

General Weierstrass Equations

Arthur Freitas Ramos David Barros Hulak
Ruy J. G. B. de Queiroz

October 6, 2026

Abstract

This entry develops the general Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

over commutative rings and fields. It defines the standard invariants, proves $c_4^3 - c_6^2 = 1728\Delta$, formalizes the affine and projective equations and their singular points, and proves over every field that the projective cubic is geometrically nonsingular exactly when $\Delta \neq 0$. Geometric singularities are taken over the algebraic closure, so the statement includes imperfect fields and characteristics 2 and 3. A final bridge specializes the development to the short equation and reuses the AFP *Elliptic Curves Group Law* entry [1]. The definitions and invariant formulas follow the standard treatment in [2]. AI assistance was used for proof engineering. The final definitions, statements, and proofs are checked by Isabelle.

Contents

1	General Weierstrass coefficients	2
2	Standard invariants	3
3	The affine equation	4
4	Homogeneous coordinates	5
5	The projective cubic	6
6	Formal partial derivatives	7
7	Singular points	8
8	The affine chart	9
9	Elimination polynomials	10

10 Elimination identities	11
11 Characteristic two	12
12 Odd characteristic	15
13 The discriminant criterion	17
14 The partial j-invariant	19
15 Specialization to short Weierstrass equations	19
theory <i>Weierstrass-Coefficients</i>	
imports	
<i>HOL-Computational-Algebra.Polynomial</i>	
begin	

1 General Weierstrass coefficients

record *'a weierstrass-coeffs* =

a1 :: *'a*
a2 :: *'a*
a3 :: *'a*
a4 :: *'a*
a6 :: *'a*

lemma *weierstrass-coeffs-eqI*:

fixes *W V* :: *'a weierstrass-coeffs*
assumes *a1 W = a1 V*
and *a2 W = a2 V*
and *a3 W = a3 V*
and *a4 W = a4 V*
and *a6 W = a6 V*
shows *W = V*
<proof>

definition *map-weierstrass-coeffs* ::

('a ⇒ 'b) ⇒ 'a weierstrass-coeffs ⇒ 'b weierstrass-coeffs

where

map-weierstrass-coeffs f W =

*(λ a1 = f (a1 W), a2 = f (a2 W), a3 = f (a3 W),
a4 = f (a4 W), a6 = f (a6 W))*

lemma *map-weierstrass-coeffs-simps* [*simp*]:

a1 (map-weierstrass-coeffs f W) = f (a1 W)
a2 (map-weierstrass-coeffs f W) = f (a2 W)
a3 (map-weierstrass-coeffs f W) = f (a3 W)
a4 (map-weierstrass-coeffs f W) = f (a4 W)
a6 (map-weierstrass-coeffs f W) = f (a6 W)

$\langle \text{proof} \rangle$

lemma *map-weierstrass-coeffs-id* [simp]:
 $\text{map-weierstrass-coeffs id } W = W$
 $\langle \text{proof} \rangle$

lemma *map-weierstrass-coeffs-comp*:
 $\text{map-weierstrass-coeffs } f (\text{map-weierstrass-coeffs } g W) =$
 $\text{map-weierstrass-coeffs } (f \circ g) W$
 $\langle \text{proof} \rangle$

definition *short-weierstrass-coeffs* ::
 $'a :: \text{zero} \Rightarrow 'a \Rightarrow 'a \text{ weierstrass-coeffs}$
 where
 $\text{short-weierstrass-coeffs } A B =$
 $(a1 = 0, a2 = 0, a3 = 0, a4 = A, a6 = B)$

lemma *short-weierstrass-coeffs-simps* [simp]:
 $a1 (\text{short-weierstrass-coeffs } A B) = 0$
 $a2 (\text{short-weierstrass-coeffs } A B) = 0$
 $a3 (\text{short-weierstrass-coeffs } A B) = 0$
 $a4 (\text{short-weierstrass-coeffs } A B) = A$
 $a6 (\text{short-weierstrass-coeffs } A B) = B$
 $\langle \text{proof} \rangle$

end
theory *Weierstrass-Invariants*
 imports *Weierstrass-Coefficients*
begin

2 Standard invariants

definition $b2 :: 'a :: \text{comm-ring-1} \text{ weierstrass-coeffs} \Rightarrow 'a$
 where $b2 W = a1 W^2 + 4 * a2 W$

definition $b4 :: 'a :: \text{comm-ring-1} \text{ weierstrass-coeffs} \Rightarrow 'a$
 where $b4 W = 2 * a4 W + a1 W * a3 W$

definition $b6 :: 'a :: \text{comm-ring-1} \text{ weierstrass-coeffs} \Rightarrow 'a$
 where $b6 W = a3 W^2 + 4 * a6 W$

definition $b8 :: 'a :: \text{comm-ring-1} \text{ weierstrass-coeffs} \Rightarrow 'a$
 where
 $b8 W =$
 $a1 W^2 * a6 W + 4 * a2 W * a6 W - a1 W * a3 W * a4 W +$
 $a2 W * a3 W^2 - a4 W^2$

definition $c4 :: 'a :: \text{comm-ring-1} \text{ weierstrass-coeffs} \Rightarrow 'a$
 where $c4 W = b2 W^2 - 24 * b4 W$

definition $c6 :: 'a::comm-ring-1 \text{ weierstrass-coeffs} \Rightarrow 'a$
where $c6 \ W = -(b2 \ W \wedge 3) + 36 * b2 \ W * b4 \ W - 216 * b6 \ W$

definition $discriminant :: 'a::comm-ring-1 \text{ weierstrass-coeffs} \Rightarrow 'a$
where
 $discriminant \ W =$
 $-(b2 \ W \wedge 2) * b8 \ W - 8 * b4 \ W \wedge 3 - 27 * b6 \ W \wedge 2 +$
 $9 * b2 \ W * b4 \ W * b6 \ W$

lemma $b2-b6-minus-b4-squared$:
 $b2 \ W * b6 \ W - b4 \ W \wedge 2 = 4 * b8 \ W$
 $\langle proof \rangle$

theorem $c4-c6-discriminant-identity$:
 $c4 \ W \wedge 3 - c6 \ W \wedge 2 = 1728 * discriminant \ W$
 $\langle proof \rangle$

lemma $four-discriminant-expanded$:
 $4 * discriminant \ W =$
 $-(b2 \ W \wedge 3) * b6 \ W + b2 \ W \wedge 2 * b4 \ W \wedge 2 -$
 $32 * b4 \ W \wedge 3 - 108 * b6 \ W \wedge 2 +$
 $36 * b2 \ W * b4 \ W * b6 \ W$
 $\langle proof \rangle$

end
theory $Weierstrass-Affine-Curve$
imports $Weierstrass-Invariants$
begin

3 The affine equation

definition $weierstrass-affine-poly ::$
 $'a::comm-ring-1 \text{ weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$
where
 $weierstrass-affine-poly \ W \ x \ y =$
 $y \wedge 2 + a1 \ W * x * y + a3 \ W * y -$
 $(x \wedge 3 + a2 \ W * x \wedge 2 + a4 \ W * x + a6 \ W)$

definition $on-weierstrass-affine ::$
 $'a::comm-ring-1 \text{ weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow bool$
where
 $on-weierstrass-affine \ W \ x \ y \longleftrightarrow$
 $y \wedge 2 + a1 \ W * x * y + a3 \ W * y =$
 $x \wedge 3 + a2 \ W * x \wedge 2 + a4 \ W * x + a6 \ W$

lemma $on-weierstrass-affine-iff-poly-zero$:
 $on-weierstrass-affine \ W \ x \ y \longleftrightarrow$
 $weierstrass-affine-poly \ W \ x \ y = 0$

```

    <proof>

end
theory Weierstrass-Projective-Curve
  imports Weierstrass-Affine-Curve
begin

```

4 Homogeneous coordinates

```

type-synonym 'a weierstrass-projective-coords = 'a × 'a × 'a

```

```

definition scale-projective ::
  'a::times ⇒ 'a weierstrass-projective-coords ⇒
  'a weierstrass-projective-coords
where
  scale-projective u = (λ(X, Y, Z). (u * X, u * Y, u * Z))

```

```

lemma scale-projective-simps [simp]:
  scale-projective u (X, Y, Z) = (u * X, u * Y, u * Z)
<proof>

```

```

definition projective-coords-valid ::
  'a::zero weierstrass-projective-coords ⇒ bool
where
  projective-coords-valid = (λ(X, Y, Z). X ≠ 0 ∨ Y ≠ 0 ∨ Z ≠ 0)

```

```

definition projectively-equivalent ::
  'a::field weierstrass-projective-coords ⇒
  'a weierstrass-projective-coords ⇒ bool
where
  projectively-equivalent p q ⟷
    (∃ u. u ≠ 0 ∧ q = scale-projective u p)

```

```

lemma scale-projective-one [simp]:
  scale-projective 1 p = p
for p :: 'a::monoid-mult weierstrass-projective-coords
<proof>

```

```

lemma scale-projective-mult:
  scale-projective u (scale-projective v p) = scale-projective (u * v) p
for p :: 'a::monoid-mult weierstrass-projective-coords
<proof>

```

```

lemma projective-coords-valid-scale-iff:
  projective-coords-valid (scale-projective u p) ⟷
    u ≠ 0 ∧ projective-coords-valid p
for u :: 'a::field
<proof>

```

lemma *projectively-equivalent-refl* [simp]:

projectively-equivalent p p

$\langle \text{proof} \rangle$

lemma *projectively-equivalent-sym*:

projectively-equivalent p $q \implies \text{projectively-equivalent } q$ p

$\langle \text{proof} \rangle$

lemma *projectively-equivalent-trans*:

projectively-equivalent p $q \implies$

projectively-equivalent q $r \implies$

projectively-equivalent p r

$\langle \text{proof} \rangle$

5 The projective cubic

definition *weierstrass-projective-poly* ::

$'a::\text{comm-ring-1}$ *weierstrass-coeffs* $\Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$

where

weierstrass-projective-poly W X Y $Z =$

$Y^2 * Z + a1 * W * X * Y * Z + a3 * W * Y * Z^2 -$

$(X^3 + a2 * W * X^2 * Z + a4 * W * X * Z^2 + a6 * W * Z^3)$

definition *on-projective-weierstrass* ::

$'a::\text{comm-ring-1}$ *weierstrass-coeffs* $\Rightarrow$

$'a$ *weierstrass-projective-coords* $\Rightarrow \text{bool}$

where

on-projective-weierstrass $W =$

$(\lambda(X, Y, Z).$

projective-coords-valid $(X, Y, Z) \wedge$

weierstrass-projective-poly W X Y $Z = 0)$

lemma *weierstrass-projective-poly-scale*:

weierstrass-projective-poly W $(u * X)$ $(u * Y)$ $(u * Z) =$

$u^3 * \text{weierstrass-projective-poly } W$ X Y Z

$\langle \text{proof} \rangle$

lemma *on-projective-weierstrass-scale-iff*:

fixes $u :: 'a::\text{field}$

assumes $u \neq 0$

shows *on-projective-weierstrass* W $(\text{scale-projective } u$ $p) \longleftrightarrow$

on-projective-weierstrass W p

$\langle \text{proof} \rangle$

definition *affine-to-projective* ::

$'a::\text{one} \Rightarrow 'a \Rightarrow 'a$ *weierstrass-projective-coords*

where

affine-to-projective x $y = (x, y, 1)$

lemma *weierstrass-projective-poly-affine* [simp]:
weierstrass-projective-poly $W\ x\ y\ 1 = \text{weierstrass-affine-poly}\ W\ x\ y$
 ⟨proof⟩

theorem *on-projective-weierstrass-affine*:
on-projective-weierstrass $W\ (\text{affine-to-projective}\ x\ y) \longleftrightarrow$
on-weierstrass-affine $W\ x\ y$
 ⟨proof⟩

theorem *on-projective-weierstrass-chart*:
fixes $X\ Y\ Z :: 'a::\text{field}$
assumes $Z \neq 0$
shows *on-projective-weierstrass* $W\ (X,\ Y,\ Z) \longleftrightarrow$
on-weierstrass-affine $W\ (X\ /\ Z)\ (Y\ /\ Z)$
 ⟨proof⟩

definition *weierstrass-infinity* ::
 $'a::\text{zero-neq-one}\ \text{weierstrass-projective-coords}$
where
weierstrass-infinity = $(0,\ 1,\ 0)$

lemma *weierstrass-infinity-on-curve* [simp]:
on-projective-weierstrass $W\ \text{weierstrass-infinity}$
 ⟨proof⟩

lemma *on-projective-weierstrass-at-infinity-iff*:
on-projective-weierstrass $W\ (X,\ Y,\ 0) \longleftrightarrow$
 $X = 0 \wedge Y \neq 0$
for $X\ Y :: 'a::\text{field}$
 ⟨proof⟩

theorem *projective-weierstrass-at-infinity*:
assumes *on-projective-weierstrass* $W\ (X,\ Y,\ 0)$
shows *projectively-equivalent* $(X,\ Y,\ 0)\ \text{weierstrass-infinity}$
 ⟨proof⟩

end
theory *Weierstrass-Singularities*
imports *Weierstrass-Projective-Curve*
begin

6 Formal partial derivatives

definition *weierstrass-projective-dx* ::
 $'a::\text{comm-ring-1}\ \text{weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$
where
weierstrass-projective-dx $W\ X\ Y\ Z =$
 $a1\ W * Y * Z - 3 * X^2 - 2 * a2\ W * X * Z - a4\ W * Z^2$

definition *weierstrass-projective-dy* ::
 'a::comm-ring-1 weierstrass-coeffs $\Rightarrow$ 'a $\Rightarrow$ 'a $\Rightarrow$ 'a $\Rightarrow$ 'a
where
weierstrass-projective-dy W X Y Z =
 $2 * Y * Z + a1 * W * X * Z + a3 * W * Z^2$

definition *weierstrass-projective-dz* ::
 'a::comm-ring-1 weierstrass-coeffs $\Rightarrow$ 'a $\Rightarrow$ 'a $\Rightarrow$ 'a $\Rightarrow$ 'a
where
weierstrass-projective-dz W X Y Z =
 $Y^2 + a1 * W * X * Y + 2 * a3 * W * Y * Z -$
 $a2 * W * X^2 - 2 * a4 * W * X * Z - 3 * a6 * W * Z^2$

lemma *weierstrass-projective-dx-scale*:
weierstrass-projective-dx W (u * X) (u * Y) (u * Z) =
 $u^2 * \text{weierstrass-projective-dx } W X Y Z$
 <proof>

lemma *weierstrass-projective-dy-scale*:
weierstrass-projective-dy W (u * X) (u * Y) (u * Z) =
 $u^2 * \text{weierstrass-projective-dy } W X Y Z$
 <proof>

lemma *weierstrass-projective-dz-scale*:
weierstrass-projective-dz W (u * X) (u * Y) (u * Z) =
 $u^2 * \text{weierstrass-projective-dz } W X Y Z$
 <proof>

lemma *weierstrass-projective-euler*:
 $X * \text{weierstrass-projective-dx } W X Y Z +$
 $Y * \text{weierstrass-projective-dy } W X Y Z +$
 $Z * \text{weierstrass-projective-dz } W X Y Z =$
 $3 * \text{weierstrass-projective-poly } W X Y Z$
 <proof>

7 Singular points

definition *singular-projective-point* ::
 'a::field weierstrass-coeffs $\Rightarrow$
 'a weierstrass-projective-coords $\Rightarrow$ bool
where
singular-projective-point W =
 $(\lambda(X, Y, Z).$
 $\text{projective-coords-valid } (X, Y, Z) \wedge$
 $\text{weierstrass-projective-poly } W X Y Z = 0 \wedge$
 $\text{weierstrass-projective-dx } W X Y Z = 0 \wedge$
 $\text{weierstrass-projective-dy } W X Y Z = 0 \wedge$
 $\text{weierstrass-projective-dz } W X Y Z = 0)$

lemma *singular-projective-point-on-curve*:
singular-projective-point $W\ p \implies \text{on-projective-weierstrass } W\ p$
 $\langle \text{proof} \rangle$

theorem *singular-projective-point-scale-iff*:
fixes $u :: 'a::\text{field}$
assumes $u \neq 0$
shows *singular-projective-point* $W\ (\text{scale-projective } u\ p) \longleftrightarrow$
singular-projective-point $W\ p$
 $\langle \text{proof} \rangle$

theorem *point-at-infinity-nonsingular*:
 $\neg \text{singular-projective-point } W\ \text{weierstrass-infinity}$
 $\langle \text{proof} \rangle$

lemma *singular-projective-point-imp-z-nonzero*:
assumes *singular-projective-point* $W\ (X, Y, Z)$
shows $Z \neq 0$
 $\langle \text{proof} \rangle$

8 The affine chart

definition *weierstrass-affine-dx* ::
 $'a::\text{comm-ring-1}\ \text{weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$
where
weierstrass-affine-dx $W\ x\ y =$
 $a1\ W * y - 3 * x^2 - 2 * a2\ W * x - a4\ W$

definition *weierstrass-affine-dy* ::
 $'a::\text{comm-ring-1}\ \text{weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow 'a$
where
weierstrass-affine-dy $W\ x\ y = 2 * y + a1\ W * x + a3\ W$

definition *singular-affine-point* ::
 $'a::\text{field}\ \text{weierstrass-coeffs} \Rightarrow 'a \Rightarrow 'a \Rightarrow \text{bool}$
where
singular-affine-point $W\ x\ y \longleftrightarrow$
weierstrass-affine-poly $W\ x\ y = 0 \wedge$
weierstrass-affine-dx $W\ x\ y = 0 \wedge$
weierstrass-affine-dy $W\ x\ y = 0$

lemma *weierstrass-projective-dx-affine [simp]*:
weierstrass-projective-dx $W\ x\ y\ 1 = \text{weierstrass-affine-dx } W\ x\ y$
 $\langle \text{proof} \rangle$

lemma *weierstrass-projective-dy-affine [simp]*:
weierstrass-projective-dy $W\ x\ y\ 1 = \text{weierstrass-affine-dy } W\ x\ y$
 $\langle \text{proof} \rangle$

lemma *weierstrass-projective-dz-affine:*

weierstrass-projective-dz $W \ x \ y \ 1 =$
 $3 * \text{weierstrass-affine-poly } W \ x \ y -$
 $x * \text{weierstrass-affine-dx } W \ x \ y -$
 $y * \text{weierstrass-affine-dy } W \ x \ y$
 ⟨proof⟩

lemma *singular-projective-affine-iff:*

singular-projective-point $W \ (\text{affine-to-projective } x \ y) \longleftrightarrow$
singular-affine-point $W \ x \ y$
 ⟨proof⟩

theorem *projective-singular-iff-affine-singular:*

$(\exists p. \text{ singular-projective-point } W \ p) \longleftrightarrow$
 $(\exists x \ y. \text{ singular-affine-point } W \ x \ y)$
 ⟨proof⟩

definition *projective-weierstrass-nonsingular-over ::*

'a::field weierstrass-coeffs $\Rightarrow \text{bool}$

where

projective-weierstrass-nonsingular-over $W \longleftrightarrow$
 $\neg (\exists p. \text{ singular-projective-point } W \ p)$

lemma *projective-weierstrass-nonsingular-over-iff:*

projective-weierstrass-nonsingular-over $W \longleftrightarrow$
 $\neg (\exists x \ y. \text{ singular-affine-point } W \ x \ y)$
 ⟨proof⟩

9 Elimination polynomials

definition *weierstrass-g ::*

'a::comm-ring-1 weierstrass-coeffs $\Rightarrow 'a \Rightarrow 'a$

where

weierstrass-g $W \ x =$
 $4 * x^3 + b2 \ W * x^2 + 2 * b4 \ W * x + b6 \ W$

definition *weierstrass-h ::*

'a::comm-ring-1 weierstrass-coeffs $\Rightarrow 'a \Rightarrow 'a$

where

weierstrass-h $W \ x = 6 * x^2 + b2 \ W * x + b4 \ W$

lemma *affine-dy-squared-minus-g:*

weierstrass-affine-dy $W \ x \ y^2 - \text{weierstrass-g } W \ x =$
 $4 * \text{weierstrass-affine-poly } W \ x \ y$
 ⟨proof⟩

lemma *two-affine-dx-minus-a1-dy:*

$2 * \text{weierstrass-affine-dx } W \ x \ y -$
 $a1 \ W * \text{weierstrass-affine-dy } W \ x \ y =$

```

    - weierstrass-h W x
  <proof>

end
theory Weierstrass-Discriminant-Criterion
  imports
    Weierstrass-Singularities
    HOL-Algebra.Algebraic-Closure-Type
begin

```

10 Elimination identities

lemma *four-discriminant-bezout*:

```

  4 * discriminant W =
    - (b2 W ^ 3 + 6 * b2 W ^ 2 * x - 30 * b2 W * b4 W -
      144 * b4 W * x + 108 * b6 W) * weierstrass-g W x +
    (b2 W ^ 3 * x + b2 W ^ 2 * b4 W + 4 * b2 W ^ 2 * x ^ 2 -
      28 * b2 W * b4 W * x + 6 * b2 W * b6 W -
      32 * b4 W ^ 2 - 96 * b4 W * x ^ 2 + 72 * b6 W * x) *
    weierstrass-h W x
  <proof>

```

lemma *singular-affine-imp-g-zero*:

```

  assumes singular-affine-point W x y
  shows weierstrass-g W x = 0
  <proof>

```

lemma *singular-affine-imp-h-zero*:

```

  assumes singular-affine-point W x y
  shows weierstrass-h W x = 0
  <proof>

```

lemma *twice-negative-half*:

```

  fixes z :: 'a::field
  assumes (2 :: 'a) ≠ 0
  shows 2 * (- z / 2) + z = 0
  <proof>

```

lemma *four-ne-zero-of-two-ne-zero*:

```

  fixes dummy :: 'a::field
  assumes two: (2 :: 'a) ≠ 0
  shows (4 :: 'a) ≠ 0
  <proof>

```

lemma *affine-singular-of-g-h*:

```

  fixes W :: 'a::field weierstrass-coeffs
  assumes two: (2 :: 'a) ≠ 0
  and g: weierstrass-g W x = 0
  and h: weierstrass-h W x = 0

```

shows *singular-affine-point* $W\ x\ (-\ (a1\ W * x + a3\ W) / 2)$
 $\langle proof \rangle$

lemma *singular-affine-imp-discriminant-zero-odd*:
fixes $W :: 'a::field\ weierstrass-coeffs$
assumes $two: (2 :: 'a) \neq 0$
and *singular*: *singular-affine-point* $W\ x\ y$
shows *discriminant* $W = 0$
 $\langle proof \rangle$

11 Characteristic two

lemma *char-two-three*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $(3 :: 'a) = 1$
 $\langle proof \rangle$

lemma *char-two-four*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $(4 :: 'a) = 0$
 $\langle proof \rangle$

lemma *char-two-eight*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $(8 :: 'a) = 0$
 $\langle proof \rangle$

lemma *char-two-nine*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $(9 :: 'a) = 1$
 $\langle proof \rangle$

lemma *char-two-twenty-seven*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $(27 :: 'a) = 1$
 $\langle proof \rangle$

lemma *char-two-neg*:
fixes $x :: 'a::comm-ring-1$
assumes $two: (2 :: 'a) = 0$
shows $-x = x$
 $\langle proof \rangle$

lemma *b2-char-two*:

```

fixes  $W :: 'a::comm-ring-1$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
shows  $b2\ W = a1\ W^2$ 
 $\langle proof \rangle$ 

lemma b4-char-two:
fixes  $W :: 'a::comm-ring-1$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
shows  $b4\ W = a1\ W * a3\ W$ 
 $\langle proof \rangle$ 

lemma b6-char-two:
fixes  $W :: 'a::comm-ring-1$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
shows  $b6\ W = a3\ W^2$ 
 $\langle proof \rangle$ 

lemma b8-char-two:
fixes  $W :: 'a::comm-ring-1$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
shows  $b8\ W =$ 
 $a1\ W^2 * a6\ W + a1\ W * a3\ W * a4\ W +$ 
 $a2\ W * a3\ W^2 + a4\ W^2$ 
 $\langle proof \rangle$ 

lemma discriminant-char-two-expanded:
fixes  $W :: 'a::comm-ring-1$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
shows discriminant  $W =$ 
 $a1\ W^6 * a6\ W + a1\ W^5 * a3\ W * a4\ W +$ 
 $a1\ W^4 * a2\ W * a3\ W^2 + a1\ W^4 * a4\ W^2 +$ 
 $a3\ W^4 + a1\ W^3 * a3\ W^3$ 
 $\langle proof \rangle$ 

lemma discriminant-char-two-a1-zero:
fixes  $W :: 'a::field$  weierstrass-coeffs
assumes  $two: (2 :: 'a) = 0$ 
and  $a1: a1\ W = 0$ 
shows discriminant  $W = a3\ W^4$ 
 $\langle proof \rangle$ 

lemma scaled-power-eq:
fixes  $q\ x\ n :: 'a::comm-semiring-1$ 
assumes  $q * x = n$ 
shows  $q^k * x^k = n^k$ 
 $\langle proof \rangle$ 

lemma scale-linear-six:
fixes  $a\ c\ x :: 'a::comm-ring-1$ 

```

shows $a \wedge 6 * (c * x) = a \wedge 5 * c * (a * x)$
 <proof>

lemma *diff-rearrange*:

fixes $a\ x\ y\ c :: 'a::comm-ring-1$
assumes $a * y - x \wedge 2 - c = 0$
shows $y * a = x \wedge 2 + c$
 <proof>

lemma *char-two-affine-certificate-raw*:

fixes $A1\ A2\ A3\ A4\ A6 :: 'a::field$
assumes *two*: $(2 :: 'a) = 0$
and $A1: A1 \neq 0$
shows $A1 \wedge 6 * (((((A3 / A1) \wedge 2 + A4) / A1) \wedge 2 + A1 * (A3 / A1) * (((A3 / A1) \wedge 2 + A4) / A1) + A3 * (((A3 / A1) \wedge 2 + A4) / A1)) - ((A3 / A1) \wedge 3 + A2 * (A3 / A1) \wedge 2 + A4 * (A3 / A1) + A6)) = A1 \wedge 6 * A6 + A1 \wedge 5 * A3 * A4 + A1 \wedge 4 * A2 * A3 \wedge 2 + A1 \wedge 4 * A4 \wedge 2 + A3 \wedge 4 + A1 \wedge 3 * A3 \wedge 3$
 <proof>

lemma *discriminant-char-two-certificate*:

fixes $W :: 'a::field\ weierstrass-coeffs$
assumes *two*: $(2 :: 'a) = 0$
and $a1: a1\ W \neq 0$
shows $a1\ W \wedge 6 * (weierstrass-affine-poly\ W\ (a3\ W / a1\ W) (((a3\ W / a1\ W) \wedge 2 + a4\ W) / a1\ W) = discriminant\ W$
 <proof>

lemma *singular-affine-imp-discriminant-zero-char-two*:

fixes $W :: 'a::field\ weierstrass-coeffs$
assumes *two*: $(2 :: 'a) = 0$
and *singular*: *singular-affine-point* $W\ x\ y$
shows *discriminant* $W = 0$
 <proof>

lemma *discriminant-zero-imp-affine-singular-char-two*:

fixes $W :: 'a::alg-closed-field\ weierstrass-coeffs$
assumes *two*: $(2 :: 'a) = 0$
and *delta*: *discriminant* $W = 0$
shows $\exists x\ y. \text{ singular-affine-point } W\ x\ y$
 <proof>

12 Odd characteristic

lemma *scale-quadratic*:

fixes $q\ x\ b\ c :: 'a::comm-ring-1$
shows $q^2 * (6 * x^2 + b * x + c) =$
 $6 * (q^2 * x^2) + b * q * (q * x) + c * q^2$
 $\langle proof \rangle$

lemma *c4-h-n-square*:

fixes $b\ c\ d :: 'a::comm-ring-1$
shows $(18 * d - b * c)^2 =$
 $324 * d^2 - 36 * b * c * d + b^2 * c^2$
 $\langle proof \rangle$

lemma *c4-h-q-square*:

fixes $b\ c :: 'a::comm-ring-1$
shows $(b^2 - 24 * c)^2 =$
 $b^4 - 48 * b^2 * c + 576 * c^2$
 $\langle proof \rangle$

lemma *c4-h-middle*:

fixes $b\ c\ d :: 'a::comm-ring-1$
shows $b * (b^2 - 24 * c) * (18 * d - b * c) =$
 $18 * b^3 * d - b^4 * c - 432 * b * c * d +$
 $24 * b^2 * c^2$
 $\langle proof \rangle$

lemma *c4-h-polynomial*:

fixes $b\ c\ d :: 'a::comm-ring-1$
shows $6 * (18 * d - b * c)^2 +$
 $b * (b^2 - 24 * c) * (18 * d - b * c) +$
 $c * (b^2 - 24 * c)^2 =$
 $18 * (b^3 * d - b^2 * c^2 - 36 * b * c * d +$
 $32 * c^3 + 108 * d^2)$
 $\langle proof \rangle$

lemma *c4-candidate-h-raw*:

fixes $b\ c\ d :: 'a::field$
assumes $b^2 - 24 * c \neq 0$
shows $(b^2 - 24 * c)^2 *$
 $(6 * ((18 * d - b * c) / (b^2 - 24 * c))^2 +$
 $b * ((18 * d - b * c) / (b^2 - 24 * c)) + c) =$
 $18 * (b^3 * d - b^2 * c^2 - 36 * b * c * d +$
 $32 * c^3 + 108 * d^2)$
 $\langle proof \rangle$

lemma *c4-candidate-h-certificate*:

fixes $W :: 'a::field\ weierstrass-coeffs$
assumes $c4: c4\ W \neq 0$

shows $c_4 W^{\wedge 2} * \text{weierstrass-h } W ((18 * b_6 W - b_2 W * b_4 W) / c_4 W) = -72 * \text{discriminant } W$
 <proof>

lemma bezout-coefficient-rearrange:
fixes $b \ c \ d \ x :: 'a::\text{comm-ring-1}$
shows $b^{\wedge 3} + 6 * b^{\wedge 2} * x - 30 * b * c - 144 * c * x + 108 * d = b^{\wedge 3} - 30 * b * c + 108 * d + 6 * ((b^{\wedge 2} - 24 * c) * x)$
 <proof>

lemma c4-candidate-bezout-coefficient:
fixes $W :: 'a::\text{field weierstrass-coeffs}$
assumes $c_4: c_4 W \neq 0$
shows $b_2 W^{\wedge 3} + 6 * b_2 W^{\wedge 2} * ((18 * b_6 W - b_2 W * b_4 W) / c_4 W) - 30 * b_2 W * b_4 W - 144 * b_4 W * ((18 * b_6 W - b_2 W * b_4 W) / c_4 W) + 108 * b_6 W = -c_6 W$
 <proof>

lemma c4-candidate-g-from-h-delta:
fixes $W :: 'a::\text{field weierstrass-coeffs}$
assumes $c_4: c_4 W \neq 0$
and $\text{delta: discriminant } W = 0$
and $h: \text{weierstrass-h } W$
 $((18 * b_6 W - b_2 W * b_4 W) / c_4 W) = 0$
shows $\text{weierstrass-g } W$
 $((18 * b_6 W - b_2 W * b_4 W) / c_4 W) = 0$
 <proof>

lemma square-twelve-scale:
fixes $b \ x :: 'a::\text{comm-ring-1}$
shows $144 * b * x^{\wedge 2} = b * (12 * x)^{\wedge 2}$
 <proof>

lemma zero-h-rearrange:
fixes $x \ b \ c :: 'a::\text{comm-ring-1}$
shows $24 * (6 * x^{\wedge 2} + b * x + c) = (12 * x)^{\wedge 2} + 2 * b * (12 * x) + 24 * c$
 <proof>

lemma zero-g-rearrange:
fixes $x \ b \ c \ d :: 'a::\text{comm-ring-1}$
shows $216 * (4 * x^{\wedge 3} + b * x^{\wedge 2} + 2 * c * x + d) = 72 * x^{\wedge 2} * (12 * x + 3 * b) + 36 * c * (12 * x) + 216 * d$

$\langle \text{proof} \rangle$

lemma *zero-c-invariant-h-raw*:

fixes $b\ c :: 'a::\text{field}$

assumes $(12 :: 'a) \neq 0$

shows $24 * (6 * (-b / 12) ^ 2 + b * (-b / 12) + c) =$
 $- (b ^ 2 - 24 * c)$

$\langle \text{proof} \rangle$

lemma *zero-c-invariant-g-raw*:

fixes $b\ c\ d :: 'a::\text{field}$

assumes $(12 :: 'a) \neq 0$

shows $216 * (4 * (-b / 12) ^ 3 + b * (-b / 12) ^ 2 +$
 $2 * c * (-b / 12) + d) =$
 $b ^ 3 - 36 * b * c + 216 * d$

$\langle \text{proof} \rangle$

lemma *zero-c-invariant-h-certificate*:

fixes $W :: 'a::\text{field weierstrass-coeffs}$

assumes $(12 :: 'a) \neq 0$

shows $24 * \text{weierstrass-h } W (-b2\ W / 12) = -\ c4\ W$

$\langle \text{proof} \rangle$

lemma *zero-c-invariant-g-certificate*:

fixes $W :: 'a::\text{field weierstrass-coeffs}$

assumes $(12 :: 'a) \neq 0$

shows $216 * \text{weierstrass-g } W (-b2\ W / 12) = -\ c6\ W$

$\langle \text{proof} \rangle$

lemma *discriminant-zero-imp-affine-singular-odd*:

fixes $W :: 'a::\text{alg-closed-field weierstrass-coeffs}$

assumes $\text{two}: (2 :: 'a) \neq 0$

and $\text{delta}: \text{discriminant } W = 0$

shows $\exists x\ y. \text{ singular-affine-point } W\ x\ y$

$\langle \text{proof} \rangle$

13 The discriminant criterion

lemma *singular-affine-imp-discriminant-zero*:

fixes $W :: 'a::\text{field weierstrass-coeffs}$

assumes $\text{singular-affine-point } W\ x\ y$

shows $\text{discriminant } W = 0$

$\langle \text{proof} \rangle$

theorem *projective-singular-iff-discriminant-zero*:

fixes $W :: 'a::\text{alg-closed-field weierstrass-coeffs}$

shows $(\exists p. \text{ singular-projective-point } W\ p) \longleftrightarrow$
 $\text{discriminant } W = 0$

$\langle \text{proof} \rangle$

lemma *b2-map-to-ac* [simp]:
 $b2 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (b2 \ W)$
 ⟨proof⟩

lemma *b4-map-to-ac* [simp]:
 $b4 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (b4 \ W)$
 ⟨proof⟩

lemma *b6-map-to-ac* [simp]:
 $b6 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (b6 \ W)$
 ⟨proof⟩

lemma *b8-map-to-ac* [simp]:
 $b8 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (b8 \ W)$
 ⟨proof⟩

lemma *c4-map-to-ac* [simp]:
 $c4 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (c4 \ W)$
 ⟨proof⟩

lemma *c6-map-to-ac* [simp]:
 $c6 \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) = to\text{-}ac \ (c6 \ W)$
 ⟨proof⟩

lemma *discriminant-map-to-ac* [simp]:
 $discriminant \ (map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W) =$
 $to\text{-}ac \ (discriminant \ W)$
 ⟨proof⟩

definition *projective-weierstrass-nonsingular* ::
 $'a::field \ weierstrass\text{-}coeffs \Rightarrow bool$
where
 $projective\text{-}weierstrass\text{-}nonsingular \ W \longleftrightarrow$
 $projective\text{-}weierstrass\text{-}nonsingular\text{-}over$
 $(map\text{-}weierstrass\text{-}coeffs \ to\text{-}ac \ W)$

theorem *weierstrass-nonsingular-iff*:
fixes $W :: 'a::field \ weierstrass\text{-}coeffs$
shows $projective\text{-}weierstrass\text{-}nonsingular \ W \longleftrightarrow$
 $discriminant \ W \neq 0$
 ⟨proof⟩

end
theory *Weierstrass-j-Invariant*
imports *Weierstrass-Discriminant-Criterion*
begin

14 The partial j-invariant

definition *weierstrass-j* ::

'a::field weierstrass-coeffs $\Rightarrow$ 'a option

where

weierstrass-j W =

(if projective-weierstrass-nonsingular W

then Some (c4 W $\wedge$ 3 / discriminant W)

else None)

lemma *weierstrass-j-nonsingular:*

assumes *projective-weierstrass-nonsingular W*

shows *weierstrass-j W = Some (c4 W $\wedge$ 3 / discriminant W)*

<proof>

lemma *weierstrass-j-discriminant-nonzero:*

assumes *discriminant W $\neq$ 0*

shows *weierstrass-j W = Some (c4 W $\wedge$ 3 / discriminant W)*

<proof>

lemma *weierstrass-j-singular:*

assumes $\neg$ *projective-weierstrass-nonsingular W*

shows *weierstrass-j W = None*

<proof>

lemma *weierstrass-j-eq-none-iff [simp]:*

weierstrass-j W = None $\longleftrightarrow$ discriminant W = 0

<proof>

lemma *weierstrass-j-eq-some-iff:*

weierstrass-j W = Some j $\longleftrightarrow$

discriminant W $\neq$ 0 $\wedge$ j = c4 W $\wedge$ 3 / discriminant W

<proof>

lemma *weierstrass-j-defined-iff:*

weierstrass-j W $\neq$ None $\longleftrightarrow$

projective-weierstrass-nonsingular W

<proof>

end

theory *Short-Weierstrass-Bridge*

imports

Weierstrass-j-Invariant

Elliptic-Curves-Group-Law.Elliptic-Axclass

begin

15 Specialization to short Weierstrass equations

lemma *discriminant-short-weierstrass:*

```

fixes A B :: 'a::comm-ring-1
shows discriminant (short-weierstrass-coeffs A B) =
  -16 * (4 * A ^ 3 + 27 * B ^ 2)
  <proof>

lemma on-weierstrass-affine-short:
  fixes A B x y :: 'a::comm-ring-1
  shows on-weierstrass-affine (short-weierstrass-coeffs A B) x y
     $\longleftrightarrow y^2 = x^3 + A * x + B$ 
    <proof>

lemma on-weierstrass-affine-short-iff-on-curve:
  fixes A B x y :: 'a::ell-field
  shows on-weierstrass-affine (short-weierstrass-coeffs A B) x y
     $\longleftrightarrow$  on-curve A B (Point x y)
    <proof>

theorem projective-weierstrass-nonsingular-short-iff:
  fixes A B :: 'a::ell-field
  shows projective-weierstrass-nonsingular
    (short-weierstrass-coeffs A B)
     $\longleftrightarrow$  nonsingular A B
    <proof>

end

```

References

- [1] S. Berghofer. The group law for elliptic curves. *Archive of Formal Proofs*, February 2017. https://isa-afp.org/entries/Elliptic_Curves_Group_Law.html, Formal proof development.
- [2] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009. DOI: <https://doi.org/10.1007/978-0-387-09494-6>.