Elliptic curves in mathlib

David Ang

London School of Geometry and Number Theory

Wednesday, 26 June 2024

Overview: definitions

Elliptic curves in `Mathlib/AlgebraicGeometry/EllipticCurve` are defined in terms of Weierstrass curves over a commutative ring R.

Definition (`WeierstrassCurve` in `Weierstrass.lean`)

A **Weierstrass curve** W_R is a tuple $(a_1, a_2, a_3, a_4, a_6) \in R^5$.
An **elliptic curve** E_R is a Weierstrass curve such that $\Delta(a_i) \in R^\times$.

Overview: definitions

Elliptic curves in `Mathlib/AlgebraicGeometry/EllipticCurve` are defined in terms of Weierstrass curves over a commutative ring R.

Definition (`WeierstrassCurve` in `Weierstrass.lean`)

A **Weierstrass curve** W_R is a tuple $(a_1, a_2, a_3, a_4, a_6) \in R^5$.
An **elliptic curve** E_R is a Weierstrass curve such that $\Delta(a_i) \in R^\times$.

Their points are defined via the affine model.

Definition (`WeierstrassCurve.Affine.Point` in `Affine.lean`)

An **affine point** of W_R is a pair $(x, y) \in R^2$ such that $W(x, y) = 0$ and either $W_X(x, y) \neq 0$ or $W_Y(x, y) \neq 0$, where

$$W := Y^2 + a_1 XY + a_3 Y - (X^3 + a_2 X^2 + a_4 X^3 + a_6).$$

The **points** $W_R(R)$ are the affine points of W_R and a point at infinity.

Overview: files

Current:

- `Weierstrass.lean`
- `Affine.lean`
- `Projective.lean`
- `Jacobian.lean`
- `Group.lean`
- `DivisionPolynomial/Basic.lean`
- `DivisionPolynomial/Degree.lean`

Future:

- `Universal.lean`
- `DivisionPolynomial/Group.lean`
- `Torsion.lean`
- `Scheme.lean` (NEW!)

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`
- geometric argument via Bézout's theorem

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`
- geometric argument via Bézout's theorem

Proofs by identification with known groups:

- a quotient $\mathbb{C}/\Lambda$ of the complex numbers by a lattice

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`
- geometric argument via Bézout's theorem

Proofs by identification with known groups:

- a quotient $\mathbb{C}/\Lambda$ of the complex numbers by a lattice
- the group of degree-zero Weil divisors $\mathrm{Pic}^0(W_F)$

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`
- geometric argument via Bézout's theorem

Proofs by identification with known groups:

- a quotient $\mathbb{C}/\Lambda$ of the complex numbers by a lattice
- the group of degree-zero Weil divisors $\mathrm{Pic}^0(W_F)$
- the ideal class group $\mathrm{Cl}(F[W_F])$ of the coordinate ring

Group law: theorem

Theorem (in `Group.lean`)

If F is a field, then $W_F(F)$ is an abelian group under an addition law.

Elementary proofs of associativity:

- polynomial manipulation via `ring`
- geometric argument via Bézout's theorem

Proofs by identification with known groups:

- a quotient $\mathbb{C}/\Lambda$ of the complex numbers by a lattice
- the group of degree-zero Weil divisors $\mathrm{Pic}^0(W_F)$
- the ideal class group $\mathrm{Cl}(F[W_F])$ of the coordinate ring

Junyan gave an pure algebraic proof via norms.

Group law: formalisation

Define

$$\begin{array}{rcrcl} \phi & : & W_F(F) & \longrightarrow & \mathrm{Cl}(F[W_F]) \\ & & 0 & \longmapsto & [\langle 1 \rangle] \\ & & (x, y) & \longmapsto & [\langle X - x, Y - y \rangle] \end{array} .$$

Group law: formalisation

Define

$$\begin{array}{rcrcl} \phi & : & W_F(F) & \longrightarrow & \mathrm{Cl}(F[W_F]) \\ & & 0 & \longmapsto & [\langle 1 \rangle] \\ & & (x, y) & \longmapsto & [\langle X - x, Y - y \rangle] \end{array}.$$

Note that $F[W_F]$ is a free algebra over $F[X]$ with basis $\{1, Y\}$, so it has a norm given by $\mathrm{Nm}(p + qY) = \det([\cdot(p + qY)])$.

Group law: formalisation

Define

$$\begin{array}{rcccl} \phi & : & W_F(F) & \longrightarrow & \mathrm{Cl}(F[W_F]) \\ & & 0 & \longmapsto & [\langle 1 \rangle] \\ & & (x, y) & \longmapsto & [\langle X - x, Y - y \rangle] \end{array}.$$

Note that $F[W_F]$ is a free algebra over $F[X]$ with basis $\{1, Y\}$, so it has a norm given by $\mathrm{Nm}(p + qY) = \det([\cdot(p + qY)])$. On one hand,

$$\deg(\mathrm{Nm}(p + qY)) = \max(2\deg(p), 2\deg(q) + 3) \neq 1.$$

Group law: formalisation

Define

$$\begin{array}{rcrcl} \phi & : & W_F(F) & \longrightarrow & \mathrm{Cl}(F[W_F]) \\ & & 0 & \longmapsto & [\langle 1 \rangle] \\ & & (x, y) & \longmapsto & [\langle X - x, Y - y \rangle] \end{array}.$$

Note that $F[W_F]$ is a free algebra over $F[X]$ with basis $\{1, Y\}$, so it has a norm given by $\mathrm{Nm}(p + qY) = \det([\cdot(p + qY)])$. On one hand,

$$\deg(\mathrm{Nm}(p + qY)) = \max(2\deg(p), 2\deg(q) + 3) \neq 1.$$

On the other hand, $F[W_F]/\langle p + qY \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$, so

$$\deg(\mathrm{Nm}(p + qY)) = \deg(pq) = \dim(F[W_F]/\langle p + qY \rangle).$$

Group law: formalisation

Define

$$\begin{array}{rcrcl} \phi & : & W_F(F) & \longrightarrow & \mathrm{Cl}(F[W_F]) \\ & & 0 & \longmapsto & [\langle 1 \rangle] \\ & & (x, y) & \longmapsto & [\langle X - x, Y - y \rangle] \end{array}.$$

Note that $F[W_F]$ is a free algebra over $F[X]$ with basis $\{1, Y\}$, so it has a norm given by $\mathrm{Nm}(p + qY) = \det([\cdot(p + qY)])$. On one hand,

$$\deg(\mathrm{Nm}(p + qY)) = \max(2\deg(p), 2\deg(q) + 3) \neq 1.$$

On the other hand, $F[W_F]/\langle p + qY \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$, so

$$\deg(\mathrm{Nm}(p + qY)) = \deg(pq) = \dim(F[W_F]/\langle p + qY \rangle).$$

Thus if $\langle X - x, Y - y \rangle = \langle p + qY \rangle$, then

$$F[W_F]/\langle p + qY \rangle = F[X, Y]/\langle W(X, Y), X - x, Y - y \rangle \cong F,$$

which contradicts $\dim(F[W_F]/\langle p + qY \rangle) \neq 1$.

Torsion subgroup: theorem

Theorem (in `Torsion.lean`)

If F is a field where $n \neq 0$, then $E_F(\overline{F})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Torsion subgroup: theorem

Theorem (in `Torsion.lean`)

If F is a field where $n \neq 0$, then $E_F(\overline{F})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Some standard proofs:

- identification with $(\mathbb{C}/\Lambda)[n]$

Torsion subgroup: theorem

Theorem (in `Torsion.lean`)

If F is a field where $n \neq 0$, then $E_F(\overline{F})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Some standard proofs:

- identification with $(\mathbb{C}/\Lambda)[n]$
- induced map of isogenies on $\mathrm{Pic}^0(E_{\overline{F}})$

Torsion subgroup: theorem

Theorem (in `Torsion.lean`)

If F is a field where $n \neq 0$, then $E_F(\overline{F})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Some standard proofs:

- identification with $(\mathbb{C}/\Lambda)[n]$
- induced map of isogenies on $\mathrm{Pic}^0(E_{\overline{F}})$
- existence of polynomials $\psi_n, \phi_n, \omega_n \in \overline{F}[X, Y]$ such that

$$[n](x, y) = \left(\frac{\phi_n(x)}{\psi_n(x)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\right)$$

and a proof that $\deg(\psi_n^2) = n^2 - 1$

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W \rangle$, so needs a specialisation map or projective coordinates

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W \rangle$, so needs a specialisation map or projective coordinates
- The definition of ψ_n is strong even-odd recursive with five base cases and an awkward even case, so proofs are very lengthy

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W \rangle$, so needs a specialisation map or projective coordinates
- The definition of ψ_n is strong even-odd recursive with five base cases and an awkward even case, so proofs are very lengthy
- The definition of ω_n is very elusive, and seemingly involves division by two in characteristic two

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W \rangle$, so needs a specialisation map or projective coordinates
- The definition of ψ_n is strong even-odd recursive with five base cases and an awkward even case, so proofs are very lengthy
- The definition of ω_n is very elusive, and seemingly involves division by two in characteristic two
- The polynomials ϕ_n and ψ_n^2 are bivariate, so needs a conversion to univariate polynomials for degree computations

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W \rangle$, so needs a specialisation map or projective coordinates
- The definition of ψ_n is strong even-odd recursive with five base cases and an awkward even case, so proofs are very lengthy
- The definition of ω_n is very elusive, and seemingly involves division by two in characteristic two
- The polynomials ϕ_n and ψ_n^2 are bivariate, so needs a conversion to univariate polynomials for degree computations
- The identity cannot be proven directly via induction, and needs elliptic divisibility sequences and elliptic nets

Torsion subgroup: formalisation

The latter proof turned out to be incredibly tricky.

- The identity holds in the universal ring $\mathbb{Z}[A_i, X, Y]/\langle W\rangle$, so needs a specialisation map or projective coordinates
- The definition of ψ_n is strong even-odd recursive with five base cases and an awkward even case, so proofs are very lengthy
- The definition of ω_n is very elusive, and seemingly involves division by two in characteristic two
- The polynomials ϕ_n and ψ_n^2 are bivariate, so needs a conversion to univariate polynomials for degree computations
- The identity cannot be proven directly via induction, and needs elliptic divisibility sequences and elliptic nets

These have been formalised in `Projective.lean`, `Jacobian.lean`, `DivisionPolynomial/*.lean`, and `Universal.lean`. These also use lemmas in `Algebra/Polynomial/Bivariate.lean` and `NumberTheory/EllipticDivisibilitySequence.lean`

Progress: current

Already in master:

- Weierstrass curves and variable changes of standard quantities
- elliptic curves with prescribed j-invariant
- affine group law and functoriality of base change
- Jacobian group law and equivalence with affine group law
- division polynomials and degree computations

Progress: current

Already in master:

- Weierstrass curves and variable changes of standard quantities
- elliptic curves with prescribed j-invariant
- affine group law and functoriality of base change
- Jacobian group law and equivalence with affine group law
- division polynomials and degree computations

Already in branches:

- Galois theory on points and n-torsion points
- projective group law and equivalence with affine group law
- the coordinate ring and other universal constructions
- elliptic divisibility sequences and elliptic nets
- multiplication by n in terms of division polynomials
- structure of the n-torsion subgroup and the Tate module
- the affine scheme associated to an elliptic curve

Progress: future

Projects without algebraic geometry:

- algorithms that only use the group law
- finite fields: the Hasse–Weil bound, the Weil conjectures
- local fields: the reduction homomorphism, Tate's algorithm, the Neron–Ogg–Shafarevich criterion, the Hasse–Weil L-function
- number fields: Neron-Tate heights, the Mordell–Weil theorem, Tate–Shafarevich groups, the Birch–Swinnerton-Dyer conjecture
- complete fields: complex uniformisation, p-adic uniformisation

Progress: future

Projects without algebraic geometry:

- algorithms that only use the group law
- finite fields: the Hasse–Weil bound, the Weil conjectures
- local fields: the reduction homomorphism, Tate's algorithm, the Neron–Ogg–Shafarevich criterion, the Hasse–Weil L-function
- number fields: Neron-Tate heights, the Mordell–Weil theorem, Tate–Shafarevich groups, the Birch–Swinnerton-Dyer conjecture
- complete fields: complex uniformisation, p-adic uniformisation

Projects with algebraic geometry:

- elliptic curves over global function fields
- the projective scheme associated to an elliptic curve
- integral models and finite flat group schemes
- divisors on curves and the Riemann–Roch theorem
- modular curves and Mazur's theorem

THANK YOU!