Parity

MA842 at BU Spring 2019

Céline Maistret

February 7, 2019

1 Parity

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.

Course overview:

Main references:

1. Vlad
2. Silverman
3. Milne

1.1 Mordell-Weil

Lecture 4 5/2/2018

Remark 1.1 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 1.2 *Let E/K be an elliptic curve*

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

for $P \in E(K)$ have $\frac{1}{2}P \in E(\overline{K})$ 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 1.3 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	rat
-2	-1	2	rat
-2	2	-1	rat
-2	-2	1	rat

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

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

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

4) Use the group structure! $\square$

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

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

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 1.6

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

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 1.7 *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* $\operatorname{im} \psi$ *is finite.*

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

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

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

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

◊

Remark 1.9 If G acts trivially on M then

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

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

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 1.10 *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 1.11

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

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

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 1.12

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

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. ???
Hensels 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.