Galois Reps from Torsion on ℓ^∞

Abelian Varieties

§0 Joint w/ names

Outline

- Elliptic curves
- Abelian surfaces
- Galois reps from torsion

Def: An Abelian variety is a compact (projective) algebraic curve, surface, or hyper-surface equipped with an "nice" abelian group law.

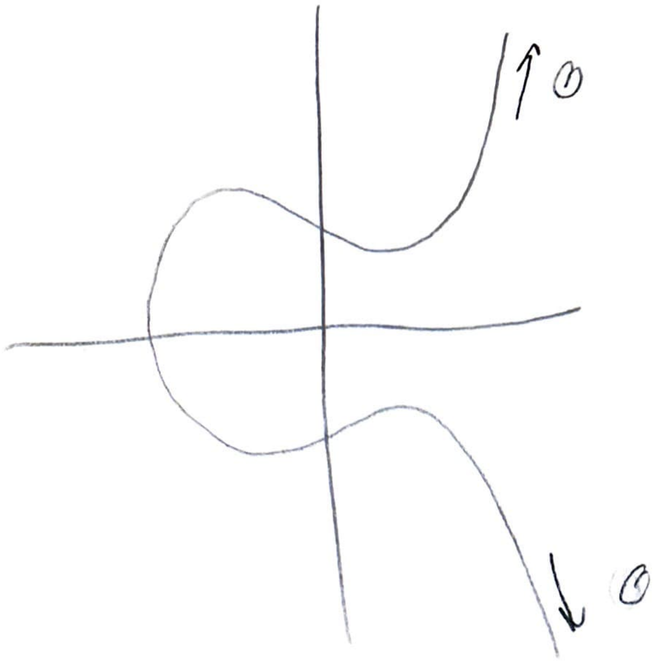
Thm: Every 1-D abelian variety is (isomorphic to) an elliptic curve

---

§1 Elliptic Curves

Def: An elliptic curve is the locus of points (x,y) satisfying $y^2 = x^3 + Ax + B$ for $4A^3 + 27B^2 \neq 0$, together with a point at infinity $\mathcal{O}$.

Ex:

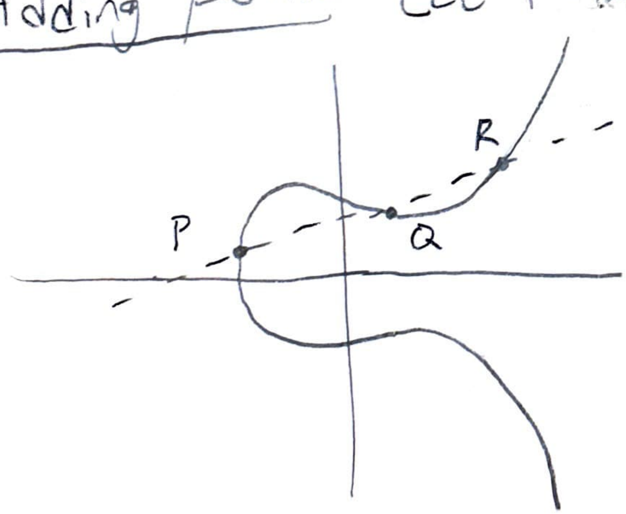


The point at infinity lies on every vertical line.
(point on the horizon)

Group law

1. Pick an identity (Convention to pick $\mathcal{O}$)
2. 3 colinear points add to $\mathcal{O}$.

Adding points Let $P=(x_1,y_1), Q=(x_2,y_2) \in E$.



Thm Let ℓ be line spanned by P, Q. $\ell \cap E$ at a unique 3rd point R.

Proof: Let $\ell : y = mx+b$. x-coords of intersection given by

$$\underbrace{x^3+Ax+B-(mx+b)^3}_{\text{cubic}} = (x-x_1)(x-x_2)(\text{linear !!})$$

$\boxed{\text{Z}}$

So, $P+Q+R=\mathcal{O}$.

Also, $R+\overline{R}+\mathcal{O}=\mathcal{O}$

So $P+Q=\overline{R}$

Observe: Let K field. If $P,Q\in K^2$, then $P+Q\in K^2$.

Def: Let $E: y^2=x^3+Ax+B$, K field w/ $A,B\in K$. Then, let $E(K)$ denote the group of K-points of E.

soln $(x,y)\in K^2$.

---

§2 Abelian Surfaces

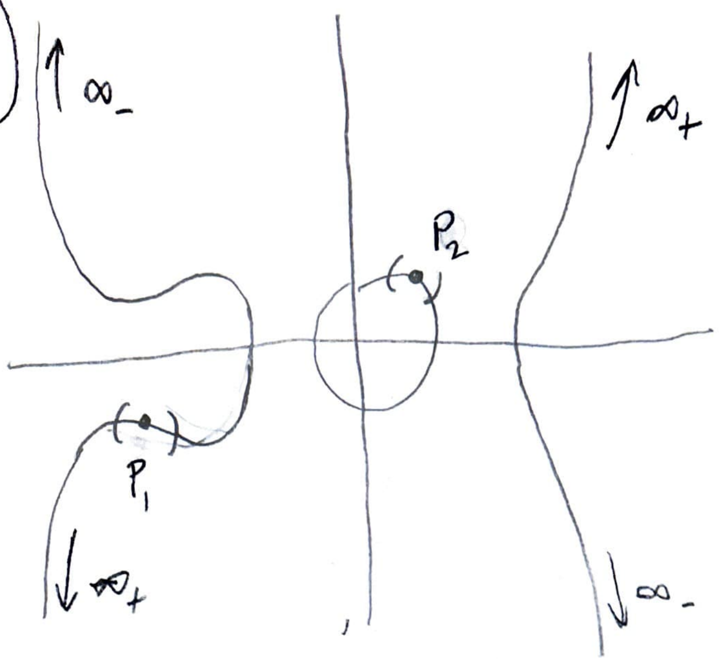
Thm Every (principally polarized) abelian surface is (iso to) either

① $E_1\times E_2$

② Jacobian of a hyperelliptic curve

Def A (genus 2) hyperelliptic curve is the locus of points (x,y) satisfying $y^2=f(x)$ for f degree 6 w/ distinct roots, together w/ two points at ∞, called ∞_+ and ∞_-.

4



Q: How to make a surface?

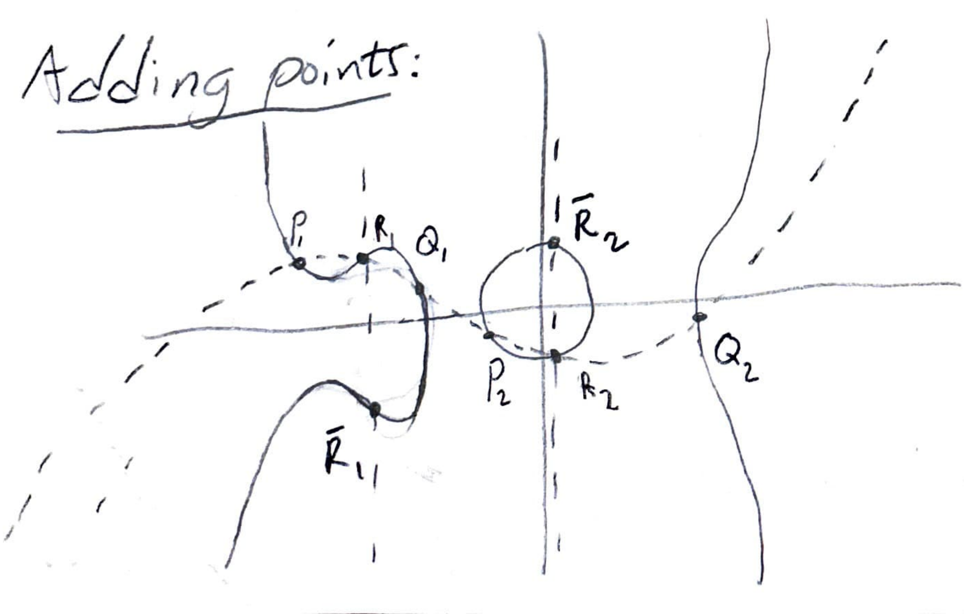
A: Look at pairs of points.

Def: The Jacobian of a (genus 2) hyperelliptic curve C is *roughly* the space of unordered points on C, with a group law.

Group law: ① Set every vertical pair to the identity.

② 3 pairs sharing a cubic add to O.

Adding points:



$P+Q+R=O$

$R+\bar{R}=O$

$\Rightarrow P+Q=\bar{R}$

(attempted) Def: Let J be a Jacobian of a genus 2 curve $C: y^2 = f(x)$ and let K be a field w/ $f(x) \in K[x]$.
Let $J(K)$ denote the point pairs w/ coords in K.

Problem: Above def does not give a group. Why?

Let $g(x)$ be cubic interpolating P, Q.

$x(g \cap C)$ given as roots of

$f(x) - g^2(x) = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$ (quadratic) $\ddot{\frown}$

Solution: $ Mumford coordinates $

Def: The mumford coordinates of a point pair $P = \{(x_1, y_1), (x_2, y_2)\}$ is the pair $(x^2 + \alpha x + \beta, \gamma x + \delta)$ where

① $x^2 + \alpha x + \beta = (x - x_1)(x - x_2)$

② $y_1 = \gamma x_1 + \delta$, $y_2 = \gamma x_2 + \delta$.

This bypasses the need to solve that quadratic.

(correct) Def: Same setup. Let $J(K)$ denote the group of point pairs w/ M.C. coefs $\alpha, \beta, \gamma, \delta \in K$.

---

§3 Galois Reps

Q: What are the field automorphisms $\mathbb{C} \to \mathbb{C}$ which fix $\mathbb{R}$ point-wise?

A: $\left\{ \begin{array}{l} z \mapsto z \\ z \mapsto \bar{z} \end{array} \right\}$

Why? $\sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i)$
$= a + b\sigma(i)$

So, suffices to set $\sigma(i)$.

$(\sigma(i))^2 = \sigma(i^2) = \sigma(-1) = -1$

So $\sigma(i)$ is a root of x^2+1, ie $\sigma(i) = \pm i$.

Rmk: Above set forms a group under composition.

Def: Let $K \subseteq L$ be fields. The Galois group $\mathrm{Gal}(L/K)$ is the group of field autos $L \to L$ fixing K (group law is composition)

☆ Fact: If $f \in K[x]$ and roots $\in L$, then $\mathrm{Gal}(L/K)$ shuffles roots. ☆

Def: The set of roots in $\mathbb{C}$ to polynomials $\in \mathbb{Q}[x]$ form a field, denoted $\overline{\mathbb{Q}}$.

Prop: Let E be an elliptic curve w/ $A, B \in \mathbb{Q}$. Then, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\overline{\mathbb{Q}})$ by

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

☆ Acts on the group, & not just the set. ☆

Proof sketch:

Fact: $$(x_1,y_1)+(x_2,y_2) = \left(\underbrace{\left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - (x_1+x_2)}_{x_3},\ \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) - y_1\right)$$

Compare $\sigma(x_1,y_1)+\sigma(x_2,y_2)$ to $\sigma((x_1,y_1)+(x_2,y_2))$.

Moral Works B.C. group law given by rational fn's.

Prop Let J be a Jacobian of a genus 2 hyper E.C..

$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \curvearrowright J(\overline{\mathbb{Q}})$ by

$$\sigma(x^2+\alpha x+\beta, \gamma x+\delta) \mapsto (x^2+\sigma(\alpha)x+\sigma(\beta), \sigma(\gamma)x+\sigma(\delta)).$$

Proof idea: Addition given by (more complicated) rational functions.

Q: $J(\overline{\mathbb{Q}})$ is huge. Does action restrict to any nice subgroups?

A: Yes! Consider the n-torsion subgroup

$$J(\overline{\mathbb{Q}})[n] = \{P \in J(\overline{\mathbb{Q}}) : nP = 0\}.$$

$J(\overline{\mathbb{Q}})[n]$ is cut out by (very complicated) polynomials, so it is preserved by $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$.

Fact: $J(\overline{\mathbb{Q}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^4$.

Rmk: For $n=p$ prime,

$$J(\overline{\mathbb{Q}})[p] \cong (\mathbb{Z}/p\mathbb{Z})^4 \cong \mathbb{F}_p^4$$

Recall: Action $G \curvearrowright X \iff$ Hom $G \to Aut(X)$

Def: The mod-p Galois representation from torsion on an abelian surface is the map

$$\rho_{J,p} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_4(\mathbb{F}_p)$$

corresponding to the action above.