The group law on an elliptic curve [1]

David Ang

London School of Geometry and Number Theory

Postgraduate Seminar

Thursday, 5 October 2023

[1] Angdinata, David Kurniadi and Xu, Junyan. *An Elementary Formal Proof of the Group Law on Weierstrass Elliptic Curves in Any Characteristic*. Fourteenth International Conference on Interactive Theorem Proving (ITP 2023)

Introduction

Pedagogical question:

Is there an *elementary* proof of the group law on *any* elliptic curve?

Introduction

Pedagogical question:

Is there an *elementary* proof of the group law on *any* elliptic curve?

Status quo:

Yes. But it depends on what is considered *elementary*.

Introduction

Pedagogical question:

Is there an *elementary* proof of the group law on *any* elliptic curve?

Status quo:

Yes. But it depends on what is considered *elementary*.

Our answer:

Yes.

Introduction

Pedagogical question:

Is there an *elementary* proof of the group law on *any* elliptic curve?

Status quo:

Yes. But it depends on what is considered *elementary*.

Our answer:

Yes. And we formalised the argument in the *Lean theorem prover*.

Introduction

Pedagogical question:

Is there an *elementary* proof of the group law on *any* elliptic curve?

Status quo:

Yes. But it depends on what is considered *elementary*.

Our answer:

Yes. And we formalised the argument in the *Lean theorem prover*.

Talk overview:

- What is an elliptic curve?
- Why is it a group?
- Where is the problem then?
- How did we do it?

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

- Wiles proved *Fermat's last theorem* by drawing a correspondence between certain elliptic curves and certain *modular forms*.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

- Wiles proved *Fermat's last theorem* by drawing a correspondence between certain elliptic curves and certain *modular forms*.
- The *Birch and Swinnerton-Dyer conjecture* predicts the behaviour of the *L-function* of an elliptic curve based on its arithmetic invariants.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

- Wiles proved *Fermat's last theorem* by drawing a correspondence between certain elliptic curves and certain *modular forms*.
- The *Birch and Swinnerton-Dyer conjecture* predicts the behaviour of the *L-function* of an elliptic curve based on its arithmetic invariants.

Outside pure mathematics, they see many computational applications.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

- Wiles proved *Fermat's last theorem* by drawing a correspondence between certain elliptic curves and certain *modular forms*.
- The *Birch and Swinnerton-Dyer conjecture* predicts the behaviour of the *L-function* of an elliptic curve based on its arithmetic invariants.

Outside pure mathematics, they see many computational applications.

- Intractability of the *discrete logarithm problem* for elliptic curves forms the basis behind many public key cryptographic protocols.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

They are the simplest non-trivial objects in arithmetic geometry.

- Wiles proved *Fermat's last theorem* by drawing a correspondence between certain elliptic curves and certain *modular forms*.
- The *Birch and Swinnerton-Dyer conjecture* predicts the behaviour of the *L-function* of an elliptic curve based on its arithmetic invariants.

Outside pure mathematics, they see many computational applications.

- Intractability of the *discrete logarithm problem* for elliptic curves forms the basis behind many public key cryptographic protocols.
- The *Atkin–Morain primality test* and *Lenstra's factorisation method* use elliptic curves and are two of the fastest known algorithms.

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

Theorem (long Weierstrass model)

Any elliptic curve E over F can be given by $E(X, Y) = 0$, where

$$E(X,Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6),$$

for some $a_i \in F$ such that $\Delta \neq 0$, [2]

[2] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

Theorem (long Weierstrass model)

Any elliptic curve E over F can be given by $E(X, Y) = 0$, where

$$E(X, Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6),$$

for some $a_i \in F$ such that $\Delta \neq 0$, [2] *with 0 being the "point at infinity".*

[2] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

Theorem (long Weierstrass model)

Any elliptic curve E over F can be given by $E(X, Y) = 0$, where

$$E(X, Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6),$$

for some $a_i \in F$ such that $\Delta \neq 0$, [2] *with 0 being the "point at infinity".*

Proof.

Follows from the *Riemann-Roch theorem* in algebraic geometry. □

[2] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Elliptic curves

An **elliptic curve** over a field F is a pair $(E, 0)$, where

- E is a *smooth projective curve* of *genus one* defined over F, and
- 0 is a distinguished point on E defined over F.

Theorem (long Weierstrass model)

Any elliptic curve E over F can be given by $E(X, Y) = 0$, where

$$E(X, Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6),$$

for some $a_i \in F$ such that $\Delta \neq 0$, [2] *with 0 being the "point at infinity".*

Proof.

Follows from the *Riemann-Roch theorem* in algebraic geometry. □

If $\mathrm{char}(F) \neq 2, 3$, then E has a **short Weierstrass model**, where

$$E(X, Y) := Y^2 - (X^3 + aX + b),$$

for some $a, b \in F$ such that $\Delta = -16(4a^3 + 27b^2) \neq 0$.

---

[2] $\Delta := -(a_1^2+4a_2)^2(a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2)-8(2a_4+a_1a_3)^3-27(a_3^2+4a_6)^2+9(a_1^2+4a_2)(2a_4+a_1a_3)(a_3^2+4a_6)$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0, *and the addition law is characterised by*

$$P + Q + R = 0 \qquad \iff \qquad P, Q, R \text{ are collinear.}$$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

If $R = 0$, then this translates to

$$P + Q = 0 \qquad \Longleftrightarrow \qquad \text{line through } P \text{ and } Q \text{ is vertical.}$$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \iff \qquad P, Q, R \text{ are collinear.}$$

If $R = 0$, then this translates to

$$P + Q = 0 \qquad \iff \qquad \text{line through } P \text{ and } Q \text{ is vertical.}$$

Thus negation can be given by

$$-(x, y) := (x, -y - a_1 x - a_3).$$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

If $R = 0$, then this translates to

$$P + Q = 0 \qquad \Longleftrightarrow \qquad \text{line through } P \text{ and } Q \text{ is vertical.}$$

Thus negation can be given by

$$-(x, y) := (x, -y - a_1 x - a_3).$$

Define an affine involution given by

$$\sigma(Y) := -Y - a_1 X - a_3.$$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

If $R = 0$, then this translates to

$$P + Q = 0 \qquad \Longleftrightarrow \qquad \text{line through } P \text{ and } Q \text{ is vertical.}$$

Thus negation can be given by

$$-(x, y) := (x, -y - a_1 x - a_3).$$

Define an affine involution given by

$$\sigma(Y) := -Y - a_1 X - a_3.$$

Note that

$$-(Y \cdot \sigma(Y)) = Y^2 + a_1 XY + a_3 Y$$

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

If $R = 0$, then this translates to

$$P + Q = 0 \qquad \Longleftrightarrow \qquad \text{line through } P \text{ and } Q \text{ is vertical.}$$

Thus negation can be given by

$$-(x, y) := (x, -y - a_1 x - a_3).$$

Define an affine involution given by

$$\sigma(Y) := -Y - a_1 X - a_3.$$

Note that in the **coordinate ring** $F[E] := F[X, Y]/\langle E(X, Y)\rangle$,

$$-(Y \cdot \sigma(Y)) = Y^2 + a_1 XY + a_3 Y \equiv X^3 + a_2 X^2 + a_4 X + a_6,$$

which is a polynomial only in X.

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \Longleftrightarrow \qquad P, Q, R \text{ are collinear.}$$

Addition can be given by $(x_1, y_1) + (x_2, y_2) := -(x_3, y_3)$.

Group law

Theorem (the group law)

The points of an elliptic curve form an abelian group, where the identity element is 0*, and the addition law is characterised by*

$$P + Q + R = 0 \qquad \iff \qquad P, Q, R \text{ are collinear.}$$

Addition can be given by $(x_1, y_1) + (x_2, y_2) := -(x_3, y_3)$. Here,

$$\lambda := \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{y_1 - \sigma(y_1)} & y_1 \neq \sigma(y_1) \\ \infty & \text{otherwise} \end{cases},$$

$$x_3 := \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 := \lambda(x_3 - x_1) + y_1.$$

Hard problem

One may attempt to prove the axioms directly.

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.
- Associativity: $(P + Q) + R = P + (Q + R)$ seems impossible?

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.
- Associativity: $(P + Q) + R = P + (Q + R)$ seems impossible?

Recall that each addition operation has five cases!

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.
- Associativity: $(P + Q) + R = P + (Q + R)$ seems impossible?

Recall that each addition operation has five cases!

In the generic case, [3] checking that their X-coordinates are equal is an equality of polynomials with 26,082 terms.

[3] P, Q, R, $P + Q$, $P + R$, and $Q + R$ are affine and have distinct X-coordinates

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.
- Associativity: $(P + Q) + R = P + (Q + R)$ seems impossible?

Recall that each addition operation has five cases!

In the generic case, [3] checking that their X-coordinates are equal is an equality of polynomials with 26,082 terms.

In the short Weierstrass model, this reduces to 2,636 terms.

[3] P, Q, R, $P + Q$, $P + R$, and $Q + R$ are affine and have distinct X-coordinates

Hard problem

One may attempt to prove the axioms directly.

- Identity: $0 + P = P = P + 0$ is trivial.
- Inverses: $(-P) + P = 0 = P + (-P)$ is easy.
- Commutativity: $P + Q = Q + P$ is easy.
- Associativity: $(P + Q) + R = P + (Q + R)$ seems impossible?

  Recall that each addition operation has five cases!

  In the generic case, [3] checking that their X-coordinates are equal is an equality of polynomials with 26,082 terms.

  In the short Weierstrass model, this reduces to 2,636 terms.

  Automation in an interactive theorem prover enables manipulation of multivariate polynomials with at most 5,000 terms.

[3] P, Q, R, $P + Q$, $P + R$, and $Q + R$ are affine and have distinct X-coordinates

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

One may instead identify the set of points $E(F)$ with a known group G.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

One may instead identify the set of points $E(F)$ with a known group G.

Pf 3. $G = \mathbb{C}/\Lambda_E$.
Riemann surfaces (*uniformisation*), but only works for $\mathrm{char}(F) = 0$.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

One may instead identify the set of points $E(F)$ with a known group G.

Pf 3. $G = \mathbb{C}/\Lambda_E$.
Riemann surfaces (*uniformisation*), but only works for $\mathrm{char}(F) = 0$.

Pf 4. $G = \mathrm{Pic}_F^0(E)$.
Algebraic geometry (*Riemann-Roch*) in general.
Ring theory (*Fermat descent*), but only works for $\mathrm{char}(F) \neq 2$.

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

One may instead identify the set of points $E(F)$ with a known group G.

Pf 3. $G = \mathbb{C}/\Lambda_E$.
Riemann surfaces (*uniformisation*), but only works for $\mathrm{char}(F) = 0$.

Pf 4. $G = \mathrm{Pic}_F^0(E)$.
Algebraic geometry (*Riemann-Roch*) in general.
Ring theory (*Fermat descent*), but only works for $\mathrm{char}(F) \neq 2$.

Undergraduate courses typically teach Pf 2 (assuming genericity), Pf 3 (assuming uniformisation), or Pf 4 (assuming Riemann-Roch).

Hard problem

Associativity is known to be mathematically difficult with many proofs.

Pf 1. Just do it.
Polynomial manipulation, but impossibly slow and many cases.

Pf 2. Count dimensions.
Projective geometry (*Cayley-Bacharach*), but only works generically.

One may instead identify the set of points $E(F)$ with a known group G.

Pf 3. $G = \mathbb{C}/\Lambda_E$.
Riemann surfaces (*uniformisation*), but only works for $\mathrm{char}(F) = 0$.

Pf 4. $G = \mathrm{Pic}^0_F(E)$.
Algebraic geometry (*Riemann-Roch*) in general.
Ring theory (*Fermat descent*), but only works for $\mathrm{char}(F) \neq 2$.

Undergraduate courses typically teach Pf 2 (assuming genericity), Pf 3 (assuming uniformisation), or Pf 4 (assuming Riemann-Roch).

Existing interactive theorem provers have used Pf 1 (Théry 2007) or Pf 4 (Bartzia–Strub 2014), both assuming the short Weierstrass model.

Algebraic analogue

Let us examine the argument for Pf 3 and Pf 4 in more detail.

Algebraic analogue

Let us examine the argument for Pf 3 and Pf 4 in more detail.

To identify $E(F)$ with G is to

- define a function $\phi : E(F) \to G$,
- prove that ϕ respects addition, and
- prove that ϕ is bijective.

Algebraic analogue

Let us examine the argument for Pf 3 and Pf 4 in more detail.

To identify $E(F)$ with *a subgroup of G* is to

- define a function $\phi : E(F) \to G$,
- prove that ϕ respects addition, and
- prove that ϕ is ~~bijective~~ injective.

Algebraic analogue

Let us examine the argument for Pf 3 and Pf 4 in more detail.

To identify $E(F)$ with *a subgroup of* G is to

- define a function $\phi : E(F) \to G$,
- prove that ϕ respects addition, and
- prove that ϕ is ~~bijective~~ injective.

Pf 4 sets $G = \mathrm{Pic}^0_F(E)$, and

$$\phi \text{ is injective} \quad \Longleftrightarrow \quad \text{there is no isomorphism } E \xrightarrow{\sim} \mathbb{P}^1,$$

which follows from isomorphism invariance of the *genus*.

Algebraic analogue

Let us examine the argument for Pf 3 and Pf 4 in more detail.

To identify $E(F)$ with *a subgroup of G* is to

- define a function $\phi : E(F) \to G$,
- prove that ϕ respects addition, and
- prove that ϕ is ~~bijective~~ injective.

Pf 4 sets $G = \mathrm{Pic}^0_F(E)$, and

$$\phi \text{ is injective} \iff \text{there is no isomorphism } E \xrightarrow{\sim} \mathbb{P}^1,$$

which follows from isomorphism invariance of the *genus*.

Our proof sets $G = \mathrm{Cl}(F[E])$, and

$$\phi \text{ is injective} \iff \text{an ideal of } F[E] \text{ is not principal},$$

which is just a statement in ring theory.

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X, Y]/\langle E(X, Y)\rangle.$$

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X, Y]/\langle E(X, Y)\rangle.$$

Exercise (easy): $F[E]$ is an integral domain.

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X, Y]/\langle E(X, Y)\rangle.$$

Exercise (easy): $F[E]$ is an integral domain.

For any integral domain R, the **ideal class group** $\mathrm{Cl}(R)$ is the quotient group of *invertible fractional ideals* by those that are *principal*.

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X,Y]/\langle E(X,Y)\rangle.$$

Exercise (easy): $F[E]$ is an integral domain.

For any integral domain R, the **ideal class group** $\mathrm{Cl}(R)$ is the quotient group of *invertible fractional ideals* by those that are *principal*.

- A submodule I is a **fractional ideal** if $\exists r \in R$ such that $r \cdot I \subseteq R$.
- I is **invertible** if there is a fractional ideal J such that $I \cdot J = R$.
- I is **principal** if $\exists r, s \in R$ such that $r \cdot I = \langle s \rangle$.

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X, Y]/\langle E(X, Y)\rangle.$$

Exercise (easy): $F[E]$ is an integral domain.

For any integral domain R, the **ideal class group** $\mathrm{Cl}(R)$ is the quotient group of *invertible fractional ideals* by those that are *principal*.

- A submodule I is a **fractional ideal** if $\exists r \in R$ such that $r \cdot I \subseteq R$.
- I is **invertible** if there is a fractional ideal J such that $I \cdot J = R$.
- I is **principal** if $\exists r, s \in R$ such that $r \cdot I = \langle s\rangle$.

Exercise (hard): $\mathrm{Cl}(R)$ is an abelian group.

Algebraic analogue

The group $\mathrm{Cl}(F[E])$ is the *ideal class group* of the coordinate ring

$$F[E] := F[X, Y]/\langle E(X, Y)\rangle.$$

Exercise (easy): $F[E]$ is an integral domain.

For any integral domain R, the **ideal class group** $\mathrm{Cl}(R)$ is the quotient group of *invertible fractional ideals* by those that are *principal*.

- A submodule I is a **fractional ideal** if $\exists r \in R$ such that $r \cdot I \subseteq R$.
- I is **invertible** if there is a fractional ideal J such that $I \cdot J = R$.
- I is **principal** if $\exists r, s \in R$ such that $r \cdot I = \langle s\rangle$.

Exercise (hard): $\mathrm{Cl}(R)$ is an abelian group.

Example (of invertible fractional ideals)

Any nonzero ideal I such that $I \cdot J$ is principal for some ideal J.

Algebraic analogue

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.

- Prove that ϕ respects addition.

- Prove that ϕ is injective. $\square$

Algebraic analogue

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$. This will be

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

- Prove that ϕ respects addition.

- Prove that ϕ is injective. □

Algebraic analogue

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$. This will be

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

  Note that ϕ is well-defined since

$$\langle X-x, Y-y \rangle \cdot \langle X-x, Y-\sigma(y) \rangle = \langle X-x \rangle.$$

- Prove that ϕ respects addition.
- Prove that ϕ is injective. □

Algebraic analogue

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$. This will be

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

  Note that ϕ is well-defined since

$$\langle X-x, Y-y\rangle \cdot \langle X-x, Y-\sigma(y)\rangle = \langle X-x\rangle.$$

- Prove that ϕ respects addition. This holds since

$$\begin{aligned} \langle X-x_1, Y-y_1\rangle \cdot \langle X-x_2, Y-y_2\rangle \cdot \langle X-x_3, Y-\sigma(y_3)\rangle \\ = \langle (Y-y_3) - \lambda(X-x_3)\rangle. \end{aligned}$$

- Prove that ϕ is injective. □

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$.

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rccc} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcrcl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1 X + a_3) \cdot Y + (X^3 + a_2 X^2 + a_4 X + a_6)$.

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1X + a_3) \cdot Y + (X^3 + a_2X^2 + a_4X + a_6)$. Then

$$\mathrm{Nm}(Y) \equiv \det \begin{pmatrix} 0 & 1 \\ X^3 + a_2X^2 + a_4X + a_6 & -(a_1X + a_3) \end{pmatrix}$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccc} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1X + a_3) \cdot Y + (X^3 + a_2X^2 + a_4X + a_6)$. Then

$$\begin{aligned} \mathrm{Nm}(Y) &\equiv \det \begin{pmatrix} 0 & 1 \\ X^3 + a_2X^2 + a_4X + a_6 & -(a_1X + a_3) \end{pmatrix} \\ &= X^3 + a_2X^2 + a_4X + a_6. \end{aligned}$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1X + a_3) \cdot Y + (X^3 + a_2X^2 + a_4X + a_6)$. Then

$$\begin{aligned} \mathrm{Nm}(Y) &\equiv \det \begin{pmatrix} 0 & 1 \\ X^3 + a_2X^2 + a_4X + a_6 & -(a_1X + a_3) \end{pmatrix} \\ &= X^3 + a_2X^2 + a_4X + a_6. \end{aligned}$$

In general, if $f = p + qY \in F[E]$ for some $p, q \in F[X]$,

$$\mathrm{Nm}(f) = p^2 - pq(a_1X + a_3) - q^2(X^3 + a_2X^2 + a_4X + a_6).$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rccc} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1X + a_3) \cdot Y + (X^3 + a_2X^2 + a_4X + a_6)$. Then

$$\begin{aligned} \mathrm{Nm}(Y) &\equiv \det \begin{pmatrix} 0 & 1 \\ X^3 + a_2X^2 + a_4X + a_6 & -(a_1X + a_3) \end{pmatrix} \\ &= X^3 + a_2X^2 + a_4X + a_6. \end{aligned}$$

In general, if $f = p + qY \in F[E]$ for some $p, q \in F[X]$,

$$\mathrm{Nm}(f) = p^2 - pq(a_1X + a_3) - q^2(X^3 + a_2X^2 + a_4X + a_6).$$

This has degree $\max(2\deg(p), 2\deg(q) + 3)$.

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rccc} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Example (of norms)

Recall that $Y \cdot Y \equiv -(a_1X + a_3) \cdot Y + (X^3 + a_2X^2 + a_4X + a_6)$. Then

$$\begin{aligned} \mathrm{Nm}(Y) &\equiv \det \begin{pmatrix} 0 & 1 \\ X^3 + a_2X^2 + a_4X + a_6 & -(a_1X + a_3) \end{pmatrix} \\ &= X^3 + a_2X^2 + a_4X + a_6. \end{aligned}$$

In general, if $f = p + qY \in F[E]$ for some $p, q \in F[X]$,

$$\mathrm{Nm}(f) = p^2 - pq(a_1X + a_3) - q^2(X^3 + a_2X^2 + a_4X + a_6).$$

This has degree $\max(2\deg(p), 2\deg(q) + 3)$. In particular,

$$\deg(\mathrm{Nm}(f)) \neq 1. \qquad (\star)$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array} .$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

On one hand, $F[E]/\langle f \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$.

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

On one hand, $F[E]/\langle f \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$. Then

$$\dim(F[E]/\langle f \rangle) = \deg(p) + \deg(q).$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

On one hand, $F[E]/\langle f \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$. Then

$$\dim(F[E]/\langle f \rangle) = \deg(p) + \deg(q).$$

On the other hand, $\mathrm{Nm}(f) = pq$.

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array}.$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

On one hand, $F[E]/\langle f \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$. Then

$$\dim(F[E]/\langle f \rangle) = \deg(p) + \deg(q).$$

On the other hand, $\mathrm{Nm}(f) = pq$. Then

$$\deg(\mathrm{Nm}(f)) = \deg(p) + \deg(q).$$

Injectivity proof

Note that $F[E]$ is free over $F[X]$ with basis $\{1, Y\}$. Thus it has a **norm**

$$\begin{array}{rcccl} \mathrm{Nm} & : & F[E] & \longmapsto & F[X] \\ & & f & \longmapsto & \det([\cdot f]) \end{array} .$$

Now $[\cdot f]$ has a Smith normal form

$$[\cdot f] \sim \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}, \qquad p, q \in F[X].$$

On one hand, $F[E]/\langle f \rangle \cong F[X]/\langle p \rangle \oplus F[X]/\langle q \rangle$. Then

$$\dim(F[E]/\langle f \rangle) = \deg(p) + \deg(q).$$

On the other hand, $\mathrm{Nm}(f) = pq$. Then

$$\deg(\mathrm{Nm}(f)) = \deg(p) + \deg(q).$$

Combining both equalities and $(\star)$ yields

$$\dim(F[E]/\langle f \rangle) \neq 1. \qquad (\dagger)$$

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective.

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$.

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y\rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

$$\langle X - x, Y - y\rangle = \langle f\rangle, \qquad f \in F[E].$$

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

$$\langle X - x, Y - y \rangle = \langle f \rangle, \qquad f \in F[E].$$

Then

$$F[E]/\langle f \rangle = F[E]/\langle X - x, Y - y \rangle$$

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

$$\langle X - x, Y - y \rangle = \langle f \rangle, \qquad f \in F[E].$$

Then

$$\begin{aligned} F[E]/\langle f \rangle &= F[E]/\langle X - x, Y - y \rangle \\ &\cong F[X, Y]/\langle E(X, Y), X - x, Y - y \rangle \qquad 3^{\text{rd}} \text{ iso thm} \end{aligned}$$

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

$$\langle X - x, Y - y \rangle = \langle f \rangle, \qquad f \in F[E].$$

Then

$$\begin{aligned} F[E]/\langle f \rangle &= F[E]/\langle X - x, Y - y \rangle \\ &\cong F[X, Y]/\langle E(X, Y), X - x, Y - y \rangle && 3^{\text{rd}} \text{ iso thm} \\ &= F[X, Y]/\langle X - x, Y - y \rangle && (x, y) \in E(F) \end{aligned}$$

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

  $$\langle X - x, Y - y \rangle = \langle f \rangle, \qquad f \in F[E].$$

  Then

  $$\begin{aligned} F[E]/\langle f \rangle &= F[E]/\langle X - x, Y - y \rangle \\ &\cong F[X, Y]/\langle E(X, Y), X - x, Y - y \rangle && 3^{\text{rd}} \text{ iso thm} \\ &= F[X, Y]/\langle X - x, Y - y \rangle && (x, y) \in E(F) \\ &\cong F && 1^{\text{st}} \text{ iso thm.} \end{aligned}$$

□

Injectivity proof

Pf 5 (A.–Xu).

- Define a function $\phi : E(F) \to \mathrm{Cl}(F[E])$.
- Prove that ϕ respects addition.
- Prove that ϕ is injective. It suffices to show that $\langle X - x, Y - y \rangle$ is not principal for any $(x, y) \in E(F)$. Suppose otherwise, that

$$\langle X - x, Y - y \rangle = \langle f \rangle, \qquad f \in F[E].$$

Then

$$\begin{aligned} F[E]/\langle f \rangle &= F[E]/\langle X - x, Y - y \rangle \\ &\cong F[X, Y]/\langle E(X, Y), X - x, Y - y \rangle && 3^{\text{rd}} \text{ iso thm} \\ &= F[X, Y]/\langle X - x, Y - y \rangle && (x, y) \in E(F) \\ &\cong F && 1^{\text{st}} \text{ iso thm.} \end{aligned}$$

Since $\dim(F) = 1$, this contradicts (†)!

□

Conclusions

Some retrospectives:

- formalisation encouraged proof accessible to undergraduates
- novel injectivity proof and novel formalisation
- proof works for *nonsingular* points of *Weierstrass* curves
- heavy use of linear algebra and ring theory in Lean's `mathlib`
- generality of ideal class groups of integral domains
- plans for many more formalisation projects!

Thank you!