow \{\pm 1\}$$

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

The group  $\pm 1$  can be viewed as automorphisms of  $C$ . So use  $\chi$  to define the cocycle

$$\xi: G_K \rightarrow \text{Isom}(C)$$

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

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

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

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

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

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

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

note that the function  $x' = x$  and  $y' = y/\sqrt{d}$  are in  $\bar{K}(x, y)_\xi$  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 1.17 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  $K$ .

$$\mu: C \times E \rightarrow C$$

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

$$v: C \times C \rightarrow E$$

$$p, q \mapsto P$$

as above.

◇

**Proposition 1.18** 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

$$\theta: E \rightarrow C$$

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

1.  $\theta$  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.  $\theta$  is a morphism over  $K$ .

**Definition 1.19** Two homogeneous space  $C/K$  and  $C'/K$  for  $E/K$  are equivalent if there is an isomorphism

$$\phi: C \rightarrow C'$$

defined over  $K$  and is compatible with the action of  $E$  on  $C$  and  $C'$ .

$$\begin{array}{ccc} C & \xrightarrow{\theta} & E \\ \phi \downarrow & & \downarrow \\ C' & \longrightarrow & E' \end{array}$$

◇

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

**Theorem 1.21** Let  $E/K$  then there is a natural bijection after fixing  $p_0 \in C$

$$WC(E/K) \rightarrow H^1(G_K, \underbrace{E(\bar{K})}_{\subseteq \text{Isom}(E)})$$

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

*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  $\xi: G_K \rightarrow E(\bar{K})$  be a cocycle representing an element in

$H^1(G_K, E)$ . Embed

$$E(\bar{K}) \hookrightarrow \text{Isom}(E)$$

$$P \mapsto \tau_P$$

and view

$$\xi \in H^1(G_K, \text{Isom } E).$$

From the theorem on

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

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

$$\phi: C \rightarrow E$$

s.t.

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

Define a map  $\mu: C \times E \rightarrow C$

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

Show that  $\mu$  is simply transitive.

Show  $\mu$  defined over  $K$ . Compute the cohomology class associated to  $C/K$  and show it is  $\xi$ . ■

**Remark 1.22** 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  $\alpha \in \text{Aut}(E)$ .

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

Lecture 7 21/2/2018

**Example 1.23**  $E/K$  and  $K(\sqrt{d})/K$  a quadratic extension. Let  $T \in E(K)$  be a non-trivial point of order 2. Then  $\xi: G_K \rightarrow E$

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

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

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

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,  $\sigma$  acts on  $\bar{K}(E)_\xi$ , which is isomorphic to  $\bar{K}(E)$  but  $\text{Gal}(\bar{K}/K)$  action is twisted by  $\xi$ , i.e.  $x^{\text{id}} \mapsto (x^{\text{id}})^\sigma$ .

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

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

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

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

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

$$\phi: E \rightarrow C$$

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

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

so that

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

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

- Prove that  $\phi$  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.

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/mE(K) & \xrightarrow{\delta} & H^1(G_K, E[m]) & \longrightarrow & WC(E/K)[m] \longrightarrow 0 \\ & & \downarrow & & \downarrow \text{Res} & & \downarrow \text{Res} \\ 0 & \longrightarrow & \prod_v E(K_v)/nE(K_v) & \xrightarrow{\delta} & \prod_v H^1(G_{K_v}, E[n]) & \longrightarrow & \prod_v WC(E/K_v)[m] \longrightarrow 0 \end{array}$$

**Definition 1.24** *m-Selmer groups.* The  $m$ -Selmer group of  $E/K$  is the subgroup of

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

defined by

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

◇

**Definition 1.25 The Shafarevich-Tate group.** The **Shafarevich-Tate** group of  $E/K$  is the subgroup of

$$\text{WC}(E/K)$$

defined by

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

◇

**Theorem 1.26** *There is an exact sequence*

1.

$$0 \rightarrow E(K)/mE(K) \rightarrow \text{Sel}^m(E/K) \rightarrow \text{III}(E/K)[m] \rightarrow 0$$

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

## 1.2 $p^\infty$ -Selmer and the structure of III

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

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

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  $\text{III}_{div}$ .

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

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

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 1.27**  $p^\infty$ -Selmer group. Consider  $\text{Sel}_{p^n}(E/K)$  and take the direct limit

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

to define the  $p^\infty$ -Selmer group. ◇

One shows that

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

called the Pontryagin dual of the  $p^\infty$  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  $\text{rk}_p$ .

**Definition 1.28**  $\text{rk}_p$  is called the  $p^\infty$ -Selmer rank of  $E/K$  and satisfies

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

◇

So if  $\text{III}$  is finite then  $\delta_p = 0$  for all  $p$ . Use BSD to compute parity of  $\text{rk}_p$ .