

Elliptic Curves

D. Zack Garza

February 28, 2020

Contents

| | | |
|---|---------------------|---|
| 1 | Wednesday January 8 | 1 |
| 2 | Mordell-Weil Groups | 1 |

1 Wednesday January 8

Summary:

1. Mordell-Weil theorem
 - For elliptic curves over global fields (number fields, function fields, finite fields, etc)
 - Proof uses Galois cohomology and height functions, essentially one proof!
 - Holds for abelian varieties, but more difficult (need an analog of height functions, i.e. an x -coordinate)
2. Height functions (possibly)
3. Elliptic curves over \mathbb{Q}_p or complete discrete valuation fields (see Silverman for basics, possibly Chapter 5), particularly Tate curves
4. Weil-Chatelet groups E/k related to $H^1(k; E)$ with coefficients in the elliptic curve
5. Galois representation of E/k for char $k = 0$, for $\rho_n g_k \rightarrow \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ which leads to $\hat{\rho} : g_k \rightarrow \mathrm{GL}(\hat{\mathbb{Z}})$.

2 Mordell-Weil Groups

Let E/k be an elliptic curve over a field k , i.e. a smooth, projective, geometrically integral curve of genus 1 with a k -rational point O .

Note: Silverman good for foundations, but assumes k is perfect! Here we'll assume k is arbitrary.

Remark: If k is not algebraically closed, such a point O may not exist.

By Riemann-Roch (easy computation) E embeds (non-canonically) into \mathbb{P}^2/k as a Weierstrass cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \Delta \neq 0.$$

This is a smoothness condition, and this equation has a k -rational point at infinity $[0 : 1 : 0]$. The line at infinity is a flex line (?), and so only intersects this curve at one point.

If $\text{char } k \neq 2, 3$ then $y^2 = x^3 + Ax + B$.

Every elliptic curve is given by a Weierstrass equation, although not in a unique way.

An amazing fact: The k -rational points $E(k)$ forms an abelian group with zero as the identity.

Proof:

1. Given any plane cubic C/k and an origin $O \in C(k)$, the chord and tangent process yields a group structure. Note that there is a symmetry in connecting rational points a, b with a line intersecting at another rational point c which is not present in most groups, so an additional inversion about O is needed to actually make this into a group. Proving associativity: difficult!
2. Look at $\text{Pic}^0 E$, the degree 0 divisors on E mod birational equivalence (?), which is equal to the degree 0 line bundles on E mod bundle isomorphism.

Exercise: Show there is a map $C(k) \rightarrow \text{Pic}^1 C$ given by sending p to its equivalence class; this is a bijection by Riemann-Roch (straightforward exercise).

We can then compose this with a map $\text{Pic}^1 \rightarrow \text{Pic}^0 C$ given by $D \mapsto D - [O]$, which decreases the degree by 1. This gives a map $\Phi : C(k) \rightarrow \text{Pic}^0 C$, just need to check that $\Phi(P \oplus Q) = \Phi(P) + \Phi(Q)$.

Check that the groups are independent of the k -rational point chosen, i.e. changing rational points yields isomorphic groups. So the group law itself does actually depend on the rational point, although the structure doesn't.

Exercise: Let $(E, O)/k$ be an elliptic curve and define $E^0 = E \setminus \{O\}$ the (nonsingular, integral) affine curve given by removing the point at infinity. Then the affine coordinate ring $k[E^0]$ is defined as $k[x, y]/(y^2 - x^3 - Ax - B)$, which is a Dedekind ring.

The interesting thing about Dedekind domains: the ideal class group! (i.e. the Picard group)

This has ideal class group $\text{Pic}[E^0]$, and one can show that

$$\begin{aligned} \text{Pic}^0 E &\longrightarrow \text{Pic}[E^0] \\ \sum_p n_p \deg(p)[p] &\mapsto \sum_{p \neq 0} n_p [p] = \prod_p p^{n_p} \end{aligned}$$

with the sum ranging over all closed points is an isomorphism.

Just note that the RHS can't have a point at infinity, so we just forget it. The isomorphism follows from some exact sequence with correction terms that vanish.

So the Mordell-Weil group of $E(k)$ is isomorphic to $\text{Pic}[E^0]$, the class group of a Dedekind domain (?).

Definitions: Let G be a commutative group.

- G is a *class group* iff there exists a Dedekind domain R such that $G \cong \text{Pic} R$.
- G is an (*elliptic*) *Mordell-Weil group* iff there exists a field k and an elliptic curve E/k such that $G \cong E(k)$.

Questions:

1. Which G are class groups?
2. Which G are Mordell-Weil groups?

An answer to question 1:

Theorem (Clayborn, 1966): Every commutative G is a class group.

Subsequent proofs: Leetham-Green (1972) and Clark (2008) following Rosen, and uses elliptic curves. See the end of Pete's Commutative Algebra notes!

An answer to question 2:

Consider E/\mathbb{C} , then $E(\mathbb{C}) \cong S^1 \times S^1$, so the torsion subgroup is $T(1) := (\mathbb{Q}/\mathbb{Z})^2 = \bigoplus_{\ell} (\mathbb{Q}_{\ell}/\mathbb{Z}_{\ell})^2$.

This in fact holds for any algebraically closed field of characteristic zero.

Fact: For any E/k , the Mordell-Weil group $E(k)$ is “ $T(1)$ -constrained”, i.e. $E(k)[\text{tors}] \hookrightarrow T(1)$.

Theorem (Clark, 2012): G is a Mordell-Weil group $\iff G$ is $T(1)$ -constrained.

Note: the analogous statement for abelian varieties, i.e being $T(g)$ constrained for some other genus $g \neq 1$, is open. Fixing $k = \mathbb{Q}$ still yields very interesting problems. Computing the rank and torsion subgroups is currently open, and the subject of modern research.