


# An Elementary Formal Proof of the Group Law on Weierstrass Elliptic Curves in Any Characteristic

David Kurniadi Angdinata ✉ 🏠 

London School of Geometry and Number Theory, UK

Junyan Xu ✉ 

Cancer Data Science Laboratory, National Cancer Institute, Bethesda, MD, USA

---

## Abstract

Elliptic curves are fundamental objects in number theory and algebraic geometry, whose points over a field form an abelian group under a geometric addition law. Any elliptic curve over a field admits a Weierstrass model, but prior formal proofs that the addition law is associative in this model involve either advanced algebraic geometry or tedious computation, especially in characteristic two. We formalise in the Lean theorem prover, the type of nonsingular points of a Weierstrass curve over a field of any characteristic and a purely algebraic proof that it forms an abelian group.

**2012 ACM Subject Classification** Theory of computation → Interactive proof systems; Security and privacy → Logic and verification; Mathematics of computing → Mathematical software

**Keywords and phrases** formal math, algebraic geometry, elliptic curve, group law, Lean, mathlib

**Digital Object Identifier** 10.4230/LIPIcs.ITP.2023.6

**Supplementary Material** *Software (Source Code)*: <https://github.com/alreadydone/mathlib/tree/associativity>, archived at `swh:1:dir:1bd75e80371560806d5f287177a4922b6282f7e2`

**Funding** This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], EPSRC Centre for Doctoral Training in Geometry and Number Theory (London School of Geometry and Number Theory), University College London. This research was supported in part by the Intramural Research Program of the Center for Cancer Research, National Cancer Institute, NIH.

**Acknowledgements** We thank the Lean community for their continual support. We thank the `mathlib` contributors, especially Anne Baanen, for developing libraries this work depends on. We thank Marc Masdeu and Michael Stoll for proposing alternative proofs. DKA would like to thank Kevin Buzzard for his guidance and Mel Levin for suggesting the formalisation in the first place.

## 1 Introduction

### 1.1 Elliptic curves

In its earliest form, algebraic geometry is the branch of mathematics studying the solutions to systems of polynomial equations over a base field  $F$ , namely sets of the form

$$\{(x_1, \dots, x_n) \in F^n : f_1(x_1, \dots, x_n) = 0, \dots, f_k(x_1, \dots, x_n) = 0\},$$

for some polynomials  $f_i \in F[X_1, \dots, X_n]$ . These are called **affine varieties**, and they can be endowed with topologies and a notion of morphisms which makes them simultaneously geometric objects. General **varieties** are locally modelled on affine ones, with morphisms between them locally given by polynomials, and are often classified by their geometric properties such as *smoothness*, or invariants such as the *dimension* or the *genus*.

Having dimension one and genus one, *elliptic curves* are amongst the simplest varieties with respect to these geometric notions, and their set of points can be endowed with the structure of an abelian group. When the base field is the rationals  $\mathbb{Q}$ , a common definition



© David Kurniadi Angdinata and Junyan Xu;  
licensed under Creative Commons License CC-BY 4.0

14th International Conference on Interactive Theorem Proving (ITP 2023).

Editors: Adam Naumowicz and René Thiemann; Article No. 6; pp. 6:1–6:19

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

uses the *short Weierstrass model*, given by the equation  $y^2 = x^3 + ax + b$  for some fixed  $a, b \in \mathbb{Q}$ , and its group law can be defined explicitly by quotients of polynomial functions.

Elliptic curves are blessed with an extremely rich theory, spanning the fields of algebraic geometry, complex analysis, number theory, representation theory, dynamical systems, and even information security. The *Birch and Swinnerton-Dyer conjecture* [29] in number theory, one of the seven *Millennium Prize Problems*, is an equality between an analytic quantity of an elliptic curve over  $\mathbb{Q}$  and an algebraic quantity defined in terms of its group structure. Their close relation with modular forms is precisely the content of the *Taniyama–Shimura conjecture* proven by Andrew Wiles [30], which implies *Fermat’s last theorem* and laid the foundations of the *Langlands programme*, a web of influential conjectures linking number theory and geometry described to be “kind of a grand unified theory of mathematics” [19]. Outside of mathematics, elliptic curves over finite fields see applications in primality proving [2] and integer factorisation [22], as well as in public key cryptography [13].

## 1.2 Formalisation attempts

The group law on an elliptic curve in the short Weierstrass model over a field  $F$  has been formalised in several theorem provers,<sup>1</sup> but this model fails to be an elliptic curve when  $\text{char}(F) = 2$ , and there has been no known successful attempts to formalise the group law in a *universal* model that captures all elliptic curves in all  $\text{char}(F)$ . The issue was that a computational proof of associativity in any universal model is, as Russinoff described, “an elementary but computationally intensive arithmetic exercise” involving massive polynomials [27],<sup>2</sup> while a typical conceptual proof is “a deep theorem of algebraic or projective geometry” requiring prior formalisation of advanced geometric constructions, with “evidence that an elementary hand proof of this result is a practical impossibility” [25]. On the other hand, having the group law in  $\text{char}(F) = 2$  is necessary for certain applications, such as the proof of Fermat’s last theorem. It is less crucial from an information security viewpoint, as curves over binary fields are prone to attacks and no longer recommended by NIST [9].

We give a conceptual yet computation-light proof of the group law in the full *Weierstrass model*, which is universal in all  $\text{char}(F)$ . The argument is purely algebraic and easily surveyable, in the sense that all logical deductions and necessary computations can be performed by hand in a matter of minutes. The proof is formalised in *Lean 3* [12], an interactive theorem prover based on the calculus of constructions with inductive types, and is integrated as part of its monolithic mathematical library `mathlib` [11]. The implementation extensively uses existing constructions in the linear algebra and ring theory libraries of `mathlib`, particularly constructions and results surrounding `algebra.norm` and `class_group` [10]. The relevant code is primarily split into two files `weierstrass.lean` and `point.lean` under the folder `algebraic_geometry/elliptic_curve` in the `associativity` branch of `mathlib`, both of which are currently undergoing reviews for their merge. With this paper, we hope that our simple proof will be replicated and will open the way for the formalisation of elliptic curve cryptography in many other theorem provers, which has been a major motivation of recent formalisation attempts [25, 15, 18, 4].

The remainder of this paper will describe the relevant constructions (Section 2), detail the mathematical argument of the proof (Section 3), and discuss implementation considerations (Section 4). Throughout, definitions will be described in code snippets where relevant, but proofs of lemmas will be outlined mathematically for the sake of clarity. The reader may refer to the `mathlib` documentation [10] for definitions and lemmas involved.

<sup>1</sup> see Section 4.1 for related work

<sup>2</sup> see Section 4.2 for experimental results

## 2 Weierstrass equations

Let  $F$  be a field. In the sense of modern algebraic geometry, an **elliptic curve**  $E$  over  $F$  is a smooth projective curve<sup>3</sup> of genus one equipped with a base point  $\mathcal{O}_E \in E$  with coordinates in  $F$ . More concretely, any elliptic curve over  $F$  admits a model in the projective plane  $\mathbb{P}_F^2$  defined by an explicit polynomial equation in homogeneous coordinates  $[X : Y : Z]$ .

► **Proposition 1.** *If  $E$  is an elliptic curve over  $F$ , then there are rational functions  $x, y : E \rightarrow F$  such that the map  $\phi : E \rightarrow \mathbb{P}_F^2$  given by  $\phi(P) = [x(P) : y(P) : 1]$  maps  $\mathcal{O}_E$  to  $[0 : 1 : 0]$ , and defines an isomorphism of varieties between  $E$  and the curve*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

for some coefficients  $a_i \in F$ . Conversely, any curve  $W$  in  $\mathbb{P}_F^2$  given by such an equation, with coefficients  $a_i \in F$ , is an elliptic curve over  $F$  with base point  $[0 : 1 : 0]$  if the quantity

$$\begin{aligned} \Delta_W := & -(a_1^2 + 4a_2)^2(a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2) - 8(2a_4 + a_1a_3)^3 \\ & - 27(a_3^2 + 4a_6)^2 + 9(a_1^2 + 4a_2)(2a_4 + a_1a_3)(a_3^2 + 4a_6) \in F \end{aligned}$$

is nonzero.

**Proof.** This is a consequence of the Riemann–Roch theorem [26, Proposition III.3.1]. ◀

This is the **Weierstrass model** of  $E$ , and such a curve is called a **Weierstrass curve**, whose corresponding **Weierstrass equation** in the affine chart  $Z \neq 0$  is

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

In this model, the smoothness condition on  $E$  becomes equivalent to the **discriminant**  $\Delta_E \in F$  being nonzero, so an elliptic curve over  $F$  may instead be defined as a Weierstrass curve with the discriminant condition, which is more amenable for computational purposes.

### 2.1 Weierstrass curves

Let  $F$  be a commutative ring, and let  $W$  be a Weierstrass curve over  $F$ . Explicitly, this is merely the data of five coefficients  $a_1, a_2, a_3, a_4, a_6 \in F$ , noting that the Weierstrass equation is not visible at this stage. For the sake of generality, the structure `weierstrass_curve` is defined more generally over an arbitrary type  $F$ , but all subsequent constructions will assume that  $F$  is at least a commutative ring. The structure `elliptic_curve` then **extends** `weierstrass_curve` by adding the data of an element  $\Delta'$  in the group of units  $F^\times$  of  $F$  and a proof that  $\Delta' = \Delta_W$ , so most definitions for `weierstrass_curve` carry over automatically.

```
structure weierstrass_curve (F : Type) := (a1 a2 a3 a4 a6 : F)

structure elliptic_curve (F : Type) [comm_ring F] extends weierstrass_curve F :=
  (Δ' : F×) (coe_Δ' : ↑Δ' = to_weierstrass_curve.Δ)
```

Here, `to_weierstrass_curve` is a function generated automatically by the `extends` keyword, which projects an `elliptic_curve` down to its underlying `weierstrass_curve` by forgetting  $\Delta'$  and the proof that  $\Delta' = \Delta_W$ . Note that `elliptic_curve` was originally defined in one stretch by Buzzard, but is now refactored through the more general `weierstrass_curve`.

<sup>3</sup> variety of dimension one

## 6:4 The Group Law on Weierstrass Elliptic Curves

► Remark 2. This definition of an elliptic curve is universal over a large class of commutative rings, namely those with trivial Picard group [21, Section 2.2], which includes fields, and also local rings and unique factorisation domains. In general, an elliptic curve  $E$  may be defined relative to an arbitrary scheme  $S$  as a smooth proper morphism  $E \rightarrow S$  in the category of schemes whose geometric fibres are all integral curves of genus one, equipped with a section  $S \rightarrow E$  that plays the role of the base point  $\mathcal{O}_E$  for all fibres simultaneously. When  $S$  is the spectrum of such a commutative ring, the Riemann–Roch theorem can be generalised so that  $E$  remains isomorphic to a Weierstrass curve, but over a general commutative ring,  $E$  only has Weierstrass equations locally that may not patch together to form a global equation.

The discriminant  $\Delta_W \in F$  is expressed entirely in terms of the five coefficients, but it is clearer to extract intermediate quantities [26, Section III.1] to simplify the large expression.

```
namespace weierstrass_curve

variables {F : Type} [comm_ring F] (W : weierstrass_curve F)

def b2 : F := W.a1^2 + 4*W.a2
def b4 : F := 2*W.a4 + W.a1*W.a3
def b6 : F := W.a3^2 + 4*W.a6
def b8 : F := W.a1^2*W.a6 + 4*W.a2*W.a6 - W.a1*W.a3*W.a4 + W.a2*W.a3^2 - W.a4^2

def Δ : F := -W.b2^2*W.b8 - 8*W.b4^3 - 27*W.b6^2 + 9*W.b2*W.b4*W.b6
```

Here, dot notation allows for the fields corresponding to the five coefficients  $a_i \in F$  to be accessed as  $W.a_i$ , and living inside the namespace `weierstrass_curve` means that the quantities  $b_i \in F$  and  $\Delta \in F$  may also be accessed as  $W.b_i$  and  $W.\Delta$  respectively.

These quantities are indexed as such as a result of their transformation upon applying the linear change of variables  $(X, Y) \mapsto (u^2X + r, u^3Y + u^2sX + t)$ , for some  $u \in F^\times$  and some  $r, s, t \in F$ . In fact, these are all the possible isomorphisms of varieties between elliptic curves in the Weierstrass model [26, Proposition III.3.1].

```
variables (u : F×) (r s t : F)

@[simps] def variable_change : weierstrass_curve F :=
{ a1 := ↑u-1*(W.a1 + 2*s),
  a2 := ↑u-1*2*(W.a2 - s*W.a1 + 3*r - s^2),
  a3 := ↑u-1*3*(W.a3 + r*W.a1 + 2*t),
  a4 := ↑u-1*4*(W.a4 - s*W.a3 + 2*r*W.a2 - (t + r*s)*W.a1 + 3*r^2 - 2*s*t),
  a6 := ↑u-1*6*(W.a6 + r*W.a4 + r^2*W.a2 + r^3 - t*W.a3 - t^2 - r*t*W.a1) }

@[simp] lemma variable_change_b2 : (W.variable_change u r s t).b2 = ↑u-1*2*(...)
@[simp] lemma variable_change_b4 : (W.variable_change u r s t).b4 = ↑u-1*4*(...)
@[simp] lemma variable_change_b6 : (W.variable_change u r s t).b6 = ↑u-1*6*(...)
@[simp] lemma variable_change_b8 : (W.variable_change u r s t).b8 = ↑u-1*8*(...)

@[simp] lemma variable_change_Δ : (W.variable_change u r s t).Δ = ↑u-1*12*W.Δ
```

Here, `variable_change` defines a new `weierstrass_curve` under the change of variables by explicitly stating how each of the five coefficients are transformed, and is tagged with `simps` to automatically generate `simp` lemmas corresponding to each of the five projections. The exact expressions for the transformed quantities are not too important, but note that their indices precisely correspond to the exponent of  $u^{-1} \in F^\times$  in the transformation.

## 2.2 Equations and nonsingularity

Now consider the polynomial in  $F[X, Y]$  associated to  $W$  denoted by

$$W(X, Y) := Y^2 + (a_1X + a_3)Y - (X^3 + a_2X^2 + a_4X + a_6),$$

so that the Weierstrass equation literally reads  $W(X, Y) = 0$ , and its partial derivatives

$$W_X(X, Y) := a_1Y - (3X^2 + 2a_2X + a_4), \quad W_Y(X, Y) := 2Y + a_1X + a_3.$$

When they do not simultaneously vanish when evaluated at an affine point  $(x, y) \in W$ , the affine point is said to be **nonsingular**. This is implemented slightly confusingly as follows.<sup>4</sup>

```
def polynomial : F[X][Y] :=
  Y^2 + C (C W.a1*X + C W.a3)*Y - C (X^3 + C W.a2*X^2 + C W.a4*X + C W.a6)
def equation (x y : F) : Prop := (W.polynomial.eval (C y)).eval x = 0

def polynomial_X : F[X][Y] := C (C W.a1)*Y - C (C 3*X^2 + C (2*W.a2)*X + C W.a4)
def polynomial_Y : F[X][Y] := C (C 2)*Y + C (C W.a1*X + C W.a3)
def nonsingular (x y : F) : Prop :=
  W.equation x y ^ ((W.polynomial_X.eval (C y)).eval x ≠ 0
    ∨ (W.polynomial_Y.eval (C y)).eval x ≠ 0)
```

Here,  $F[X][Y]$  denotes the polynomial ring over the polynomial ring over  $F$ , to simulate the bivariate polynomial ring  $F[X, Y]$  over  $F$ . The outer variable  $Y$  is denoted by the symbol  $Y$  and the inner variable  $X$  is denoted by the constant function  $C$  applied to the symbol  $X$ , while actual constants are enclosed in two layers of the constant function  $C$ .

► Remark 3. This definition of nonsingularity in terms of partial derivatives is valid and convenient when the base ring is a field, but over a general commutative ring the same notion should be characterised locally with a notion of smoothness relative to the base spectrum.

Many properties of Weierstrass curves remain invariant under the aforementioned changes of variables, and it is often easier to prove results for Weierstrass equations with fewer terms. For instance, if  $\text{char}(F) \neq 2$ , then  $(X, Y) \mapsto (X, Y - \frac{1}{2}a_1X - \frac{1}{2}a_3)$  completes the square for  $W(X, Y)$  and eliminates the  $XY$  and  $Y$  terms, and if further  $\text{char}(F) \neq 3$ , then  $(X, Y) \mapsto (X - \frac{1}{12}b_2, Y)$  completes the cube for  $W(X, Y)$  and eliminates the  $X^2$  term as well.

Perhaps a more prominent application is the proof that, for any affine point  $(x, y) \in W$ , the nonvanishing of  $\Delta_W$  implies that  $(x, y)$  is nonsingular. This statement is easy for  $(x, y) = (0, 0)$ , since  $(0, 0) \in W$  implies that  $a_6 = 0$ , and  $(0, 0)$  being singular implies that  $a_3 = a_4 = 0$ , so that  $\Delta_W = 0$  by a simple substitution. On the other hand, for any  $(x, y) \in F^2$ , the change of variables  $(X, Y) \mapsto (X - x, Y - y)$  merely translates  $W$  so that  $(0, 0)$  gets mapped to  $(x, y)$ , so the same statement clearly also holds for  $(x, y)$ .

```
lemma nonsingular_zero : W.nonsingular 0 0 ↔ W.a6 = 0 ∧ (W.a3 ≠ 0 ∨ W.a4 ≠ 0)
lemma nonsingular_zero_of_Δ_ne_zero (h : W.equation 0 0) (hΔ : W.Δ ≠ 0) :
  W.nonsingular 0 0
lemma nonsingular_iff_variable_change (x y : F) :
  W.nonsingular x y ↔ (W.variable_change 1 x 0 y).nonsingular 0 0
lemma nonsingular_of_Δ_ne_zero {x y : F} (h : W.equation x y) (hΔ : W.Δ ≠ 0) :
  W.nonsingular x y
```

In fact, it is also true that  $\Delta_W \neq 0$  if every point over the algebraic closure is nonsingular [26, Proposition III.1.4], but the proof is more difficult and has yet to be formalised.

<sup>4</sup> this representation of bivariate polynomials will be explained in Section 4.3

## 2.3 Point addition

The set of points on an elliptic curve can be endowed with an **addition law** defined by a geometric secant-and-tangent process enabled by Vieta's formulae.<sup>5</sup> This can be easily described in the Weierstrass model, where a point on  $W$  is either of the form  $(x, y)$  in the affine chart  $Z \neq 0$  and satisfies the Weierstrass equation, or is the unique point at infinity  $\mathcal{O}_W := [0 : 1 : 0]$  when  $Z = 0$ . If  $S \in W$  is a singular point, the same geometric process will yield  $P + S = S = S + P$  for any other point  $P \in W$ , so it necessitates considering only nonsingular points on  $W$  to obtain a group [26, Section III.2]. Note that if  $W$  is an elliptic curve, then all points are nonsingular by `nonsingular_of_Δ_ne_zero`.

```
inductive point
| zero
| some {x y : F} (h : W.nonsingular x y)

namespace point
```

Here, `zero` refers to  $\mathcal{O}_W$  and `some` refers to an affine point on  $W$ . Note that a proof that an affine point  $(x, y) \in W$  is nonsingular already subsumes the data of the coordinates  $(x, y) \in F^2$  in its type, so such a point is constructed by giving only the proof.

► **Remark 4.** The set of points defined here will later be shown to form an abelian group under this addition law, but the presence of division means that the base ring needs to be a field. Over a general commutative ring  $R$  these should be replaced with scheme-theoretic points  $\text{Spec}(R) \rightarrow E$ , and the elliptic curve acquires the structure of a group scheme.

In this model, the identity element in the group of points is defined to be  $\mathcal{O}_W \in W$ .

```
instance : has_zero W.point := ⟨zero⟩
```

Here, the `instance` of `has_zero` allows the notation `0` instead of `zero`.

Given a nonsingular point  $P \in W$ , its negation  $-P$  is defined to be the unique third point of intersection between  $W$  and the line through  $\mathcal{O}_W$  and  $P$ , which is vertical when drawn on the affine plane. Explicitly, if  $P := (x, y)$ , then  $-P := (x, \sigma_x(y))$ , where

$$\sigma_x(Y) := -Y - (a_1X + a_3)$$

is the **negation polynomial**, which gives a very useful involution of the affine plane.

```
def neg_polynomial : F[X][Y] := -Y - C (C W.a1*x + C W.a3)
def neg_Y (x y : F) : F := (W.neg_polynomial.eval (C y)).eval x
```

Here, `neg_Y` is defined in terms of `neg_polynomial` for clarity, but its actual definition is written out as `-y - C (C W.a1*x + C W.a3)`. This is merely to avoid requiring the `noncomputable` tag, since polynomial operations are currently `noncomputable` in `mathlib`.

To define negation, it remains to prove that the negation of a nonsingular point on  $W$  is again a nonsingular point on  $W$ , but this is straightforward.

► **Lemma 5.** *If  $(x, y) \in W$  is nonsingular, then  $(x, \sigma_x(y)) \in W$  is nonsingular.*

**Proof.** Since  $(x, y) \in W$ , verifying that  $W(x, y) = W(x, \sigma_x(y))$  gives  $(x, \sigma_x(y)) \in W$  as well. Now assume that  $W_Y(x, \sigma_x(y)) = 0$ . It can be checked that  $y = \sigma_x(y)$ , so  $W_Y(x, y) = 0$  as well. Since  $(x, y)$  is nonsingular,  $W_X(x, y) \neq 0$ , so  $W_X(x, \sigma_x(y)) \neq 0$  as well. ◀

<sup>5</sup> if a cubic polynomial has two roots in a field, then its third root is also in the field

Lemma 5 is `nonsingular_neg`, which maps a proof that  $(x, y) \in W$  is nonsingular to a proof that  $-(x, y) \in W$  is nonsingular. This leads to the definition of negation.

```
def neg : W.point → W.point
| 0      := 0
| (some h) := some (nonsingular_neg h)

instance : has_neg W.point := ⟨neg⟩
```

Here, the `instance` of `has_neg` allows the notation  $-P$  instead of `neg P`.

Given two nonsingular points  $P_1, P_2 \in W$ , their sum  $P_1 + P_2$  is defined to be the negation of the unique third point of intersection between  $W$  and the line through  $P_1$  and  $P_2$ , which again exists by Bézout's theorem. Explicitly, let  $P_1 := (x_1, y_1)$  and  $P_2 := (x_2, y_2)$ .

- If  $x_1 = x_2$  and  $y_1 = \sigma_{x_2}(y_2)$ , then this line is vertical and  $P_1 + P_2 := \mathcal{O}_W$ .
- If  $x_1 = x_2$  and  $y_1 \neq \sigma_{x_2}(y_2)$ , then this line is the tangent of  $W$  at  $P_1 = P_2$ , and has slope

$$\ell := \frac{-W_X(x_1, y_1)}{W_Y(x_1, y_1)}.$$

- Otherwise  $x_1 \neq x_2$ , then this line is the secant of  $W$  through  $P_1$  and  $P_2$ , and has slope

$$\ell := \frac{y_1 - y_2}{x_1 - x_2}.$$

In the latter two cases, the **line polynomial**

$$\lambda(X) = \lambda_{x_1, y_1, \ell}(X) := \ell(X - x_1) + y_1.$$

can be shown to satisfy  $\lambda(x_1) = y_1$  and  $\lambda(x_2) = y_2$ , so that  $x_1$  and  $x_2$  are two roots of the **addition polynomial**  $W(X, \lambda(X))$ , obtained by evaluating  $W(X, Y)$  at  $\lambda(X)$ , where  $W(X, Y)$  is viewed as a polynomial over  $F[X]$ . In an attempt to reduce code duplication for the different cases, these accept an additional parameter `L` for the slope  $\ell$ .

```
def line_polynomial (x y L : F) : F[X] := C L * (X - C x) + C y
def add_polynomial (x y L : F) : F[X] := W.polynomial.eval (line_polynomial x y L)
```

The  $X$ -coordinate of  $P_1 + P_2$  is then the third root of  $W(X, \lambda(X))$ , so that

$$W(X, \lambda(X)) = -(X - x_1)(X - x_2)(X - x_3). \quad (1)$$

By inspecting the  $X^2$  terms of  $W(X, \lambda(X))$ , this third root can be shown to be

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

so the  $Y$ -coordinate of  $-(P_1 + P_2)$  is

$$y'_3 := \lambda(x_3),$$

and that of  $P_1 + P_2$  is

$$y_3 := \sigma_{x_3}(y'_3).$$

These correspond to the coordinate functions `add_X`, `add_Y'`, and `add_Y` respectively.

```
def add_X (x1 x2 L : F) : F := L^2 + W.a1*L - W.a2 - x1 - x2
def add_Y' (x1 x2 y1 L : F) : F := (line_polynomial x1 y1 L).eval (W.add_X x1 x2 L)
def add_Y (x1 x2 y1 L : F) : F := W.neg_Y (W.add_X x1 x2 L) (W.add_Y' x1 x2 y1 L)
```

Here, `add_Y'` is defined in terms of `line_polynomial` and `add_X`, but in actuality it is again written out in the evaluated form  $C L * (X - C x_1) + C y_1$  to avoid the `noncomputable` tag.

## 6:8 The Group Law on Weierstrass Elliptic Curves

The slope itself is defined as a conditional over the three cases, and since two of them involve division, this is the first occasion where  $W$  needs to be defined over a field  $F$ .

```
variables {F : Type} [field F] (W : weierstrass_curve F)

def slope (x1 x2 y1 y2 : F) : F :=
  if hx : x1 = x2 then
    if hy : y1 = W.neg_Y x2 y2 then 0
    else (3*x1^2 + 2*W.a2*x1 + W.a4 - W.a1*y1)/(y1 - W.neg_Y x1 y1)
  else (y1 - y2)/(x1 - x2)
```

Note that `slope` returns the *junk value* of  $0 \in F$  when the slope is vertical. This practice of assigning a junk value is common in `mathlib` to avoid excessive layers of `option`, and any useful result proven using such a definition would include a condition so that this junk value will never be reached. In the case of `slope`, this is the implication  $x_1 = x_2 \rightarrow y_1 \neq \sigma_{x_2}(y_2)$ , which holds precisely either when  $x_1 \neq x_2$ , or when  $x_1 = x_2$  but  $(x_1, y_1) \neq -(x_2, y_2)$ .

```
variables {x1 x2 y1 y2 : F} (hxy : x1 = x2 → y1 ≠ W.neg_Y x2 y2)

example (hx : x1 ≠ x2) : x1 = x2 → y1 ≠ W.neg_Y x2 y2 := λ h, (hx h).elim
example (hy : y1 ≠ W.neg_Y x2 y2) : x1 = x2 → y1 ≠ W.neg_Y x2 y2 := λ _, hy
```

Here, the examples return proofs of `hxy` assuming  $x_1 \neq x_2$  and  $y_1 \neq \sigma_{x_2}(y_2)$  respectively. They are illustrated here for clarity, but they do not exist in the actual Lean code since their term mode proofs are short enough to be inserted directly whenever necessary.

To define addition, it remains to prove that the addition of two nonsingular points on  $W$  is again a nonsingular point on  $W$ . This is slightly lengthy but purely conceptual.

► **Lemma 6.** *If  $(x_1, y_1), (x_2, y_2) \in W$  are nonsingular, then  $(x_3, y_3) \in W$  is nonsingular.*

**Proof.** By `nonsingular_neg`, it suffices to prove that  $(x_3, \lambda(x_3)) = (x_3, y_3')$  is nonsingular, since  $(x_3, \lambda(x_3)) \in W$  is clear. Taking derivatives of both sides in (1) yields

$$W_X(X, \lambda(X)) + \ell \cdot W_Y(X, \lambda(X)) = -((X - x_1)(X - x_2) + (X - x_1)(X - x_3) + (X - x_2)(X - x_3)),$$

which does not vanish at  $X = x_3$ , so that  $W(X, \lambda(X))$  has at least one nonvanishing partial derivative, unless possibly when  $x_3 \in \{x_1, x_2\}$ . The latter implies that  $(x_3, \lambda(x_3)) \in \{\pm(x_1, y_1), \pm(x_2, y_2)\}$ , but these are nonsingular by assumption or by `nonsingular_neg`. ◀

Lemma 6 is `nonsingular_add`, which accepts a proof that  $(x_1, y_1) \in W$  is nonsingular, a proof that  $(x_2, y_2) \in W$  is nonsingular, and a proof of `hxy`, and returns a proof that  $(x_1, y_1) + (x_2, y_2) \in W$  is nonsingular. This finally leads to the definition of addition.

```
def add : W.point → W.point → W.point
| 0 P := P
| P 0 := P
| (@some _ _ _ x1 y1 h1) (@some _ _ _ x2 y2 h2) :=
  if hx : x1 = x2 then
    if hy : y1 = W.neg_Y x2 y2 then 0
    else some (nonsingular_add h1 h2 (λ _, hy))
  else some (nonsingular_add h1 h2 (λ h, (hx h).elim))

instance : has_add W.point := ⟨add⟩
```

Here, the `instance` of `has_add` allows the notation  $P_1 + P_2$  instead of `add P1 P2`. The annotation `@` for `some` simply gives access to all implicit variables in its definition, particularly  $x_1, x_2, y_1, y_2 \in F$  that is necessary to even state the conditions `hx` and `hy`.



### 3 Group law

Let  $W$  be a Weierstrass curve over a field  $F$ , and denote its set of nonsingular points by  $W(F)$ . The addition law defined in the previous section is in fact a **group law**.

► **Proposition 7.**  $W(F)$  forms an abelian group under this addition law.

The axioms of this group law are mostly straightforward, typically just by examining the definition for each of the five cases. For instance, the `lemma add_left_neg` that says  $-P + P = \mathcal{O}_W$  is immediate, since  $-\mathcal{O}_W + \mathcal{O}_W = \mathcal{O}_W$  by definition, and  $-(x, y) + (x, y) = (x, \sigma_x(y)) + (x, y) = \mathcal{O}_W$  for any  $(x, y) \in W(F)$  by the first case of affine addition.

On the other hand, associativity is far from being straightforward.<sup>6</sup> A notable algebro-geometric proof involves canonically identifying  $W(F)$  with its *Picard group*, a natural geometric construction associated to  $W$  with a known group structure, and proving that this identification respects the addition law on  $W$  [26, Proposition III.3.4]. This is generally regarded as the most conceptual proof, as it explains the seemingly arbitrary secant-and-tangent process, and more crucially because it works for any  $\text{char}(F)$ .

The proof in this paper is an analogue of this proof, but the arguments involved are purely algebraic without the need for any geometric machinery, in contrast to the typical algebro-geometric proof. The main idea, originally inspired by Buzzard's post on Zulip [6] and Chapman's answer on MathOverflow [8], is to construct an explicit function `to_class` from  $W(F)$  to the *ideal class group*  $\text{Cl}(R)$  of an integral domain  $R$  associated to  $W$ , then to prove that this function is injective and respects the addition law on  $W$ . This is a construction in commutative algebra whose definition will now be briefly outlined, but for a more comprehensive introduction to ideal class groups motivated by arithmetic examples, and especially specific details of their formalisation in `mathlib`, the reader is strongly urged to consult the original paper by Baanen, Dahmen, Narayanan, and Nuccio [3, Section 2].

#### 3.1 Ideal class group of the coordinate ring

Given an integral domain  $R$  with a fraction field  $K$ , a **fractional ideal** of  $R$  is simply a  $R$ -submodule  $I$  of  $K$  such that  $x \cdot I \subseteq R$  for some nonzero  $x \in R$ . This generalises the notion of an ideal of  $R$ , since any ideal is clearly a fractional ideal with  $x = 1$ , so ideals are sometimes referred to as **integral ideals** to distinguish them from fractional ideals.

In `mathlib`, this is expressed as a transitive coercion from `ideal` to `fractional_ideal`.

```
instance : has_coe_t (ideal R) (fractional_ideal R0 (fraction_ring R))
```

Here,  $R^0$  is the submonoid of non-zero-divisors of  $R$ , and `fraction_ring` returns the canonical choice of a fraction field of  $R$  obtained by adjoining inverses of elements of  $R^0$ . Since  $R$  is an integral domain in this case, all nonzero elements of  $R$  become invertible in its fraction field.

Analogously to integral ideals, the set of fractional ideals of  $R$  forms a commutative semiring under the usual operations of addition and multiplication for submodules. A fractional ideal  $I$  of  $R$  is **invertible** if  $I \cdot J = R$  for some fractional ideal  $J$  of  $R$ , and the subset of invertible fractional ideals of  $R$  forms an abelian group under multiplication. An important class of invertible fractional ideals are those generated by a nonzero element of  $K$ , called **principal fractional ideals**. The **ideal class group**  $\text{Cl}(R)$  of  $R$  is then defined to be the quotient group of invertible fractional ideals by principal fractional ideals.

<sup>6</sup> see Section 4.2 for alternative proofs

## 6:10 The Group Law on Weierstrass Elliptic Curves

In `mathlib`, a `class_group` element is constructed from an invertible `fractional_ideal` via `class_group.mk`, and this association is a `monoid_hom` that respects multiplication.

```
def class_group.mk : (fractional_ideal R0 K)× →* class_group R := ...
```

Here, it is worth noting that  $\text{Cl}(R)$  is typically defined only when  $R$  is **Dedekind**, namely when every nonzero fractional ideal is invertible, and in such domains, `class_group.mk` constructs a `class_group` element directly from a nonzero `fractional_ideal`.

The integral domain in consideration is the **coordinate ring** of  $W$ , that is

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

whose fraction field is the **function field**  $F(W) := \text{Frac}(F[W])$  of  $W$ .

```
@[derive comm_ring] def coordinate_ring : Type := adjoin_root W.polynomial
abbreviation function_field : Type := fraction_ring W.coordinate_ring

namespace coordinate_ring
```

Here,  $W(X, Y)$  is viewed as a quadratic monic polynomial with coefficients in  $F[X]$ , so `adjoin_root` constructs the quotient ring  $F[W]$  by adjoining its root  $Y$ . The tag `derive comm_ring` automatically generates an `instance` of `comm_ring` present in `adjoin_root`,<sup>7</sup> while `abbreviation` is just a `def` that inherits every `instance` from `fraction_ring`.

A priori,  $F[W]$  is only a commutative ring, but for  $\text{Cl}(F[W])$  to make sense it needs to be at least an integral domain, which is straightforward from the shape of  $W(X, Y)$ .

► **Lemma 8.**  *$F[W]$  is an integral domain.*

**Proof.** It suffices to prove that  $W(X, Y)$  is prime, but  $F[X, Y]$  is a unique factorisation domain since  $F$  is a field, so it suffices to prove that  $W(X, Y)$  is irreducible. Suppose for a contradiction that it were reducible as a product of two factors. Since it is a monic polynomial in  $Y$ , the leading coefficients of the two factors multiply to 1, so without loss of generality

$$W(X, Y) = (Y - p(X))(Y - q(X)),$$

for some polynomials  $p(X), q(X) \in F[X]$ . Comparing coefficients yields

$$a_1X + a_3 = -(p(X) + q(X)), \quad -(X^3 + a_2X^2 + a_4X + a_6) = p(X)q(X),$$

which cannot simultaneously hold by considering  $\deg_X(p(X))$  and  $\deg_X(q(X))$ . ◀

Lemma 8 is formalised as an `instance` of `is_domain` for `W.coordinate_ring`. In fact,  $F[W]$  is also Dedekind when  $\Delta_W \neq 0$ , but this will not be necessary in the proof.

► **Remark 9.** This argument with ideal class groups is essentially an algebraic translation of the algebro-geometric argument with Picard groups. An invertible fractional ideal on an integral domain  $R$  is equivalent to an invertible sheaf on its spectrum  $\text{Spec}(R)$ , so the Picard group  $\text{Pic}(\text{Spec}(F[W]))$  of invertible sheaves is precisely the ideal class group  $\text{Cl}(F[W])$  of invertible fractional ideals [20, Example II.6.3.2]. Note that an invertible  $R$ -submodule of  $\text{Frac}(R)$  is automatically a fractional ideal of  $R$  [14, Theorem 11.6], so the ideal class group may also be defined purely in the language of invertible submodules.

<sup>7</sup> this has a type unification performance issue that will be detailed in Section 4.3

### 3.2 Construction of `to_class`

The function `to_class` will map a nonsingular affine point  $(x, y) \in W(F)$  to the class of the invertible fractional ideal arising from the integral ideal  $\langle X - x, Y - y \rangle$ . Defining the integral ideal explicitly is straightforward, and its associated fractional ideal is obtained by coercion.

```
def XY_ideal (x : F) (y : F[X]) : ideal W.coordinate_ring :=
  ideal.span {adjoin_root.mk W.polynomial (C (X - C x)),
             adjoin_root.mk W.polynomial (Y - C y)}
```

Here, `ideal.span` constructs an integral ideal generated by the elements of a specified set, and `adjoin_root.mk W.polynomial` is the canonical quotient map  $F[X, Y] \rightarrow F[W]$ . Note also that `XY_ideal` is defined slightly more generally than described, by allowing the second argument to be a polynomial in  $F[X]$  rather than just a constant.

On the other hand, checking that `XY_ideal` is indeed invertible is slightly fiddly.

► **Lemma 10.** *For any  $(x, y) \in W(F)$ ,*

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

**Proof.** Since  $W(x, y) = 0$ , there is an identity in  $F[W]$  given by

$$(Y - y)(Y - \sigma_x(y)) \equiv (X - x)(X^2 + (x + a_2)X + (x^2 + a_2x + a_4) - a_1Y),$$

so the required equality may be reduced to  $\langle X - x \rangle \cdot I = \langle X - x \rangle$  in  $F[X, Y]$ , where

$$I := \langle X - x, Y - y, Y - \sigma_x(y), X^2 + (x + a_2)X + (x^2 + a_2x + a_4) - a_1Y \rangle.$$

Since  $(x, y)$  is nonsingular, either  $W_X(x, y) \neq 0$  or  $W_Y(x, y) \neq 0$ , but

$$W_X(x, y) = -(X + 2x + a_2)(X - x) + a_1(Y - y) + (X^2 + (x + a_2)X + (x^2 + a_2x + a_4) - a_1Y),$$

and  $W_Y(x, y) = -(Y - y) + (Y - \sigma_x(y))$ , so  $I = F[X, Y]$  in both cases. ◀

► **Remark 11.** Geometrically, Lemma 10 says that the line  $X = x$  intersects  $W$  at  $\mathcal{O}_W$  and at precisely two affine points  $(x, y)$  and  $(x, \sigma_x(y))$ , counted with multiplicity if they are equal.

Lemma 10 is `XY_ideal_neg_mul`, and it follows that the fractional ideal  $\langle X - x, Y - y \rangle$  has inverse  $\langle X - x, Y - \sigma_x(y) \rangle \cdot \langle X - x \rangle^{-1}$ . This is formalised as `XY_ideal'_mul_inv`, which maps a proof that  $(x, y) \in W$  is nonsingular to a proof that the fractional ideal  $\langle X - x, Y - y \rangle$  has the specified right inverse. Passing this proof to `units.mk_of_mul_eq_one` then constructs the invertible fractional ideal of  $F[W]$  associated to  $\langle X - x, Y - y \rangle$ .

```
def XY_ideal' (h : W.nonsingular x y) :
  (fractional_ideal W.coordinate_ring0 W.function_field)× :=
  units.mk_of_mul_eq_one _ _ (XY_ideal'_mul_inv h)
```

Now `to_class` will be a `add_monoid_hom`, namely a function bundled with proofs that it maps zero to zero and respects addition. Its underlying unbundled function  $W(F) \rightarrow \text{Cl}(F[W])$ , appropriately named `to_class_fun`, is defined separately to allow the equation compiler to generate lemmas automatically used in the proof that `to_class` respects addition.

```
def to_class_fun : W.point → additive (class_group W.coordinate_ring)
| 0 := 0
| (some h) := additive.of_mul (class_group.mk (XY_ideal' h))
```

Here, `additive G` creates a type synonym of a multiplicative group  $G$ , and the multiplicative group instance on  $G$  is turned into an additive `add_group` instance on `additive G`. This is necessary to bundle `to_class` as an `add_monoid_hom`, since `mathlib` does not have homomorphisms between an additive group and a multiplicative group by design.

## 6:12 The Group Law on Weierstrass Elliptic Curves

Now `to_class_fun` maps zero to zero by construction, but proving that it respects addition requires checking the five cases for `add` separately. The first two cases are trivial and the third case follows from `XY_ideal_neg_mul`, while the last two cases are handled simultaneously by assuming `hxy` and checking an identity of integral ideals of  $F[W]$ .

► **Lemma 12.** *For any  $(x_1, y_1), (x_2, y_2) \in W(F)$ , if  $x_1 = x_2$  implies  $y_1 \neq \sigma_{x_2}(y_2)$ , then*

$$\langle X - x_1, Y - y_1 \rangle \cdot \langle X - x_2, Y - y_2 \rangle \cdot \langle X - x_3 \rangle = \langle X - x_3, Y - y_3 \rangle \cdot \langle Y - \lambda(X) \rangle,$$

where  $(x_3, y_3) := (x_1, y_1) + (x_2, y_2)$ .

**Proof.** In both valid cases of `hxy`, the line  $Y = \lambda(X)$  contains  $(x_1, y_1)$  and  $(x_2, y_2)$ , so

$$\langle X - x_1, Y - y_1 \rangle = \langle X - x_1, Y - \lambda(X) \rangle, \quad \langle X - x_2, Y - y_2 \rangle = \langle X - x_2, Y - \lambda(X) \rangle.$$

Furthermore, by (1) and the identity  $W(X, \lambda(X)) \equiv (Y - \lambda(X))(\sigma_X(Y) - \lambda(X))$  in  $F[W]$ , the required equality is reduced to checking that  $I := \langle X - x_1, X - x_2, Y - \sigma_X(Y) \rangle$  satisfies

$$I \cdot \langle X - x_3 \rangle + \langle \sigma_X(Y) - \lambda(X) \rangle = \langle X - x_3, Y - y_3 \rangle,$$

where  $Y - \lambda(X)$  has been replaced by  $Y - \sigma_X(Y)$  in  $I$  since  $\sigma_X(Y) - \lambda(X)$  is present as a summand in the left hand side. By construction, the line  $Y = \lambda(X)$  contains  $(x_3, \lambda(x_3))$ , so the negated line  $\sigma_X(Y) = \lambda(X)$  contains its negation  $(x_3, \sigma_{x_3}(\lambda(x_3))) = (x_3, y_3)$ . Then

$$\langle X - x_3, Y - y_3 \rangle = \langle X - x_3, \sigma_X(Y) - \lambda(X) \rangle,$$

so it suffices to check that  $I = F[W]$ . Now  $x_1 - x_2 = -(X - x_1) + (X - x_2)$ , so  $I = F[W]$  if  $x_1 \neq x_2$ . Otherwise  $y_1 \neq \sigma_{x_1}(y_1)$ , then there are no common solutions to  $Y = \sigma_{x_1}(Y)$  and  $W(x_1, Y) = 0$ , so  $I = F[W]$  by the Nullstellensatz. Explicitly, this follows from the identity

$$(y_1 - \sigma_{x_1}(y_1))^2 \equiv -(4X^2 + (4x_1 + b_2)X + (4x_1^2 + b_2x_1 + 2b_4))(X - x_1) + (Y - \sigma_X(Y))^2$$

in  $F[W]$ , since  $W(x_1, y_1) = 0$ . ◀

► **Remark 13.** Geometrically, the line  $Y = \lambda(X)$  intersects  $W$  at precisely three affine points  $(x_1, y_1)$ ,  $(x_2, y_2)$ , and  $(x_3, \sigma_{x_3}(y_3))$ , which translates to the identity of integral ideals

$$\langle X - x_1, Y - y_1 \rangle \cdot \langle X - x_2, Y - y_2 \rangle \cdot \langle X - x_3, Y - \sigma_{x_3}(y_3) \rangle = \langle Y - \lambda(X) \rangle. \quad (2)$$

The identity in Lemma 12 is then deduced by multiplying (2) with the identity in Lemma 10 and cancelling  $\langle X - x_3, Y - \sigma_{x_3}(y_3) \rangle$  from both sides. Note that Lemma 12 does not need the affine points to be nonsingular, while directly proving (2) does.

Lemma 12 is `XY_ideal_mul_XY_ideal`, and under these hypotheses, it follows immediately that the invertible fractional ideals  $\langle X - x_1, Y - y_1 \rangle$  and  $\langle X - x_2, Y - y_2 \rangle$  multiply to  $\langle X - x_3, Y - y_3 \rangle$  as classes in  $\text{Cl}(F[W])$ , which along with `XY_ideal_neg_mul` say that `to_class` respects addition. The actual Lean proof is slightly technical, using the new library lemmas `class_group.mk_eq_one_of_coe_ideal` and `class_group.mk_eq_mk_of_coe_ideal` to reduce the equality between ideal classes arising from integral ideals to an equality between their underlying integral ideals up to multiplication by principal integral ideals, so the tactic mode proof below will only be sketched as a comment for the sake of brevity.

```
@[simp] def to_class : W.point →+ additive (class_group W.coordinate_ring) :=
{ to_fun      := to_class_fun,
  map_zero'   := rfl,
  map_add'    := /- Split the cases for P1 + P2. If P1 = 0 or P2 = 0, simplify.
                  Otherwise P1 = (x1, y1) and P2 = (x2, y2).
                  If x1 = x2 and y1 = W.neg_Y x2 y2, use XY_ideal_neg_mul.
                  Otherwise use XY_ideal_mul_XY_ideal. -/ }
```

### 3.3 Injectivity of `to_class`

Injectivity is the statement that  $P_1 = P_2$  if `to_class` of  $P_1$  equals `to_class` of  $P_2$  for any  $P_1, P_2 \in W(F)$ , but a simple variant of `add_left_neg` shows that  $-P_1 + P_2 = 0$  precisely when  $P_1 = P_2$ . Since `to_class` is a `add_monoid_hom`, injectivity is equivalent to showing that `to_class` of  $P$  is trivial implies  $P = 0$  for any  $P \in W(F)$ . In other words, it suffices to show that the integral ideal  $\langle X - x, Y - y \rangle$  is never principal for any affine point  $(x, y) \in W(F)$ .

The approach taken circles around the fact that  $F[W]$  is a free  $F[X]$ -algebra of finite rank, so it carries the notion of a **norm**  $\text{Nm} : F[W] \rightarrow F[X]$ . If  $f \in F[W]$ , then  $\text{Nm}(f) \in F[X]$  may be given by the determinant of left multiplication by  $f$  as an  $F[X]$ -linear map, which is most easily computed by exhibiting an explicit basis  $\{1, Y\}$  of  $F[W]$  over  $F[X]$ .

```
lemma monic_polynomial : W.polynomial.monic
lemma nat_degree_polynomial : W.polynomial.nat_degree = 2

def basis : basis (fin 2) F[X] W.coordinate_ring :=
  (adjoin_root.power_basis' W.monic_polynomial).basis.reindex
  (fin_congr W.nat_degree_polynomial)
```

Here, `adjoin_root.power_basis'` returns the canonical basis of powers  $\{Y^i : 0 \leq i < \deg_Y(W(X, Y))\}$ , given the proof `monic_polynomial` that  $W(X, Y)$  is monic. This is a type indexed by the finite type with  $\deg_Y(W(X, Y))$  elements, which can be reindexed by the canonical finite type with two elements, since  $\deg_Y(W(X, Y)) = 2$  by `nat_degree_polynomial`.

With this basis, any element  $f \in F[W]$  may be expressed uniquely as  $f = p(X) + q(X)Y$  with  $p(X), q(X) \in F[X]$ , and the degree<sup>8</sup> of its norm can be computed directly.

► **Lemma 14.** *For any  $p(X), q(X) \in F[X]$ ,*

$$\deg_X(\text{Nm}(p(X) + q(X)Y)) = \max(2 \deg_X(p(X)), 2 \deg_X(q(X)) + 3).$$

**Proof.** Let  $f := p(X) + q(X)Y$ . In  $F[W]$  with the basis  $\{1, Y\}$  over  $F[X]$ ,

$$\begin{aligned} \text{Nm}(f) &\equiv \det \begin{pmatrix} p(X) & q(X) \\ q(X)(X^3 + a_2X^2 + a_4X + a_6) & p(X) - q(X)(a_1X + a_3) \end{pmatrix} \\ &= p(X)^2 - p(X)q(X)(a_1X + a_3) - q(X)^2(X^3 + a_2X^2 + a_4X + a_6). \end{aligned}$$

Let  $p := \deg_X(p(X))$  and  $q := \deg_X(q(X))$ . Then

$$\begin{aligned} \deg_X(p(X)^2) &= 2p, & \deg_X(q(X)^2(X^3 + a_2X^2 + a_4X + a_6)) &= 2q + 3, \\ \deg_X(p(X)q(X)(a_1X + a_3)) &\leq p + q + 1. \end{aligned}$$

If  $p \leq q + 1$ , then both  $p + q + 1 < 2q + 3$  and  $2p < 2q + 3$ , so  $\deg_X(\text{Nm}(f)) = 2q + 3$ . Otherwise  $q + 1 < p$ , then both  $p + q + 1 < 2p$  and  $2q + 3 < 2p$ , so  $\deg_X(\text{Nm}(f)) = 2p$ . ◀

Lemma 14 is `norm_smul_basis`, and it follows by considering cases that  $\deg_X \text{Nm}(f) \neq 1$  for any  $f \in F[W]$ , which is formalised as `nat_degree_norm_ne_one`.

► **Remark 15.** Geometrically,  $\text{Nm}(f)$  is the order of the pole of the rational function  $f \in F(W)$  at  $\mathcal{O}_W$ . Using the norm allows for a purely algebraic argument for injectivity, which was inspired from an exercise in Hartshorne that assumes a short Weierstrass model where  $\text{char}(F) \neq 2$  [20, Exercise I.6.2]. This was also the last missing step in the whole argument, as JX only started computing degrees after he saw Borchers's solutions to the exercise [5].

On the other hand, this degree is also the dimension of an  $F$ -vector space.

<sup>8</sup> `polynomial.degree` where  $\deg_X(0) := -\infty$  rather than `polynomial.nat_degree` where  $\deg_X(0) := 0$

## 6:14 The Group Law on Weierstrass Elliptic Curves

► **Lemma 16.** *For any nonzero  $f \in F[W]$ ,*

$$\deg_X(\text{Nm}(f)) = \dim_F(F[W]/\langle f \rangle).$$

**Proof.** In  $F[W]$  with the basis  $\{1, Y\}$  over  $F[X]$ , multiplication by  $f$  as an  $F[X]$ -linear map can be represented by a square matrix  $[f]$  over  $F[X]$ , which has a Smith normal form  $M[f]N$ , a diagonal matrix with diagonal entries some nonzero  $p(X), q(X) \in F[X]$ , for some invertible matrices  $M$  and  $N$  over  $F[X]$ . Now the quotient by  $f$  decomposes as a direct sum

$$F[W]/\langle f \rangle \cong F[X]/\langle p(X) \rangle \oplus F[X]/\langle q(X) \rangle,$$

whose dimension as  $F$ -vector spaces are precisely  $\deg_X(p(X))$  and  $\deg_X(q(X))$  respectively. On the other hand, the determinant of  $M[f]N$  is  $\det(M)\text{Nm}(f)\det(N) = p(X)q(X)$ , so

$$\deg_X(\text{Nm}(f)) = \deg_X(p(X)) + \deg_X(q(X)),$$

since the units  $\det(M), \det(N) \in F[X]$  are nonzero constant polynomials. ◀

Lemma 16 is `finrank_quotient_span_eq_nat_degree_norm`, and crucially uses the library lemma `ideal_quotient_equiv_pi_span` to decompose the quotient by  $\langle f \rangle$  into a direct sum of quotients by its Smith coefficients. It is worth noting that the same argument clearly works more generally by replacing  $F[W]$  by any  $F[X]$ -algebra with a finite basis. The proof of the injectivity of `to_class` then proceeds by contradiction.

► **Lemma 17.** *The function  $W(F) \rightarrow \text{Cl}(F[W])$  is injective.*

**Proof.** Let  $(x, y) \in W(F)$ . It suffices to show that  $\langle X - x, Y - y \rangle$  is not principal, so suppose for a contradiction that it were generated by some  $f \in F[W]$ . By Lemma 16,

$$\deg_X(\text{Nm}(f)) = \dim_F(F[W]/\langle f \rangle) = \dim_F(F[W]/\langle X - x, Y - y \rangle).$$

On the other hand, evaluating at  $(X, Y) = (x, y)$  is a surjective homomorphism  $F[X, Y] \rightarrow F$  with kernel  $\langle X - x, Y - y \rangle$ , and this contains the element  $W(X, Y)$  since  $W(x, y) = 0$ . Explicitly, this follows from the identity in  $F[X, Y]$  given by

$$W(X, Y) = (a_1y - (X^2 + (x + a_2)X + (x^2 + a_2x + a_4)))(X - x) + (y - \sigma_X(Y))(Y - y).$$

Thus by the first and third isomorphism theorems, there are  $F$ -algebra isomorphisms

$$F[W]/\langle X - x, Y - y \rangle \xrightarrow{\sim} F[X, Y]/\langle W(X, Y), X - x, Y - y \rangle = F[X, Y]/\langle X - x, Y - y \rangle \xrightarrow{\sim} F,$$

so  $\deg_X(\text{Nm}(f)) = \dim_F(F) = 1$ , which contradicts `nat_degree_norm_ne_one`. ◀

► **Remark 18.** Lemma 17 can also be proven without the Smith normal form, by considering the ideal generated by the norms of elements in  $\langle X - x, Y - y \rangle$  for  $(x, y) \in W(F)$ , namely

$$I := \langle (X - x)^2, (X - x)((Y - y) + (\sigma_X(Y) - y)), (Y - y)(\sigma_X(Y) - y) \rangle.$$

On one hand, as an integral ideal in  $F[W]$ , it can be shown that  $I$  is generated by the linear polynomial  $X - x$ . On the other hand, if  $\langle X - x, Y - y \rangle$  were generated by some  $f \in F[W]$ , then its ideal norm  $I$  is generated by  $\text{Nm}(f)$ , which cannot be linear by Lemma 14.

Lemma 17 is `to_class_injective`, and allows the proofs of commutativity and associativity in  $\text{Cl}(F[W])$  to be pulled back to  $W(F)$ , thus proving Proposition 7.

```
lemma add_comm (P1 P2 : W.point) : P1 + P2 = P2 + P1
lemma add_assoc (P1 P2 P3 : W.point) : (P1 + P2) + P3 = P1 + (P2 + P3)

instance : add_comm_group W.point :=
  ⟨zero, neg, add, zero_add, add_zero, add_left_neg, add_comm, add_assoc⟩
```

## 4 Discussion

### 4.1 Related work

As aforementioned, formalising the group law of an elliptic curve  $E$  over a field  $F$  is not novel, and has been done in several theorem provers to varying extents. Friedl (1998) [16] gave a computational proof in the short Weierstrass model, leaving some of the heavy computations for associativity to CoCoA as a trusted oracle, and his argument was subsequently formalised by Théry (2007) [28] in Coq. Fox, Gordon, and Hurd (2006) [15] formalised the addition law in the full Weierstrass model in HOL, but did not prove associativity. Hales and Raya (2020) [18] formalised a computational proof in Isabelle, but worked in the alternative Edwards model, which also fails to be an elliptic curve when  $\text{char}(F) = 2$ .

The first known formalisation of an algebro-geometric proof was done by Bartzia and Strub (2014) [4], who also worked in the short Weierstrass model. In 3,500 lines of Coq, they formalised the geometric notion of a Weil divisor<sup>9</sup> of a rational function  $f \in F(E)$  to define the degree-zero Weil divisor class group  $\text{Pic}^0(E)$ , which is isomorphic to the Picard group  $\text{Pic}(\text{Spec}(F[E]))$  since  $E$  is nonsingular [20, Corollary II.6.16]. In another 6,500 lines of Coq, they constructed an analogous bijection between  $\text{Pic}^0(E)$  and the points of  $E$  over the algebraic closure, but their argument is a simplification of the typical conceptual proof via the Riemann–Roch theorem and does not generalise easily to  $\text{char}(F) = 2$ . In contrast, the algebraic proof with the ideal class group  $\text{Cl}(F[E])$  only spans 1,500 lines of Lean 3, avoiding the geometric theory and reusing much of the well-maintained algebraic libraries.

### 4.2 Experimental attempts

The entire development process went through several iterations of trial and error, and various definitions of elliptic curves were proposed in Buzzard’s topic on Zulip. The abstract definition as in Remark 2 would be ideal, but algebraic geometry in `mathlib` is at its primitive stages, where describing properties of scheme morphisms like smoothness or properness, or defining the genus of a curve, would be a challenge. Since the Weierstrass model is universal over fields, the general consensus was that proving its equivalence with the abstract definition should proceed independently from proving theorems under the Weierstrass model.

Unfortunately, proving associativity became a huge issue in this model. The obvious first course of action is to check the equalities in all possible combinations of cases of addition, using the `field_simp` and `ring` tactics to normalise rational expressions. In doing this, the number of cases quickly explode, and in the nontrivial cases of affine addition, the polynomial expressions involved become gargantuan. There are optimisations that could be made to reduce the number of cases, as coded by Masdeu [23] adapting Friedl’s original argument into Lean, but a good way to manipulate the expressions remains elusive. In the generic case where three nonsingular affine points  $P_1, P_2, P_3 \in W(F)$  are in general position,<sup>10</sup> experiments by DKA with the aid of SageMath suggested that proving  $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$  by bashing out the algebra would involve polynomials each with tens of thousands of monomials, which is highly time-consuming in a formal system and definitely infeasible to work out by hand, despite taking only half a second in SageMath. The `ring` tactic, which uses proof generation by normalising to Horner form [17], seems to be an order of magnitude too slow to work with such expressions, resulting in deterministic timeouts.

<sup>9</sup> a formal  $\mathbb{Z}$ -linear combination of points  $P \in E$  weighted by the order of vanishing of  $f$  at  $P$

<sup>10</sup> the affine points  $P_1, P_2, P_3, P_1 + P_2, P_1 + P_3,$  and  $P_2 + P_3$  have pairwise distinct  $X$ -coordinates

The main culprits for the huge polynomials are the  $XY$  and  $Y$  terms in the Weierstrass equation, which do not allow even exponents of  $Y$  in the expressions to be substituted with polynomials solely in  $X$ . When  $\text{char}(F) \neq 2$ , these terms disappear with a change of variables, reducing the expressions to the computationally feasible range of hundreds of terms, hence enabling the work by Théry (2007), or a transformation to the Edwards model whose group law was already formalised by Hales and Raya (2020). In principle, since  $2 = 0$  when  $\text{char}(F) = 2$ , enough multiples of 2 may be cancelled from the expressions until a brute-force attack becomes feasible, but `mathlib` currently has no good tactic to do these cancellations except to manually extract these multiples of 2, such as by rewriting the expressions into the form  $p + 2q$  using `ring`, which is too slow in the first place, and deleting  $2q$ .

The mathematical literature typically deals with associativity by providing alternative proofs, in addition to the aforementioned algebro-geometric proof via the Picard group. One notable method goes via the uniformisation theorem in complex analysis [26, Corollary VI.5.1.1], but `mathlib` also lacks much of the complex-analytic machinery to prove it, and this approach is only valid for  $\text{char}(F) = 0$  via the Lefschetz principle. Another approach uses the Cayley–Bacharach theorem in projective geometry [7, Lemma 7.1], which proves associativity generically by a dimension counting argument. By continuing on Masdeu’s branch, this approach seemed viable, but required redefining Weierstrass curves in projective coordinates and a convenient way to switch back to affine coordinates via dehomogenisation. Furthermore, the argument fails in a less generic case with a repeated point, which could be fixed by introducing an ad-hoc notion of intersection multiplicity between a line and a cubic, as suggested by Stoll. DKA started refactoring the definitions in an attempt at this approach, but ultimately switched to the current approach when proposed by JX. Note that an explicit exposition of a version of this argument can also be found in Nuida (2021) [24].

### 4.3 Implementation issues

**Bivariate polynomials.** A bivariate polynomial in  $X$  and  $Y$  over a commutative ring  $R$  is typically represented in `mathlib` by a finitely supported function  $(\{0, 1\} \rightarrow \mathbb{N}) \rightarrow R$ , associating a function  $f : \{0, 1\} \rightarrow \mathbb{N}$  to the coefficient of  $X^{f(0)}Y^{f(1)}$ . This representation is very cumbersome when performing concrete manipulations, such as those in Lemma 10 and Lemma 12, since explicit functions  $\{0, 1\} \rightarrow \mathbb{N}$  are needed to obtain coefficients.

In contrast, a polynomial in  $X$  over  $R$  is represented in `mathlib` by a finitely supported function  $\mathbb{N} \rightarrow R$ , associating a natural number  $n \in \mathbb{N}$  to the coefficient of  $X^n$ . A polynomial in  $Y$  with coefficients polynomials in  $X$  performs the same function as a bivariate polynomial in  $X$  and  $Y$ , but the coefficient of  $X^nY^m$  is obtained by sequentially supplying two natural numbers  $m, n \in \mathbb{N}$ . This has the additional advantage of aligning with the API for `adjoin_root`, which gives a power basis needed in the proof of injectivity.

This representation does have the slightly awkward problem that  $X$  is denoted by `C X` while  $Y$  is denoted by `X`, but this is easily fixed by introducing `notation Y := X` and `notation R[X] [Y] := polynomial (polynomial R)`. A more serious drawback is that existing results about multivariate polynomials, such as the Nullstellensatz, do not carry over to this representation, so explicit proofs with polynomial identities are sometimes necessary, namely in the proofs of Lemma 10, Lemma 12, and Lemma 17. Another issue is that the partial derivative with respect to  $X$  is obtained by applying the `polynomial.derivative` linear map to each coefficient of the polynomial in  $Y$ , but the current `polynomial.map` only accepts a ring homomorphism, which explains why the partial derivatives `polynomial_X` and `polynomial_Y` were defined manually instead. In light of this, it has been suggested that `polynomial.map` should be refactored to accept set-theoretic functions instead.



**Performance issues.** In the original definition of `to_class`, it was observed that the function `class_group.mk`, when applied to an invertible fractional ideal of `coordinate_ring`, took a while to compile. Baanen diagnosed this problem and proposed the following solution [1].

```
local attribute [irreducible] coordinate_ring.comm_ring
```

Although `coordinate_ring` is marked as `irreducible`, its `derive comm_ring` tag generates a `reducible` instance of `comm_ring`. In certain circumstances this is extremely slow, because the number of times an instance gets unified grows exponentially with its depth due to a lack of caching, and Baanen’s solution was to force its `comm_ring` instance to be `irreducible` locally whenever necessary. Note that this should have been fixed in Lean 4, and the port of `mathlib` to Lean 4 is expected to finish in a few months’ time.

There are other performance issues that led to timeouts during development, but they were fixed by generalising the statements so they involve less complicated types.

**Proof automation.** The proofs of many basic lemmas often reduce to checking an equality of two polynomial expressions, such as in Lemma 5 and Lemma 6, but equality often holds only under some local hypotheses. Rather than rewriting these into the goal and applying the `ring` tactic, it is convenient to use `linear_combination`, a newly-developed tactic that subtracts a linear combination of known equalities from the goal, before applying `ring`.

When several rewrite lemmas are often used together, it is also convenient to write a custom tactic to chain them. For instance, the evaluation map `eval` on a polynomial expression is often propagated inwards, so grouping the lemmas allows for a single tactic call.

```
meta def eval_simp : tactic unit :=
  '[simp only [eval_C, eval_X, eval_neg, eval_add, eval_sub, eval_mul, eval_pow]]
```

## 4.4 Future projects

Formalising the group law opens the doors to an expansive array of possible further work. An immediate project would be to enrich the API for nonsingular points by adding basic functorial properties with respect to a base change to a field extension  $K/F$ . For instance, this could be defining the induced map  $E(F) \rightarrow E(K)$ , or if  $K/F$  is Galois, computing the subgroup of  $E(K)$  invariant under the action of  $\text{Gal}(K/F)$  to be precisely  $E(F)$ .

It is worth noting the two ongoing projects by each of the two authors. DKA is formalising an inductive definition of division polynomials to understand the structure of the  $n$ -torsion subgroup  $E[n]$  to compute the structure of the  $\ell$ -adic Tate module  $\varprojlim_n E[\ell^n]$ , while JX is formalising a proof that the reduction map  $E(K) \rightarrow E(R/\mathfrak{m})$  is a group homomorphism for a discrete valuation ring  $R$  with fraction field  $K$  and maximal ideal  $\mathfrak{m}$ .

In the longer run, one could explore the rich arithmetic theory over specific fields. Once the theory of local fields is sufficiently developed in `mathlib`, one could define the formal group of an elliptic curve, classify its reduction types, or state Tate’s algorithm. These will be useful for the global theory, where one could define the Selmer and Tate–Shafarevich groups, give a Galois cohomological proof of the Mordell–Weil theorem, or state the full Birch and Swinnerton-Dyer conjecture. Over a finite field, one could verify the correctness of primality and factorisation algorithms as well as cryptographic protocols, or prove the Hasse–Weil bound or the Weil conjectures for elliptic curves.

Ultimately, a long term goal would be to redefine elliptic curves in `mathlib` as in Remark 2 and prove Proposition 1, but this will require a version of the Riemann–Roch theorem, whose proof will require a robust theory of sheaves of modules and their cohomology.

## References

- 1 David Angdinata. `class_group`. URL: [https://leanprover-community.github.io/archive/stream/116395-maths/topic/Why.20is.20class\\_group.2Emk.20so.20slow.3F.html](https://leanprover-community.github.io/archive/stream/116395-maths/topic/Why.20is.20class_group.2Emk.20so.20slow.3F.html).
- 2 A. O. L. Atkin and François Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993. doi:10.2307/2152935.
- 3 Anne Baanen, Sander Dahmen, Ashvni Narayanan, and Filippo Nuccio Mortarino Majno di Capriglio. A formalization of Dedekind domains and class groups of global fields. *Journal of Automated Reasoning*, 66:611–637, 2022. doi:10.1007/s10817-022-09644-0.
- 4 Evmorfia-Iro Bartzia and Pierre-Yves Strub. A formal library for elliptic curves in the Coq proof assistant. *ITP*, pages 77–92, 2014. doi:10.1007/978-3-319-08970-6\_6.
- 5 Richard Borcherds. Hartshorne, Chapter 1.6, Answers to Exercises. URL: <https://math.berkeley.edu/~reb/courses/256A/1.6.pdf>.
- 6 Kevin Buzzard. Thoughts on elliptic curves. URL: <https://leanprover-community.github.io/archive/stream/116395-maths/topic/thoughts.20on.20elliptic.20curves.html>.
- 7 J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.
- 8 Robin Chapman. Why is an elliptic curve a group? URL: <https://mathoverflow.net/q/20623>.
- 9 Lily Chen, Dustin Moody, Karen Randall, Andrew Regenscheid, and Angela Robinson. Recommendations for discrete logarithm-based cryptography: elliptic curve domain parameters, 2023. doi:10.6028/NIST.SP.800-186.
- 10 The Mathlib Community. mathlib documentation. URL: [https://leanprover-community.github.io/mathlib\\_docs/](https://leanprover-community.github.io/mathlib_docs/).
- 11 The Mathlib Community. The Lean mathematical library. *CPP*, 2020. doi:10.1145/3372885.3373824.
- 12 Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. The Lean theorem prover (system description). *CADE*, 2015. doi:10.1007/978-3-319-21401-6\_26.
- 13 Pierre Philip du Preez. Understanding EC Diffie-Hellman. URL: <https://medium.com/swlh/understanding-ec-diffie-hellman-9c07be338d4a>.
- 14 David Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Springer New York, 1995.
- 15 Anthony Fox, Mike Gordon, and Joe Hurd. Formalized elliptic curve cryptography. *High Confidence Software and Systems*, 2006.
- 16 Stefan Friedl. An elementary proof of the group law for elliptic curves. *Groups Complexity Cryptology*, 9(2):117–123, 2017. doi:10.1515/gcc-2017-0010.
- 17 Benjamin Grégoire and Assia Mahboubi. Proving equalities in a commutative ring done right in Coq. *Lecture Notes in Computer Science*, 3603:98–113, 2005. doi:10.1007/11541868\_7.
- 18 Thomas Hales and Rodrigo Raya. Formal proof of the group law for Edwards elliptic curves. *Automated Reasoning*, 12167:254–269, 2020. doi:10.1007/978-3-030-51054-1\_15.
- 19 Kevin Hartnett. Math quartet joins forces on unified theory. URL: <https://www.quantamagazine.org/math-quartet-joins-forces-on-unified-theory-20151208/>.
- 20 Robin Hartshorne. *Algebraic Geometry*. Springer New York, 1977.
- 21 Nicholas Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*. Princeton University Press, 1985.
- 22 Hendrik Lenstra. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987. doi:10.2307/1971363.
- 23 Marc Masdeu. `ell_add_assoc`. URL: [https://github.com/leanprover-community/mathlib/blob/ell\\_add\\_assoc/src/algebraic\\_geometry/EllipticCurveGroupLaw.lean](https://github.com/leanprover-community/mathlib/blob/ell_add_assoc/src/algebraic_geometry/EllipticCurveGroupLaw.lean).
- 24 Koji Nuida. An elementary linear-algebraic proof without computer-aided arguments for the group law on elliptic curves. *International Journal of Mathematics for Industry*, 13(1), 2021. doi:10.1142/S2661335221500015.

- 25 David Russinoff. A computationally surveyable proof of the group properties of an elliptic curve. *In Proceedings ACL2Workshop*, 2017. doi:10.4204/EPTCS.249.3.
- 26 Joseph Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2009.
- 27 Andrew Sutherland. Algebraic proof of the associativity of the elliptic curve group law on curves defined by a short Weierstrass equation, as presented in Lecture 2 of 18.783. URL: [https://cocalc.com/share/public\\_paths/a6a1c2b188bd61d94c3dd3bfd5aa73722e8bd38b](https://cocalc.com/share/public_paths/a6a1c2b188bd61d94c3dd3bfd5aa73722e8bd38b).
- 28 Laurent Théry. Proving the group law for elliptic curves formally. *INRIA*, 2007.
- 29 Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. URL: <https://www.claymath.org/sites/default/files/birchswin.pdf>.
- 30 Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, 141(3):443–551, 1995. doi:10.2307/2118559.