Parity

MA842 at BU Spring 2019

Céline Maistret

February 6, 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

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

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

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

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

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

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

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

4) Use the group structure! □

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

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

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 1.6

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