Elliptic Curves

Harry Armitage

November 3, 2020

Contents

1 Fermat's Method of Infinite Descent

Suppose we have a right-angled triangle Δ with side lengths a, b, c, so that by Pythagoras we have $a^2 + b^2 = c^2$, and area$(\Delta) = \frac{1}{2}ab$.

Definition 1.1. *Δ is* **rational** *if $a, b, c \in \mathbb{Q}$, and* **primitive** *if $a, b, c \in \mathbb{Z}$ coprime.*

Lemma 1.2. *Every primitive triangle is of the form $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$ for coprime integers $u > v > 0$.*

Proof. If a, b were both odd, then $a^2 + b^2 \equiv 2 \mod 4$, and we have no solutions for c. If a, b both even, then they are not coprime. So we may assume a is odd, b is even, c is odd.

Then $(\frac{b}{2})^2 = \frac{c+a}{2}\frac{c-a}{2}$, and the right hand side is a product of coprime positive integers. So by unique prime factorisation in the integers, $\frac{c+a}{2} = u^2$, $\frac{c-a}{2} = v^2$ for some coprime integers u, v. Rearranging, we have the lemma. □

Definition 1.3. *$D \in \mathbb{Q}_{>0}$ is a* **congruent number** *if it is the area of a rational triangle.*

Note that, by scaling the triangle, it suffices to consider $D \in \mathbb{Z}_{>0}$ squarefree.

For example, $D = 5, 6$ are congruent numbers. $6 = \frac{1}{2} \cdot 3 \cdot 4$, and $3^2 + 4^2 = 5^2$, and 5 is left as an exercise.

Lemma 1.4. *$D \in \mathbb{Q}_{>0}$ is congruent if and only if $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}, y \neq 0$.*

Proof. Lemma **1.2** shows that D is congruent if and only if $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$.

Setting $x = \frac{u}{v}, y = \frac{w}{v^2}$ finishes the proof. □

Fermat showed that 1 is not a congruent number.

Theorem 1.5. *There is no solution to*

$$w^2 = uv(u + v)(u - v) \tag{$*$}$$

in integers u, v, w with $w \neq 0$.

Proof. Without loss of generality, u, v are coprime with $u > 0, w > 0$. If $v < 0$ then replace (u, v, w) by $(-v, u, w)$. If u, v are both odd, then replace (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$. So we may assume that all of $u, v, u + v, u - v$ are coprime positive integers whose product is a square, and hence are all squares, say a^2, b^2, c^2, d^2 respectively, where $a, b, c, d \in \mathbb{Z}_{>0}$.

Since $u \not\equiv v \mod 2$, both c, d are odd. Consider the right angled triangle with side lengths, $\frac{c+d}{2}, \frac{c-d}{2}, a$. This is a primitive triangle, and it has area $\frac{c^2-d^2}{8} = \frac{v}{4} = (\frac{b}{2})^2$.

Let $w_1 = \frac{b}{2}$. Then lemma **1.2** gives $w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$ for some $u_1, v_1 \in \mathbb{Z}$, giving a new solution to $(*)$. But $4w_1^2 = b^2 = v | w^2$, and so $w_1 \leq \frac{1}{2}w$.

So by Fermat's method of infinite descent, if there were a solution we would have a strictly decreasing infinite sequence of positive integers $\lightning$. Hence there is no solution to $(*)$. □

1.1 A Variant for Polynomials

Here, K is a field with char $K \neq 2$. The algebraic closure of K will be $\overline{K}$.

Lemma 1.6. *Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for four distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in K$.*

Proof. Without loss of generality we may assume $K = \overline{K}$, as that doesn't change the degree of polynomials, and every square is still a square.

Changing coordinates on $\mathbb{P}^1$, we may assume the ratios $\alpha : \beta$ are $(1:0), (0:1), (1:-1), (1:-\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$, with $\mu = \sqrt{\lambda}$.

Then $u = a^2, v = b^2, u - v = (a+b)(a-b), u - \lambda v = (a + \mu b)(a - \mu b)$ are all squares. They are also coprime, and so by unique factorisation in $K[t]$, $(a+b), (a-b), (a+\mu b), (a - \mu b)$ are all squares.

But $\max\{\deg a, \deg b\} \leq \frac{1}{2} \max\{\deg u, \deg v\}$. So by Fermat's method of infinite descent, we get that the original $u, v \in K$. $\square$

Now we have some important definitions:

Definition 1.7.

1. *An* **elliptic curve** *E over a field K is the projective closure of the affine curve $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic polynomial with distinct roots.*
2. *For L/K any field extension, $E(L) = \{(x, y) \in L^2 : y^2 = f(x)\} \cup \{0\}$. 0 is called the* **point at infinity**.

We call the point at infinity 0 because we will see that $E(L)$ is naturally an abelian group under an operation we will denote by $+$, and 0 will be the identity for that group. In this course we will study $E(L)$ for L a finite field, a local field, and a number field.

Lemma **1.4** and theorem **1.5** together imply that, if E is given by $y^2 = x^3 - x$, then $E(\mathbb{Q}) = \{0, (0,0), (\pm 1, 0)\}$, which we will see is the group $C_2 \times C_2$.

Corollary 1.8. *Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.*

Proof. Without loss of generality, $K = \overline{K}$. By a change of coordinates we may assume $E : y^2 = x(x-1)(x-\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ with $u, v \in K[t]$ coprime. Then $w^2 = uv(u-v)(u - \lambda v)$ for some $w \in K[t]$.

Unique factorisation in $K[t]$ gives $u, v, u - v, u - \lambda v$ are all squares, and so by lemma **1.6**, $u, v \in K$, and so $x, y \in K$. $\square$

2 Some Remarks on Algebraic Curves

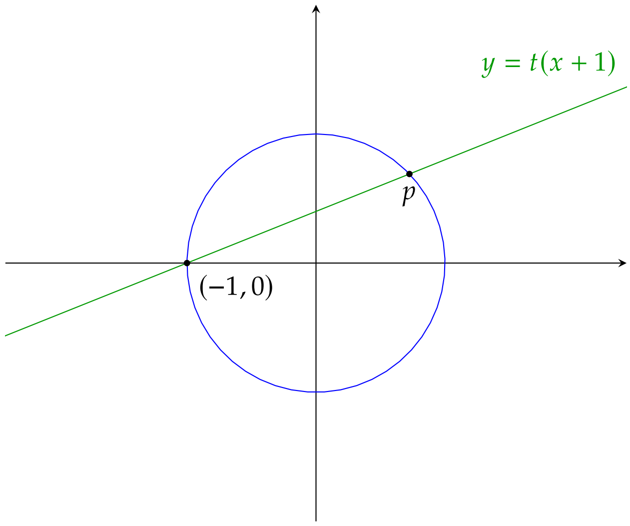
We will be working over an algebraically closed field K.

Definition 2.1. *An (irreducible) plane algebraic curve $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$ is* **rational** *if it has a rational parametrization, i.e. there are $\phi, \psi \in K(t)$ such that:*

1. *$\mathbb{A}^1 \to \mathbb{A}^2; t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finite set}\}$.*
2. *$f(\phi(t), \psi(t)) = 0$.*

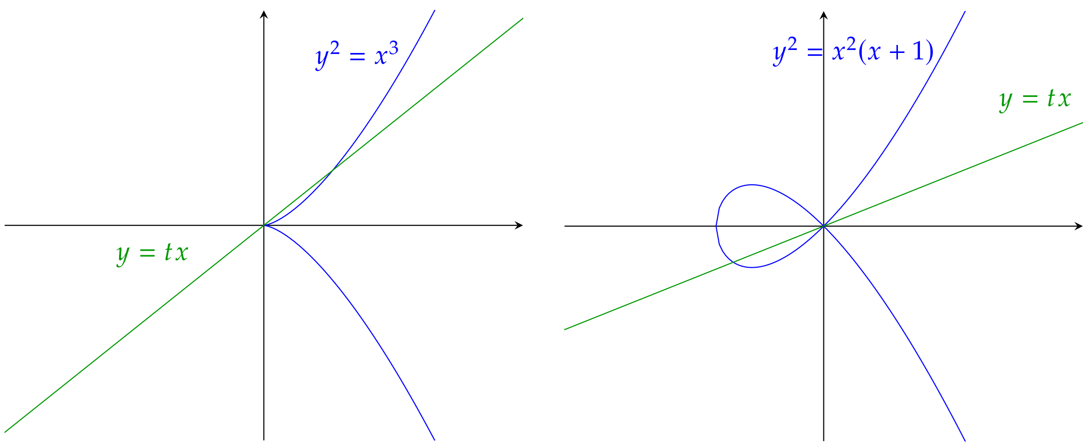
Examples 2.2.

1. Any nonsingular plane conic is rational. For example, take a circle $x^2 + y^2 = 1$. Pick a point on it, $(-1, 0)$. Now draw a line through it with slope t, and solve for the points of intersection between the curve and the line.



Solving for the coordinates of p, we get the quadratic $x^2 + t^2(x+1)^2 = 1$, i.e. $x = -1$ or $\frac{1-t^2}{1+t^2}$. So we have the rational parametrization $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$

2. Any singular plane cubic is rational.



(a) Rational Parametrization $(x, y) = (t^2, t^3)$

(b) Left as an example on the first sheet

3. Corollary **1.8** shows that elliptic curves are *not* rational.

Definition 2.3. *The* **genus** $g(C) \in \mathbb{Z}_{\geq 0}$ *is an invariant of a smooth projective curve.*

- *If $K = \mathbb{C}$, then $g(C)$ = genus of the Riemann surface C.*

- *A smooth plane curve $C \subset \mathbb{P}^2$ of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$.*

Proposition 2.4. *Let C be a smooth projective curve over K, an algebraically closed field. Then:*

1. *C is rational $\iff$ $g(C) = 0$.*
2. *C is an elliptic curve $\iff$ $g(C) = 1$.*

Proof. A proof of *1* is omitted from this course. For 2, we check (on the first example sheet) that elliptic curves are smooth plane curves. Then they have degree 3, so genus $\frac{2\cdot 1}{2} = 1$. For the other direction, see later on in the course. $\square$

2.1 Order of Vanishing

C will be an algebraic curve, and $K(C)$ its function field, with $P \in C$ a smooth point. Write $\mathrm{ord}_P(f)$ to mean the order of vanishing of $f \in K(C)$ at P (negative if f has a pole).

Fact: $\mathrm{ord}_P : K(C)^\times \to \mathbb{Z}$ is a discrete valuation, i.e. $\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2)$ and $\mathrm{ord}_P(f_1 + f_2) \geq \min\{\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)\}$.

We say $t \in K(C)^\times$ is a ***uniformizer*** at the point P if $\mathrm{ord}_P(t) = 1$.

Example 2.5. Let $C = \{g(x,y) = 0\} \subseteq \mathbb{A}^2$, where $g \in K[x,y]$ is irreducible. Then $K(C) = \mathrm{Frac}\,\frac{K[x,y]}{(g)}$, with $g = g_0 + g_1(x,y) + g_2(x,y) + \ldots$, g_i homogeneous of degree i.

Suppose $P = (0,0) \in C$ is a smooth point, i.e. $g_0 = 0, g_1(x,y) = \alpha x + \beta y$ with α, β not both zero.

Let $\gamma, \delta \in K$. It is a fact that $\gamma x + \delta y \in K(C)$ is a uniformizer at P if and only if $\frac{\gamma}{\delta} \neq \frac{\alpha}{\beta}$, i.e. $\alpha\delta - \beta\gamma \neq 0$.

Example 2.6. $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2, \lambda \neq 0, 1$. We take the projective closure, i.e. homogenize the equation as $\{Y^2 Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2$ by setting $x = X/Z, y = Y/Z$.

Have we got new points by taking projective closure? We only get these when $Z = 0$, i.e. $0 = X^3 \implies X = 0, Y \neq 0$. Since we're in projective space, this is just one point: $P = (0:1:0)$. We compute $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$. Put $t = X/Y, w = Z/Y$ (since we can't return to the original affine piece, as it doesn't contain $Z = 0$). Then we get $w = t(t-w)(t-\lambda w)$. Now P is the point $(t,w) = (0,0)$. This is a smooth point, as there are linear terms at that point (namely w). So $\mathrm{ord}_P(t) = \mathrm{ord}_P(t-2) = \mathrm{ord}_P(t - \lambda w) = 1$, and $\mathrm{ord}_P(w) = 1+1+1 = 3$.

Then:

$$
\begin{aligned}
\mathrm{ord}_P(x) &= \mathrm{ord}_P(X/Z) = \mathrm{ord}_P(t/w) = 1 - 3 = -2\\
\mathrm{ord}_P(y) &= \mathrm{ord}_P(Y/Z) = \mathrm{ord}_P(1/w) = -3
\end{aligned}
$$

2.2 Riemann Roch Spaces

Let C be a smooth projective curve. Then a ***divisor*** is a formal sum of points on C, say $D = \sum_{P \in C} n_P P$ where $n_P \in \mathbb{Z}$, and only finitely many n_P are nonzero, and let $\deg D = \sum_{P \in C} n_P$. These divisors form a group under addition, denoted $\mathrm{Div}(C)$.

D is said to be ***effective***, written $D \geq 0$ if $n_p \geq 0$ for all $P \in C$.

If $f \in K(C)^\times$, we write $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$.

The Riemann Roch space of $D \in \mathrm{Div}(C)$ is:

$$\mathscr{L}(D) = \{f \in K(C) : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$$

i.e. the K-vector space of rational functions on C with "poles no worse than specified by D."

Theorem 2.7 (Riemann Roch for genus 1)**.**

$$\dim \mathscr{L}(D) = \begin{cases} 0 & \deg D < 0 \\ 0 \textit{ or } 1 & \deg D = 0 \\ \deg D & \deg D > 0 \end{cases}$$

Example 2.6 (revisited). Our curve is $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$, together with $P = (0:1:0)$, the point at infinity. Recall $\mathrm{ord}_P(x) = -2, \mathrm{ord}_P(x) = -3$.

We thus deduce that $\mathscr{L}(2P) = \langle 1, x\rangle, \mathscr{L}(3P) = \langle 1, x, y\rangle$.

Proposition 2.8. *Let K be an algebraically closed field not of characteristic 2. Let $C \subset \mathbb{P}^2$ be a smooth plane cubic, and that $P \in C$ is a point of inflection. Then we may change coordinates such that:*

$$C : Y^2Z = X(X-Z)(X-\lambda Z), \quad \lambda \neq 0, 1$$
$$P = (0:1:0)$$

Proof. We make a change of coordinates such that $P = (0:1:0)$ and the tangent line to C at P, $T_P(C) = \{Z = 0\}$. Now let $C = \{F(X,Y,Z) = 0\}$.

Since $P \in C$ is a point of inflection, $F(t,1,0)$ has a triple root at $t = 0$. But F is degree 3, so we have $F(t,1,0) = kt^3$ for k some constant. I.e., there are no terms in F of the form X^2Y, XY^2, Y^3.

So $F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3\rangle$. The coefficient of Y^2Z is nonzero, as otherwise P would be singular. The coefficient of X^3 is also nonzero, as C is irreducible and otherwise $\{Z = 0\} \subset C$.

We are free to rescale X, Y, Z, F, and so WLOG C is defined by

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

We call this Weierstrass form.

Since our field doesn't have characteristic 2, we may complete the square by substituting $Y = Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$, we may assume $a_1 = a_3 = 0$.

Now $C : Y^2Z = Z^3f(X/Z)$, where f is a monic cubic polynomial. Since C is smooth, f has distinct roots, which are WLOG $0, 1, \lambda$. So

$$C : Y^2Z = X(X-Z)(X-\lambda Z)$$

which we call the Legendre form. □

It may be shown that the points of inflection on $C = \{F = 0\} \subset \mathbb{P}^2$ are given by $F = \det\left(\frac{\partial^2 f}{\partial X_i \partial X_j}\right) = 0$

2.3 The Degree of a Morphism

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Let $\phi^* : K(C_2) \to K(C_1), f \mapsto f \circ \phi$.

Definition.

1. $\deg \phi = [K(C_1) : \phi^* K(C_2)]$
2. *ϕ is separable if $K(C_1)/\phi^* K(C_2)$ is a separable field extension (which by Galois theory is automatic if* $\operatorname{char} K = 0$*)*

Suppose $P \in C_1, Q \in C_2, \phi : P \to Q$. Let $t \in K(C_2)$ be a uniformizer at Q. We then define $e_\phi(p) = \operatorname{ord}_P(\phi^* t)$, which is always ≥ 1, and independent of t. $e_\phi(P)$ is called the ***ramification index*** of ϕ at p.

Theorem 2.9. *Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then*

$$\sum_{p \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

for any point $Q \in C_2$. Moreover, if ϕ is separable then $e_\phi(P) = 1$ with at most finitely many exceptions.

In particular:

1. *ϕ is surjective*
2. *If ϕ is separable, $\#\phi^{-1}(Q) \leq \deg \phi$, with equality for all but finitely many choices of Q.*

Remark 2.10. Let C be an algebraic curve. A rational map is given by $\phi : C \dashrightarrow \mathbb{P}^n, P \mapsto (f_0(P) : \ldots : f_n(P))$, where $f_0, \ldots, f_n \in K(C)$ are not all zero. If C is smooth then ϕ is a morphism.

3 Weierstrass Equations

In this section, K is a perfect field (so that all finite extensions of K are separable), with algebraic closure $\bar{K}$.

Definition. An elliptic curve E over K is a smooth projective curve of genus 1 defined over K with a specified K-rational point O_E.

Example: Take $\{X^3 + pY^3 + p^2 Z^3 = 0\} \subset \mathbb{P}^2$ for p prime. This is not an elliptic curve over $\mathbb{Q}$ since there is no $\mathbb{Q}$-points.

Theorem 3.1. *Every elliptic curve E is isomorphic over K to a curve in Weierstrass form via an isomorphism taking O_E to* $(0 : 1 : 0)$.

Proposition **2.8** treated the special case where E is a smooth plane cubic and O_E is a point of inflection.

If $D \in \operatorname{Div}(E)$ is defined over K (i.e. fixed by the natural action of $\operatorname{Gal}(\bar{K}/K)$, then $\mathscr{L}(D)$ has a basis in $K(E)$, not just in $\bar{K}(E)$).

Proof. Note that

$$\mathscr{L}(2O_E) \subset \mathscr{L}(3O_E)$$

Pick bases of these spaces, say $\{1, x\}$ and $\{1, x, y\}$.

Note that $\mathrm{ord}_{O_E}(x) = -2, \mathrm{ord}_{O_E}(y) = -3$. The 7 elements $\{1, x, y, x^2, xy, x^3, y^2\}$ are rational functions with no pole except at O_E, where they have poles of degree at most 6, so they all lie in $\mathscr{L}(6O_E)$. Riemann-Roch tells us this space has dimension 6, so there is a dependence relation between these elements.

Leaving out x^3 or y^2 gives a basis for $\mathscr{L}(6O_E)$ since each term has a different order pole at O_E, so they are independent.

Therefore this dependence relation *must* involve both x^3 and y^2. Rescaling x, y we get

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

Let E' be the curve defined by this equation (or rather its projective closure).

There is a morphism

$$\begin{aligned} \phi : E &\to E' \\ P &\mapsto (x(P) : y(P) : 1) = \left(\frac{x}{y}(P) : 1 : \frac{1}{y}(P)\right) \\ O_E &\mapsto (0 : 1 : 0) \end{aligned}$$

$[K(E) : K(x)] = \deg(E \xrightarrow{x} \mathbb{P}^1) = \mathrm{ord}_{O_E}\left(\frac{1}{x}\right) = 2$
$[K(E) : K(y)] = \deg(E \xrightarrow{y} \mathbb{P}^1) = \mathrm{ord}_{O_E}\left(\frac{1}{y}\right) = 3$

This gives us a diagram of field extensions

$$\begin{tikzcd} & K(E) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "3"] & \\ & K(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\ K(x) & & K(y) \end{tikzcd}$$

So $[K(E) : K(x, y)]$ divides both 2 and 3 by the tower law, and hence $K(E) = K(x, y)$, and hence $\deg(E \xrightarrow{\phi} E') = 1$, and ϕ is birational. If E' is singular, then it is rational, and so E is also rational $\lightning$. So E' is not singular and hence smooth, and we may use remark **2.10** to ϕ^{-1} to see that ϕ^{-1} is a morphism, and hence ϕ is an isomorphism. $\square$

Proposition 3.2. *Let E, E' be elliptic curves over K in Weierstrass form. Then $E \cong E'$ over K if and only if the Weierstrass equations are related by a change of variables of the form*

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

for $u, r, s, t \in K, u \neq 0$.

Proof. Using the notation of the previous proof,

$$\begin{aligned} \langle 1, x\rangle =& \mathscr{L}(2O_E) = \langle 1, x'\rangle \\ \langle 1, x, y\rangle =& \mathscr{L}(3O_E) = \langle 1, x', y'\rangle \\ \implies & \begin{cases} x = \lambda x' + r & \lambda_1 r \in K, \lambda \neq 0 \\ y = \mu y' + \sigma x' + t & \mu, \sigma, t \in K, \mu \neq 0 \end{cases} \end{aligned}$$

Looking at the coefficients of x^3 and y^2, $\lambda^3 = \mu^2 \implies (\lambda, \mu) = (u^2, u^3)$ for $u \in K^\times$.
Put $s = \sigma/u^2$ □

The effect of this transformation on the coefficients a_i is on the formula sheet for this course. A Weierstrass equation defines an elliptic curve if and only if defines a smooth curve, if and only if $\Delta(a_1, \dots, a_6) \neq 0$ where Δ is as follows:

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_3 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{aligned}$$

If $\operatorname{char} K \neq 2, 3$, then we can reduce to the case

$$\begin{aligned} E : y^2 &= x^3 + ax + b \\ \Delta &= -16(4a^3 + 26b^2) \end{aligned}$$

Corollary 3.3. *Assume* $\operatorname{char} K \neq 2, 3$. *If we have two elliptic curves*

$$\begin{aligned} E : y^2 &= x^3 + ax + b \\ E' : y^2 &= x^3 + a'x + b' \end{aligned}$$

then they are isomorphic over K if and only if

$$\begin{aligned} a' &= u^4 a \\ b' &= u^6 b \end{aligned}$$

for some $u \in K^\times$.

Proof. E and E' are related as in **3.2** with $r = s = t = 0$. □

Definition. The ***j-invariant*** is $j(E) = \frac{1728(4a^3)}{4a^3+27b^2}$. Note that the denominator is nonzero since the discriminant is nonzero.

Corollary 3.4. $E \cong E' \implies j(E) = j(E')$*, and the converse holds if* $K = \bar{K}$.

Proof.

$$\begin{aligned} E \cong E' &\iff a' = u^4 a; b' = u^6 b \text{ for some } u \in K^\times \\ &\implies (a^3 : b^2) = ((a')^3 : (b')^2) \\ &\iff j(E) = j(E') \end{aligned}$$

and the reverse implication holds in the second line if $K = \bar{K}$. □

4 Group Law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic, and $O_E \in E(K)$. Since E is of degree 3, it meets each line in 3 points counted with multiplicity. Hence, given two points P, Q on E, the line $\overline{PQ}$ meets E at a third point S. Then the line $\overline{O_E S}$ meets E at a third point R. We then define $P \oplus Q = R$.

If $P = Q$, then we take the tangent line at P, likewise if $S = O_E$. We can view this diagrammatically as follows:

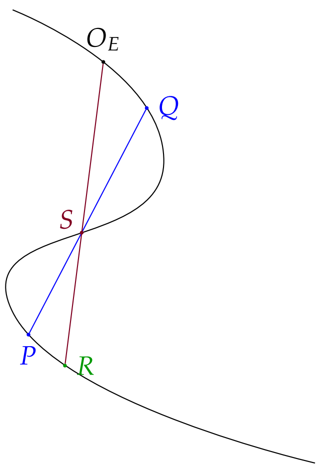


Figure 2: Illustration of the group operation on an elliptic curve

We call this the "chord and tangent process".

Theorem 4.1. $(E, \oplus)$ *is an abelian group.*

Proof.

(i) $P \oplus Q = Q \oplus P$ by construction.

(ii) O_E is the identity.

(iii) For inverses, let S be the third point of intersection of T_{O_E} and E, and Q be the third point of intersection of $\overline{PS}$ and E. Then $P \oplus Q = O_E$.

(iv) Associativity is much harder.

□

Definition. $D_1, D_2 \in Div(E)$ are ***linearly equivalent*** (written $D_1 \sim D_2$) if there is $f \in \bar{K}(E)^\times$ such that $\mathrm{div}(f) = D_1 - D_2$. Then we will let $[D] = \{D' : D' \sim D\}$.

Definition. The ***Picard group of E***, $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$. We write $\mathrm{Div}^0(E) := \ker\left(\mathrm{Div}(E) \xrightarrow{\deg} \mathbb{Z}\right)$ for the group of degree 0 divisors on E, and then $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$. Sometimes Pic^0 is called the Jacobian.

Proposition 4.2. *Let $\psi : E \to \mathrm{Pic}^0(E); P \mapsto [(P) - (O_E)]$. Then:*

1. $\psi(P \oplus Q) = \psi(P) + \psi(Q)$
2. *ψ is a bijection*

Proof.

1. Referring back to Fig. 2, let $\{\ell = 0\}$ be the line $\overline{PQ}$, and $\{m = 0\}$ be the line $\overline{O_E R}$. Then:

$$\begin{aligned} \mathrm{div}(\ell/m) &= (P) + (S) + (Q) - (R) - (S) - (O_E) \\ &= (P) + (Q) - (O_E) - (P \oplus Q) \\ \implies (P \oplus Q) + (O_E) &\sim (P) + (Q) \\ \implies (P \oplus Q) - (O_E) &\sim (P) - (O_E) + (Q) - (O_E) \\ \implies \psi(P \oplus Q) &= \psi(P) + \psi(Q) \end{aligned}$$

2. For injectivity, suppose $\psi(P) = \psi(Q)$. Then there is $f \in \bar{K}(E)^\times$ such that $\mathrm{div}(f) = P - Q$. Then $\deg\left(E \xrightarrow{f} \mathbb{P}^1\right) = \mathrm{ord}_P(f) = 1$. But then f is a birational morphism, so an isomorphism, and $E \cong \mathbb{P}^1 \lightning$.

   For surjectivity, let $[D] \in \mathrm{Pic}^0(E)$. Then $D + (O_E)$ has degree 1 (as D had degree 0). Then Riemann-Roch tells us $\dim \mathscr{L}(D + (O_E)) = 1$, and so there exists some $f \in \bar{K}(E)^\times$ such that $\mathrm{div}(f) + D + (O_E) \geq 0$. Since f is rational, $\deg \mathrm{div}(f) = 0$, and $\deg D = 0$. So the coefficients of $\mathrm{div}(f) + D + (O_E)$ are non-negative and sum to 1, hence one of them is 1 and the rest are 0. So $\mathrm{div}(f) + D + (O_E) = (P)$ for some $P \in E$. But then $(P) - (O_E) \sim D$, i.e. $\psi(P) = [D]$.

□

So ψ is a bijection respecting the group law, and so we deduce that $\oplus$ is associative, and then $(E, \oplus) \overset{\psi}{\cong} (\mathrm{Pic}^0 E, +)$.

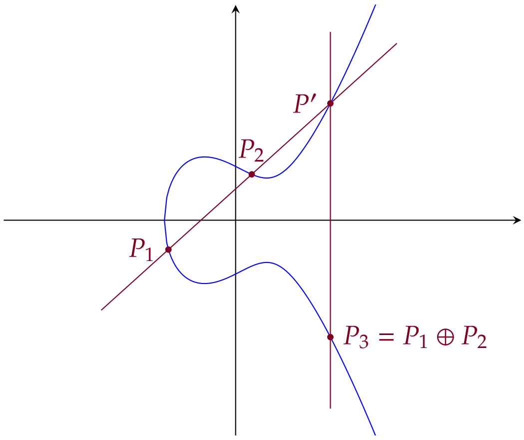
4.1 Explicit Formulae for the Group Law

We consider E in Weierstrass form, with O_E the point at infinity:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{$*$}$$

Note that O_E is a point of inflection. Now $P_1 \oplus P_2 \oplus P_3 = O_E \iff P_1, P_2, P_3$ are collinear.

We will use the following notation:



and put $P_i = (x_i, y_i)$, $P' = (x', y')$.

Now $\ominus P_1 = (x_1, -(a_1 x_1 + a_3) - y_1)$, just by setting $y = -y_1$ in $(*)$.

The line through P_1, P_2 has equation say $y = \lambda x + \nu$. Substituting into $(*)$ and looking at the coefficient of x^2, we get:

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x'$$

Since $x_3 = x'$, we have:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(a_1 x' + a_3) - y' \\ &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

It remains to find λ and ν. There are 3 cases:

1. $x_1 = x_2, P_1 \neq P_2$.

   Then $P_1 \oplus P_2 = O_E$.

2. $x_1 \neq x_2$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = y_1 - \lambda x_1 = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

3. $P_1 = P_2$.

   Here we have to compute the equation of the tangent line etc. The solutions are:

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}$$

Corollary 4.3. *$E(K)$ is an abelian group.*

Proof. It is a subgroup of E $(= E(\bar{K}))$.

Identity: $O_E \in E(K)$ by definition.

Closure: See formulae above.

Inverses: See formulae above.

Associativity: Inherited from $E(\bar{K})$.

Commutativity: Inherited from $E(\bar{K})$.

□

If there is no ambiguity (i.e. we are not also adding numbers at the same time), the circles will be dropped from the group operation.

Theorem 4.4. *Elliptic curves are group varieties.*

i.e., $[-1] : E \longrightarrow E; P \mapsto -P$ *and* $+ : E \times E \longrightarrow E; (P, Q) \mapsto P + Q$ *are morphisms of algebraic varieties.*

Proof. The above formulae show that $[-1]$ and $+$ are rational maps. We know immediately that $[-1]$ is a morphism, as it is a rational map from a smooth curve to a projective variety.

The formulae also show that $+$ is regular on the set

$$U = \{(P, Q) \in E \times E \mid P, Q, P + Q, P - Q \neq O_E\}$$

For $P \in E$, let $\tau_P : E \longrightarrow E; X \mapsto P + X$ be the "translation by P" map.

Then τ_P is a rational map from a smooth curve to a projective variety, so is a morphism.

We factor $+$ as:

$$E \times E \xrightarrow[\tau_{-A} \times \tau_{-B}]{} E \times E \xrightarrow[\tau_{A+B}]{} E \xrightarrow[\tau_{A+B}]{} E$$

Now $+$ is regular on $(\tau_A \times \tau_B)(U)$ for all $A, B \in E$, and so $+$ is regular on $E \times E$. □

Definition. For any $n \in \mathbb{Z}_{>0}$, let $[n] : E \longrightarrow E; P \mapsto P + \ldots + P$, n times, and $[-n] = [-1] \circ [n]$, $[0] : P \mapsto O_E$ (i.e., the standard way of turning an abelian group into $\mathbb{Z}$ module).

Definition. The ***n-torsion*** subgroup of E is $E[n] = \ker([n] : E \longrightarrow E)$.

Lemma 4.5. *If* $\mathrm{char}(K) \neq 2$, *and* $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$.

Then $E[2] = (0, (e_1, 0), (e_2, 0), (e_3 0)) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Proof. Let $P = (x, y) \in E$. Then $[2]P = 0 \iff P = -P \iff (x, y) = (x, -y) \iff y = 0$. □

4.2 Elliptic Curves over $\mathbb{C}$

Let $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$, where ω_1, ω_2 form a basis for $\mathbb{C}$ over $\mathbb{R}$.

Then the meromorphic functions on the Riemann surface (or lattice) $\mathbb{C}/\Lambda$ are the same as the Λ-invariant meromorphic functions on $\mathbb{C}$ (i.e. $f(z) = f(z + \lambda)$ for $\lambda \in \Lambda$).

This set of functions is a field, and is generated by $\wp(z)$ and $\wp'(z)$, where:

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

They satisfy $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$, for some $g_1, g_3 \in \mathbb{C}$ depending on λ. We call $\wp$ the ***Weierstrass p-function***.

One can show that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where E is the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. This is an isomorphism, not only of Riemann surfaces, but moreover of groups

Theorem 4.6 (Uniformisation Theorem). *Every elliptic curve over $\mathbb{C}$ arises in this way.*

Thus, for elliptic curves $E/\mathbb{C}$, we have:

1. $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$
2. $\deg[n] = n^2$

We will show that 2 holds over any field K, and 1 holds if $\operatorname{char} K \nmid n$.

Summary of Results (N.B. the isomorphisms in 1, 2, 4 respect the relevant topologies)

1. $K = \mathbb{C}$	$E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$
2. $K = \mathbb{R}$	$E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \Delta < 0 \end{cases}$
3. $K = \mathbb{F}_q$	$\lvert \#E(\mathbb{F}_q) - (q+1) \rvert \leq 2\sqrt{q}$
4. $[K : \mathbb{Q}_p] < \infty$	$E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$
5. $[K : \mathbb{Q}] < \infty$	$E(K)$ is a finitely generated abelian group.

5 Isogenies

Let E_1, E_2 be elliptic curves.

Definition. An ***isogeny*** $\phi : E_1 \to E_2$ is a non-constant morphism taking O_{E_1} to O_{E_2}, and we say E_1 and E_2 are ***isogenous*** if there is an isogeny $E_1 \to E_2$.

Definition. $\operatorname{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$. This is a group under $(\phi + \psi)(P) = \phi(P) + \psi(P)$.

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies, then $\psi\phi$ is an isogeny. The tower law tells us that $\deg(\psi\phi) = \deg(\phi)\deg(\psi)$.

Lemma 5.1. *If $0 \neq n \in \mathbb{Z}$, then $[n] : E \to E$ is an isogeny.*

Proof. Theorem **4.4** tells us that $[n]$ is a morphism. We must show that $[n] \neq 0$.

Assume $\operatorname{char} K \neq 2$, then we can use Lemma **4.5**. If $n = 2$, then $\#E[2] = 4$, and so $[2] \neq 0$.

If n is odd, then there is $0 \neq T \in E[2]$. Then $nT = T \neq 0$, so $[n]$ is not the zero map.

Now $[m][n] = [m] \circ [n]$, and any $n = 2^k m$ for m odd, so $[n]$ is not the zero map for any $n \neq 0$.

If $\operatorname{char} K = 2$, then replace **4.5** with a lemma computing $E[3]$. □

Corollary. $\operatorname{Hom}(E_1, E_2)$ *is torsion-free as a $\mathbb{Z}$-module.*

Lemma 5.2. *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.*

Sketch proof. ϕ induces a map $\phi_* : \mathrm{Div}^0(E_1) \to \mathrm{Div}^0(E_2)$ given by $\sum\limits_{P \in E_1} n_p P \mapsto \sum\limits_{P \in E_1} n_p \phi(P)$.

Recall that, via a pullback, $\phi^* : K(E_2) \hookrightarrow K(E_1)$.

If $f \in K(E_1)^*$, then $\phi_*(\operatorname{div} f) = \operatorname{div}(N_{K(E_1)/K(E_2)} f)$ - this is a fact that we'll take for granted.

So ϕ_* takes principal divisors to principal divisors. Since $\phi(O_{E_1}) = O_{E_2}$, the following diagram commutes:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\psi_1"] & E_2 \arrow[d, "\psi_2"] \\ \mathrm{Pic}^0(E_1) \arrow[r, "\phi_*"] & \mathrm{Pic}^0(E_2) \end{tikzcd}$$

,where $\psi_1 : P \mapsto [(P) - (O_{E_1})]$, $\psi_2 : Q \mapsto [(Q) - (O_{E_2})]$.

Since ϕ_* is a group homomorphism, ϕ is also a group homomorphism. □

Lemma 5.3. *Let $\phi : E_1 \to E_2$ be an isogeny. Then there is a morphism ξ making the following diagram commute:*

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x_1"] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

where x_i is the x-coordinate in a Weierstrass equation for E_i.

Moreover, if $\xi(t) = \frac{r(t)}{s(t)}$ for $r, s \in K[t]$ coprime, then $\deg \phi = \deg \xi = \max(\deg r, \deg s)$.

Proof. For $i = 1, 2$, $K(E_i)/K(x_i)$ is a degree 2 extension, since the extension is given by adjoining y_i, which satisfies a quadratic (see the Weierstrass equation). Moreover, it is Galois, as $[-1]^*$ is a non-trivial automorphism of $K(E_i)$ fixing $K(x_i)$.

Since ϕ is a group homomorphism, we have that $\phi(-P) = -\phi(P)$, i.e. $\phi \circ [-1] = [-1] \circ \phi$.

If $f \in K(x_2)$, then $[-1]^* f = f$, and $[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$. Hence $\phi^* f$ is fixed by $[-1]$, so is in $K(x_1)$, and $K(x_2) \leq K(x_1)$.

Taking $f = x_2$, then $\phi^* x_2 \in K(x_1)$, say $\xi(x_1)$ for some rational function ξ. Then ξ is as required.

Since $[K(E_1) : K(x_1)] = [K(E_2) : K(x_2)] = 2$, we have the following diagram of field extensions:

$$\begin{tikzcd}[column sep=small] & K(E_1) \arrow[dl, dash, "2"'] \arrow[dr, dash, "\deg \phi"] & \\ K(x_1) \arrow[dr, dash, "\deg \xi"'] & & K(x_2) \arrow[dl, dash, "2"] \\ & K(x_2) & \end{tikzcd}$$

Using the tower law, $\deg \phi = \deg \xi$. Now, $K(x_2) \hookrightarrow K(x_1)$ via $x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_2)}$ for $r, s \in K[t]$ coprime.

The minimal polynomial of x_1 over $K(x_2)$ is $f(t) = r(t) - s(t)x_2 \in K(x_2)[t]$ - this is clearly a polynomial for x_1, but we need to check it's irreducible.

f is irreducible in $K[t][x_2] = K[x_2][t]$ as it is of degree 1 in x_2, so one of the factors must be constant in x_2, so divide both r and s which are coprime. Then we can use Gauss's lemma, and it is irreducible in $K(x_2)[t]$.

Hence $\deg \phi = \deg \xi = [K(x_1) : K(x_2)] = \deg(r(t) - s(t)x_2) = \max(\deg r, \deg s)$. $\square$

Lemma 5.4. $\deg[2] = 4$

Proof. Assume $\operatorname{char} K \neq 2, 3$. Then $E : y^2 = x^3 + ax + b = f(x)$.

If $P = (x, y)$, then $x(2P) = \left(\frac{3x^2+a}{2y}\right)^2 - 2x = \frac{(3x^2+a)^2 - 8xf(x)}{4f(x)} = \frac{x^4+\ldots}{4f(x)}$.

The numerator and denominator are coprime - suppose there was a common factor. Then $\exists\ \theta \in \bar{K}$ with $f(\theta) = (3\theta^2 + a)^2 = f'(\theta) = 0$, and so f has a multiple root. But E is an elliptic curve so f doesn't have multiple roots.

Hence $\deg[2] = \max(\deg x^4 + \ldots, \deg 4f(x)) = \max(4, 3) = 4$. $\square$

Definition. Let A be an abelian group. We say that $q : A \to \mathbb{Z}$ is a ***quadratic form*** if it satisfies

1. $q(nx) = n^2 q(x)\ \forall n \in \mathbb{Z}, x \in A$.
2. $(x, y) \to q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.

Lemma 5.5. *$q : A \to \mathbb{Z}$ is a quadratic form if and only if it satisfies the parallelogram law:*

$$q(x + y) + q(x - y) = 2q(x) + 2q(y)\ \forall x, y \in A$$

Proof. For the forwards direction, let $\langle x, y\rangle = q(x + y) - q(x) - q(y)$.

Then $\langle x, x\rangle = q(2x) - 2q(x) = 2q(x)$.

Then $\frac{1}{2}\langle x+y, x+y\rangle + \frac{1}{2}\langle x-y, x-y\rangle = \langle x, x\rangle + \langle y, y\rangle$ by bilinearity, and hence $q(x+y)+q(x-y) = 2q(x) + 2q(y)$.

The reverse direction is left as an exercise on example sheet 2. $\square$

Theorem 5.6.

$$\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a quadratic form.

Proof. For the proof, we will assume $\operatorname{char} K \neq 2, 3$ for simplicity - the result still holds in those characteristics.

We write $E_2 : y^2 = x^3 + ax + b$.

Let $P, Q \in E_2$ with $P, Q, P + Q, P - Q \neq 0$, and let $x_1, \ldots, x_4$ be the x-coordinates of these 4 points. Then we have:

Lemma 5.7. *There exists $w_0, w_1, w_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree ≤ 2 in x_1 and in x_2 such that $(1 : x_3 + x_4 : x_3x_4) = (w_0 : w_1 : w_2)$.*

Proof. We could prove this by direct calculation, leading to the formulae:

$$\begin{aligned}
w_0 &= (x_1 - x_2)^2 \\
w_1 &= 2(x_1x_2 + a)(x_1 + x_2) + 4b \\
w_2 &= x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1 + x_2) + a^2
\end{aligned}$$

As an alternative proof, let $y = \lambda x + \nu$ be the line through P and Q. Then

$$x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3$$

where s_i is the i^{th} symmetric polynomial in (x_1, x_2, x_3).

Comparing coefficients:

$$\begin{aligned}
\lambda^2 &= s_1 \\
-2\lambda\nu + a &= s_2 \\
\nu^2 - b &= s_3
\end{aligned}$$

Eliminating λ, ν, we have $F(x_1, x_2, x_3) := (s_2 - a)^2 - 4s_1(s_3 + b) = 0$. Then F has degree at most 2 in each x_i.

x_3 is a root of the quadratic polynomial $W(t) = F(x_1, x_2, t)$, and repeating this for the line through P and $-Q$ shows that x_4 is the other root. Hence

$$w_0(t - x_3)(t - x_4) = W(t) = w_0t^2 - w_1t + w_2$$

And so $(1 : x_3 + x_4 : x_3x_4) = (w_0 : w_1 : w_2)$. □

We then show that, if $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$, then

$$\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg(\phi) + 2\deg(\psi)$$

We may assume $\phi, \psi, \phi + \psi, \phi - \psi ! = 0$, as otherwise the result is trivial.

$$\begin{aligned}
\phi &: (x, y) \mapsto (\xi_1(x), \dots) \\
\psi &: (x, y) \mapsto (\xi_2(x), \dots) \\
\phi + \psi &: (x, y) \mapsto (\xi_3(x), \dots) \\
\phi - \psi &: (x, y) \mapsto (\xi_4(x), \dots)
\end{aligned}$$

Then **5.7** gives $(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : \dots : \dots)$.

Put $\xi_i = \frac{r_i}{s_i}$ where $r_i, s_i \in K[x]$ are coprime:

$$(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_2)^2 : \dots : \dots) \tag{$*$}$$

So we have:

$$\begin{aligned}
\deg(\phi + \psi) + \deg(\phi - \psi) &= \max(\deg r_3, \deg s_3) + \max(\deg r_4, \deg s_4) \\
&= \max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4))
\end{aligned}$$

Suppose $(s_3s_4, r_3s_4 + r_4s_3, r_3r_4)$ are not coprime, so that p irreducible divides all 3. Then p divides one of r_3, r_4, and one of s_3, s_4. p can't divide both s_i and r_i as they are coprime, so WLOG p divides r_3 and s_4 and not r_4 nor s_3. Then p doesn't divide $r_3s_4 + r_4s_3 \lightning$. Hence these polynomials are coprime.

Hence the polynomials on RHS of $(*)$ must be multiples of polynomials on the LHS by some irreducible polynomial, and hence each have degree $\geq$ their corresponding polynomial on LHS, and thus, as w_i are of degree ≤ 2 in r_1, s_1, r_2, s_2,

$$\begin{aligned}\deg(\phi+\psi)+\deg(\phi-\psi) &\leq \max(\deg(w_0), \deg(w_1), \deg(w_2)) \\ &\leq 2\max(\deg r_1, \deg s_1) + 2\max(\deg r_2, \deg s_2) \\ &= 2\deg\phi + 2\deg\psi \end{aligned} \tag{1}$$

Now replace ϕ and ψ by $\phi+\psi$ and $\phi-\psi$ to get

$$\deg(2\phi)+\deg(2\psi) \leq 2\deg(\phi+\psi) + 2\deg(\phi-\psi)$$

Since $\deg[2] = 4$,

$$2\deg(\phi)+2\deg(\psi) \leq \deg(\phi+\psi)+\deg(\phi-\psi) \tag{2}$$

(1) and (2) together give

$$2\deg(\phi)+2\deg(\psi) = \deg(\phi+\psi)+\deg(\phi-\psi)$$

so deg satisfies the parallelogram law, and hence is a quadratic form. □

Corollary 5.8.

$$deg(n\phi) = n^2\deg(\phi)\ \forall n \in \mathbb{Z}, \phi \in \mathrm{Hom}(E_1, E_2)$$

In particular, $\deg[n] = n^2$.

Example 5.9. Let E/K be an elliptic curve, suppose $\operatorname{char} K \neq 2$, and let $O_E \neq T \in E(K)[2]$.

Then we may take $E : y^2 = x(x^2+ax+b), a, b \in K, b(a^2-4b) \neq 0, T = (0,0)$

Then if $P = (x, y)$ and $P' = P + T = (x', y')$, then:

$$\begin{aligned} x' &= (y/x)^2 - a - x = \frac{x^2+ax+b}{x} - x - a - = \frac{b}{x} \\ y' &= -(y/x)x' = \frac{-by}{x^2} \end{aligned}$$

Then let $\xi = x + x' + a = \frac{x^2+ax+b}{x} = \left(\frac{y}{x}\right)^2$, and $\eta = y + y' = \frac{y}{x}(x - \frac{b}{x})$

Then $\eta^2 = \left(\frac{y}{x}\right)^2\left[\left(x+\frac{b}{x}\right)^2 - 4b\right] = \xi\left((\xi-a)^2-4b\right) = \xi(\xi^2 - 2a\xi + a^2 - 4b)$

Let $E' : y^2 = x(x^2 + a'x + b')$ where $a' = -2a, b' = a^2 - 4b$. Then there is an isogeny $\phi : E \longrightarrow E'$ given by $(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2-b)}{x^2} : 1\right); O_E \mapsto (0:1:0)$

5.3 tells us, as $x' = \left(\frac{y}{x}\right)^2 = \frac{x^2+ax+b}{x}$, that $\deg(\phi) = \max(2,1) = 2$, and we say ϕ is a 2-isogeny.

6 The Invariant Differential

Let C be an algebraic curve over an algebraically closed field. Then the ***space of differentials*** Ω_C is a vector space over the function field of the curve $K(C)$, generated by df for $f \in K(C)$ subject to the relations

1. $d(f+g) = df + dg$
2. $d(fg) = fdg + gdf$
3. $da = 0$ for $a \in K$

It turns out that $\dim \Omega_C = \dim C$, and since C is a curve, Ω_C is a 1-dimensional $K(C)$-vector space.

Let $0 \neq \omega \in \Omega_C$, and let $P \in C$ be a smooth point, with $t \in K(C)$ a uniformizer at P (has order of vanishing 1 at P). Then $w = fdt$ for some $f \in K(C)$.

We define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$. This does not depend on the choice of uniformizer.

Suppose we have $f \in K(C)^*$, and $\mathrm{ord}_P(f) = n \neq 0$. Then, if $\mathrm{char}\, K \nmid n$, $\mathrm{ord}_P(df) = n-1$.

If C is now a smooth projective curve, we define the divisor of $\omega \in \Omega_C$ to be

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P \in \mathrm{Div}(C)$$

using the fact that $\mathrm{ord}_P(\omega)$ is zero at all but finitely many points $P \in C$.

The ***space of regular differentials*** is the finite dimensional vector space over K of all $\omega \in \Omega_C$ for which $\mathrm{div}(\omega)$ is effective, i.e. there are no poles. The dimension of this space is called the ***genus*** of C, $g(C)$.

As a consequence of Riemann-Roch, we have, for $0 \neq \omega \in \Omega_C$, $\deg(\mathrm{div}(\omega)) = 2g(C) - 2$.

Lemma 6.1. *Assume* $\mathrm{char}\, K \neq 2$. *Take an elliptic curve* $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$, *where* e_1, e_2, e_3 *distinct.*

Then $\omega = \frac{dx}{y}$ *is a differential on* E, *and has no zeros and no poles, and so* $g(E) = 1$.

Moreover, the space of regular differentials is just $\langle \omega \rangle$.

Proof. Let $T_i = (e_i, 0)$, so that $E[2] = \{O, T_1, T_2, T_3\}$.

Then $\mathrm{div}(y) = (T_1) + (T_2) + (T_2) - 3(O)$ - we know the zeros at T_i are simple as y is rational, so $\deg \mathrm{div}(y) = 0$.

Then for $P \in E$, $\mathrm{div}(x - x_P) = (P) + (-P) - 2(O)$, in the same way as above.

If $P \in E \setminus E[2]$, then $\mathrm{ord}_P(x - x_P) = 1$, so $\mathrm{ord}_P(d(x - x_P)) = \mathrm{ord}_P(dx) = 1 - 1 = 0$.

If $P = T_i$, then $P = -P$, and $\mathrm{ord}_P(x - x_p) = 2$, so $\mathrm{ord}_P(dx) = 2 - 1 = 1$

If $P = O$, then $\mathrm{ord}_P(x) = -2$, so $\mathrm{ord}_P(dx) = -3$.

Hence $\mathrm{div}(dx) = (T_1) + (T_2) + (T_3) - 3(O) = \mathrm{div}(y)$.

So $\mathrm{div}(dx/y) = \mathrm{div}(dx) - \mathrm{div}(y) = 0$. Then Riemann-Roch gives $g(E) = 1$, and so the space of regular differentials is 1-dimensional, so generated by ω. $\square$

Definition. If $\phi : C_1 \to C_2$ is a non-constant morphism, then we can pull back to

$$\phi^* : \Omega_{C_1} \to \Omega_{C_2}; f dg \mapsto \phi^* f d(\phi^* g)$$

Lemma 6.2. *Let $P \in E$, $\tau_P : E \to E; X \mapsto P + X$, and $\omega = dx/y$ be as above.*

Then $\tau_P^* \omega = \omega$, and so ω is called the **invariant differential**.

Proof. Since ω had no poles, $\tau_P^* \omega$ is again a regular differential, and hence equal to $\lambda_P \omega$ for some $\lambda_P \in K$, as the regular differentials are a 1-dimensional vector space over K.

The map $E \to \mathbb{P}^1; P \mapsto \lambda_P$ is a morphism of smooth projective curves, but is not surjective as it misses 0 and ∞, and so this morphism is constant, by **2.8**.

So λ is independent of P. Take $P = O_E$, then τ_P is the identity map, and so λ is 1. □

If $K = \mathbb{C}$, then $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, via $z \mapsto (\wp(z), \wp'(z))$. Then $\frac{dx}{y} = \frac{\wp'(z)dz}{\wp'(z)} = dz$, which is invariant under $z \mapsto z +$ const..

Lemma 6.3. *Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, ω the invariant differential on E_2. Then*

$$(\phi + \psi)^*(\omega) = \phi^* \omega + \psi^* \omega$$

Proof. Write $E = E_2$, and consider the maps:

$$\begin{aligned} E \times E &\to E \\ \mu : (P, Q) &\mapsto P + Q \\ \mathrm{pr}_1 : (P, Q) &\mapsto P \\ \mathrm{pr}_2 : (P, Q) &\mapsto Q \end{aligned}$$

$\Omega_{E\times E}$ is a 2-dimensional $K(E \times E)$ vector space with basis $\mathrm{pr}_1^* \omega$ and $\mathrm{pr}_2^* \omega$.

Then $\mu^* \omega = f \mathrm{pr}_1^* \omega + g \mathrm{pr}_2^* \omega$ for some $f, g \in K(E \times E)$.

For $Q \in E$, let $\iota_Q : E \to E \times E; P \mapsto (P, Q)$. Then

$$\begin{aligned} \iota_Q^*(\mu^* \omega) = (\mu \circ \iota_Q)^* \omega &= \iota_Q^* f (\mathrm{pr}_1 \circ \iota_Q)^* \omega + \iota_Q^* g (\mathrm{pr}_2 \circ \iota_Q)^* \omega \\ \tau_Q^* \omega &= \iota_Q^* f \omega + 0 \\ \omega &= \iota_Q^* f \omega \end{aligned}$$

So $\iota_Q^* f = 1$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$.

Similarly, $g(P, Q) = 1$.

So $\mu^* \omega = \mathrm{pr}_1^* \omega + \mathrm{pr}_2^* \omega$. Now pull back by $E \to E \times E; P \mapsto (\phi(P), \psi(P))$ to get $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$. □

Lemma 6.4. *If $\phi : C_1 \to C_2$ is a non-constant morphism, then ϕ is separable if and only if $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is nonzero*

Proof. Omitted. □

Example: Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty$, with group law $\mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m; (x, y) \mapsto xy$.

Let $n \geq 2$ be an integer, $\alpha : \mathbb{G}_m \to \mathbb{G}_m; x \mapsto x^n$.

Then $\alpha^*(dx) = d(\alpha x) = d(x^n) = nx^{n-1}dx$. So if $\operatorname{char} K \nmid n$, then α is separable. So $\#\alpha^{-1}(Q) = \deg \alpha$ for all but finitely many $Q \in \mathbb{G}_m$.

But α is group homomorphism, so all fibres have the same size, and $\#\alpha^{-1}(Q) = \# \ker \alpha$, hence $\# \ker \alpha = \deg \alpha = n$. So $K (= \bar{K})$ contains exactly n n^{th} roots of unity.

Theorem 6.5. *If* $\operatorname{char} K \nmid n$, *then* $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Proof. By **6.3** and induction, $[n]^*\omega = n\omega$. So if $\operatorname{char} K \nmid n$, $[n]$ is separable. So all but finitely many fibres of $[n]$ have size $\deg[n]$, and since $[n]$ is a group homomorphism, all fibres have the same size, and hence $\#[n]^{-1}(O_E) = \#E[n] = \deg[n] = n^2$.

By the structure theorem for finite abelian groups, $E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_t\mathbb{Z}$ with $d_i | d_{i+1}$. Since this group is killed by multiplication by n, all $d_i | n$ as well, and $\prod_{i=1}^t d_i = n^2$ by the previous paragraph.

If p is a prime with $p | d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$, and by the first paragraph, $t = 2$. Then $d_1 | d_2 | n$, and $d_1 d_2 = n^2$, hence $d_1 = d_2 = n$. □

Remark (not to be used on example sheet 2). If $\operatorname{char} K = p$, then $[p]$ is not separable. It can be shown that $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$ or $E[p] = 0$. The first case is described as "ordinary", and the second case is "supersingular".

7 Elliptic Curves over Finite Fields

Lemma 7.1. *Let A be an abelian group and $q : A \to \mathbb{Z}$ a positive definite quadratic form. If $x, y \in A$ then $\langle x, y \rangle := |q(x + y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}$.*

Proof. We may assume $x \neq 0$ otherwise the result is clear. Let $m, n \in \mathbb{Z}$.

$$\begin{aligned} 0 &\leq q(mx + ny) \\ &= \frac{1}{2}\langle mx + ny, mx + ny \rangle \\ &= m^2 q(x) + mn\langle x, y \rangle + n^2 q(y) \\ &= q(x)\left(m + \frac{\langle x, y \rangle}{2q(x)} n\right)^2 + n^2\left(q(y) - \frac{\langle x, y \rangle^2}{4q(x)}\right) \end{aligned}$$

Take $m = \langle x, y \rangle, n = -2q(x)$, we deduce $\langle x, y \rangle^2 \leq 4q(x)q(y)$, so $|anglex, y| \leq 2\sqrt{q(x)q(y)}$. □

Recall that $\operatorname{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r generated by the Frobenius map $x \mapsto x^q$.

Theorem 7.2 (Hasse). *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$*

Proof. Let E have Weierstrass equation with coefficients $a_1, \ldots, a_6 \in \mathbb{F}_q$. Define the Frobenius endomorphism $\phi : E \to E; (x, y) \mapsto (x^q, y^q)$, which is an isogeny of degree q.

Then $E(\mathbb{F}_q) = \{P \in E : \phi(P) = P\} = \ker(1 - \phi)$.

$\phi^*\omega = \phi^*\left(\frac{dx}{y}\right) = \frac{dx^q}{y^q} = \frac{qx^{q-1}dx}{y^q} = 0$, since $q \equiv 0 \mod p$.

So $(1-\phi)^*\omega = 1^*\omega - \phi^*\omega = \omega - 0 = \omega \neq 0$, so $1-\phi$ is separable.

Hence the size of all but finitely many fibres is $\deg 1-\phi$, and $1-\phi$ is a group homomorphism, so $\#E[\mathbb{F}_q] = \#\ker(1-\phi) = \deg(1-\phi)$.

By **5.6**, $\deg : \mathrm{End}(E) := \mathrm{Hom}(E,E) \to \mathbb{Z}$ is a positive definite quadratic form.

By **7.1**, $|\deg(1-\phi) - 1 - \deg\phi| \leq 2\sqrt{\deg\phi}$, and hence $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$. □

7.1 Zeta Functions

For K a number field:

$$\zeta_K(s) = \sum_{\mathfrak{a}\subset O_K} \frac{1}{(N_\mathfrak{a})^s} = \prod_{\mathfrak{p}\subset O_K \text{ prime}} \left(1 - \frac{1}{(N_\mathfrak{p})^s}\right)^{-1}$$

For K a function field, e.g. $K = \mathbb{F}_q(C)$ for $C/\mathbb{F}_q$ a smooth projective curve:

$$\zeta_K(s) = \prod_{x\in|C|} \left(1 - \frac{1}{(Nx)^s}\right)^{-1}$$

where $|C|$ is the set of closed points (i.e. orbit of action of $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$) on $C(\bar{\mathbb{F}}_q)$, and $Nx = q^{\deg x}$, where $\deg x$ is the size of the orbit.

We have that $\zeta_K(s) = F(q^{-s})$ for $F \in Q[[T]]$, where

$$\begin{aligned}
F(T) &= \prod_{x\in|C|} (1 - T^{\deg x})^{-1} \\
\log F(T) &= \sum_{x\in|C|} \sum_{m=1}^{\infty} \frac{1}{m} T^{m \deg x} \\
\frac{d}{dT} \log F(T) &= \sum_{x\in|C|} \sum_{m=1}^{\infty} \deg x T^{m\deg x} \\
&= \sum_{n=1}^{\infty} \left(\sum_{\substack{x\in|C| \\ \deg x | n}} \deg x \right) T^n \\
&= \sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) T^n \\
\implies F(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n \right) =: Z_C(T)
\end{aligned}$$

We define the ***trace map*** $\mathrm{tr} : \mathrm{End}(E) \to \mathbb{Z}; \psi \mapsto \langle \psi, 1 \rangle$.

Lemma 7.3. *If $\psi \in \mathrm{End}(E)$ then $\psi^2 - [\mathrm{tr}\,\psi]\psi + [\deg\psi] = 0$, where $[n]$ means the multiplication by n endomorphism.*

Proof. Example sheet 2. □

Definition. The ***zeta function of a variety*** $V/\mathbb{F}_q$ is

$$Z_v(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#V(\mathbb{F}_{q^n})}{n} T^n\right)$$

Lemma 7.4. *Let $E/\mathbb{F}_q$ be an elliptic curve, with $E(\mathbb{F}_q) = q + 1 - a$. Then*

$$Z_E(T) = \frac{1 + aT + qT^2}{(1-T)(1-qT)}$$

Proof. Let $\phi : E \to E$ be the q-power Frobenius map. By the proof of Hasse's theorem,

$$\#E(\mathbb{F}_q) = \deg(1-\phi) = q + 1 - \mathrm{tr}(\phi)$$

Then $\mathrm{tr}(\phi) = a, \deg(\phi) = q$.

Then lemma **7.3** gives $\phi^2 - a\phi + q = 0$. Composing with ϕ^n for $n \geq 0$ gives

$$\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$$
$$\mathrm{tr}(\phi^{n+2}) - a\,\mathrm{tr}(\phi^{n+1}) + q\,\mathrm{tr}(\phi^n) = 0$$

This second-order difference equation with initial conditions $\mathrm{tr}(\phi^0) = \mathrm{tr}(1) = 2, \mathrm{tr}(\phi^1) = a$ has solutions

$$\mathrm{tr}(\phi^n) = \alpha^n + \beta^n$$

where α, β are the roots of $x^2 - ax + q = 0$.

Hence $\#E(\mathbb{F}_{q^n}) = \deg(1-\phi^n) = 1 + \deg(\phi^n) - \mathrm{tr}(\phi^n) = 1 + q^n - \alpha^n - \beta^n$.

Substituting, we have:

$$Z_E(T) = \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n}\right)$$

Since $-\log(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}$, this can be simplified to:

$$\begin{aligned} Z_E(T) &= \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} \\ &= \frac{1 - aT + qT^2}{(1-T)(1-qT)} \end{aligned}$$

□

Note that Hasse's theorem gives us $|a| \leq 2\sqrt{q}$, and so the discriminant of $x^2 - aT + q$ is negative, and so $\alpha = \bar{\beta}, |\alpha| = |\beta| = \sqrt{q}$.

Let $K = \mathbb{F}_q(E)$. Then $\zeta_K(s) = 0 \implies Z_E(q^{-s}) = 0 \implies q^2 = \alpha$ or β, and hence $\mathfrak{Re}(s) = \frac{1}{2}$.

8 Formal Groups

Here, R will be a ring with $I \subset R$ an ideal. The ***I-adic topology*** on R is the topology with basis $\{r + I^n : r \in R, n \geq 1\}$.

A sequence (x_n) in R is ***Cauchy*** if, for all k there is some N with $x_m - x_n \in I^k$ for all $m, n \geq k$.

R is ***complete*** if

1. $\bigcap_{n \geq 0} I^n = \{0\}$ and
2. every Cauchy sequence converges.

Note that, if $x \in I$ then $\frac{1}{1-x} = 1 + x + x^2 + \ldots$, and the sequence of partial sums is Cauchy, and hence converges. So $1 - x \in R^\times$.

For example, we could have:

- $R = \mathbb{Z}_p, I = p\mathbb{Z}_p$
- $R = \mathbb{Z}[[t]], I = (t)$.

Lemma 8.1 (Hensel's Lemma). *Let R be an integral domain, complete with respect to I. Let $F \in R[x], s \geq 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \mod I^s$, and $F'(a) \in R^\times$.*

Then there is a unique $b \in R$ with $F(b) = 0$ and $b \equiv a \mod I^s$.

Proof. Let $u \in R^\times$ with $F'(a) \equiv u \mod I$, e.g. $u = f'(a)$.

Replacing $F(x)$ by $\frac{F(x+a)}{u}$, we may assume $a = 0$ and $F'(0) \equiv 1 \mod I$.

We put $x_0 = 0, x_{n+1} = x_n - F(x_n)$.

By induction, $x_n \in I_s$ for all n.

$F(x) - F(y) = (x - y)(F'(0) + xG(x, y) + yH(x, y))$ for some polynomials $G, H \in R[x, y]$.

Now we claim $x_{n+1} \equiv x_n \mod I^{n+s}$ for all $n \geq 0$.

This can be proven by induction on n: in the case where $n = 0$, and $x_1 \in I^s$.

Suppose $x_n \equiv x_{n-1} \mod I^{n+s-1}$. Then

$$F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1 + c)$$

for some $c \in I$, and hence

$$F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \mod I^{n+s}$$

Rearranging, we have $x_{n+1} \equiv x_n \mod I^{n+s}$, which proves the claim.

Hence (x_n) is Cauchy, and by completeness converges to some $b \in R$. Taking the limit as $n \to \infty$, we have $b = b - F(b)$, and so $F(b) = 0$, with $b \in I^s$.

For uniqueness, we can use the expression for $F(x) - F(y)$ and the assumption that R is an integral domain. ◻

For example, take $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$

We pass to the affine piece $Y \neq 0, t = X/Y, w = -Z/Y$: Then

$$E : w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 = f(t, w)$$

We can apply Hensel's lemma with $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, $I = (t)$, and $F(x) = x - f(t, x) \in R[x]$. Taking $s = 3, a = 0$, we have:

$$F(0) = -f(t, 0) = -t^3 \equiv 0 \mod I^3 \qquad F'(0) = 1 - a_t - a_2t^2 \in R^\times$$

So there is a unique root of F, $w(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ such that $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \mod t^3$.

Following the proof of Hensel's lemma with $u = 1$ gives $w(t) = \lim_{n\to\infty} w_n(t)$ where $w_0(t) = 0, w_{n+1}(t) = f(t, w_n(t))$.

In fact, we may write $w(t) = \sum_{n=2}^{\infty} A_{n-2}t^{n-1}$ with $A_1 = a_1, A_2 = a_1^2 + a_2, A_3 = a_1^3 + 2a_1a_2 + a_3, \dots$

Lemma 8.2. *Let R be an integral domain, complete with respect to $I \trianglelefteq R$, and let $a_1, \dots, a_6 \in R, K =$ Frac(R).*

Then $\widehat{E}(I) = \{(t, w) \in E(K) : t, w \in I\} = \{(t, w(t)) \in E(K) : t \in I\}$ is a subgroup of $E(K)$.

Proof. The two descriptions of $\widehat{E}(I)$ agree, since given $t \in I$ we can solve for a unique $w \in I$ such that the pair $(t, w) \in E(K)$.

Taking $(t, w) = (0, 0)$ shows that $O_E \in \widehat{E}(I)$. So it suffices to show that, if $P_1, P_2 \in \widehat{E}(I)$, then $-P_1 - P_2 \in \widehat{E}(I)$.

If $P_1 = (t_1, w_1), P_2 = (t_2, w_2)$ lie on the straight line $\lambda t + \nu$, then $-P_1 - P_2$ is the third point of intersection of this line with E.

Then $\lambda = \frac{w(t_2)-w(t_1)}{t_2-t_1}$ if $t_1 \neq t_2$, and $w'(t_1)$ if $t_1 = t_2$.

$P_1, P_2 \in \widehat{E}(I) \implies t_1, t_2 \in I$.

Thus $\lambda = \sum_{n=2}^{\infty} A_{n-2}(t_1^n + t_1^{n-1}t_2 + \dots + t_2^n) \in I$, and $\nu = w_1 - \lambda t_1 \in I$.

Substituting $w = \lambda t + \nu$ into $w = f(t, w)$ gives $\lambda t + \nu = t^3 + a_1t(\lambda t + \nu) + a_2t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4t(\lambda t + \nu)^3 + a_6(\lambda t + \nu)^3$.

Let A be the coefficient of t^3, so $A = 1 + a_2 + a_4\lambda^2 + a_6\lambda^3$.

Let B be the coefficient of t^2, so $B = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu$.

Then $A \in R^\times, B \in I$, and $t_3 = -B/A - t_2 - t_2 \in I$, and $w_3 = \lambda t_3 + \nu \in I$.

Hence $-P_1 - P_2 \in \widehat{E}(I)$, and so $\widehat{E}(I)$ is a subgroup. □

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, and $I = (t)$, then the previous lemma tells us there is some power series $\iota \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $\iota(0) = 0$ such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, and $I = (t_1, t_2)$, then we get that there is some power series $F \in I$ such that $(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))$.

In fact, we can compute

$$\iota(x) = -x - a_1x^2 - a_2x^3 - (a_1^3 + a_3)x^4 + \dots$$
$$F(x,y) = x + y - a_1xy - a_2(x^2y + xy^2) + \dots$$

By properties of the group law, we can deduce:

1. $F(x,y) = F(y,x)$
2. $F(x,0) = x, F(0,y) = y$
3. $F(x, F(y,z)) = F(F(x,y),z)$
4. $F(x, \iota(x)) = 0$

This then motivates the following definition:

Definition. Let R be a ring. A ***formal group*** over R is a power series $F(x,y) \in R[[x,y]]$ satisfying the properties 1, 2, and 3 above.

Exercise. Show that, for any formal group, there is a unique $\iota(x) \in R[[x]]$ such that $F(x,\iota(x)) = 0$.

Examples:

1. $F(x,y) = x + y$
2. $F(x,y) = x + y + xy = (1+x)(1+y) - 1$
3. F as above.

We label these formal groups by $\widehat{\mathbb{G}}_a$, $\widehat{\mathbb{G}}_m$, and $\widehat{E}$ respectively.

Definition. Let $\mathcal{F}$, $\mathcal{G}$ be formal groups over R given by power series F, G respectively. Then:

1. A ***morphism*** $f : \mathcal{F} \to \mathcal{G}$ is a power series $f \in R[[t]]$ such that $f(0) = 0$ satisfying $f(F(x,y)) = G(f(x), f(y))$.
2. $\mathcal{F} \cong \mathcal{G}$ if there is some morphism $f : \mathcal{F} \to \mathcal{G}$, and $g : \mathcal{G} \to \mathcal{F}$ with $f(g(x)) = g(f(x)) = x$.

Theorem 8.3. *If* $\mathrm{char}(R) = 0$, *then any formal group* $\mathcal{F}$ *over* R *is isomorphic to* $\widehat{\mathbb{G}}_a$ *over* $R \otimes \mathbb{Q}$.

More precisely:

1. *There is a unique power series* $\log : T \mapsto T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$ *with* $a_i \in R$, *such that*
$$\log(F(x,y)) = \log(x) + \log(y) \tag{$*$}$$
2. *There is a unique power series* $\exp : T \mapsto T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$ *with* $b_i \in R$ *such that*
$$\exp(\log(T)) = \log(\exp(T)) = T$$

Proof.

1. Notation: $F_1(x,y) = \frac{\partial F}{\partial x}(x,y)$ (via formal differentiation).

   For uniqueness, let $p(T) = \frac{d}{dT}\log(T) = 1 + a_2T + a_3T^2 + \dots$.

Differentiating $(*)$ with respect to x, we get: $p(F(x,y))F_1(x,y) = p(x) + 0$ Setting $x = 0$, we get $p(y)F_1(0,y) = 1$, and hence $p(y) = F_1(0,y)^{-1}$, and hence p is uniquely determined, so $a_2, a_3, \ldots$ are uniquely determined. But then log is uniquely determined.

For existence, let $p(T) = F_1(0,T)^{-1} = 1 + a_2 T + a_3 T^2 + \ldots$, where $a_i \in R$.

Integrating up, we let $\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \ldots$. We now check it satisfied $(*)$.

$$\begin{aligned}
F(F(x,y),z) &= F(x,F(y,z)) \\
\frac{\partial}{\partial x}F(F(x,y),z) &= \frac{\partial}{\partial x}F(x,F(y,z)) \\
F_1(F(x,y),z)F_1(x,y) &= F_1(x,F(y,z)) \\
F_1(F(0,y),z)F_1(0,y) &= F_1(0,F(y,z)) \\
F_1(y,z)F_1(0,y) &= F_1(0,F(y,z)) \\
F_1(y,z)p(y)^{-1} &= p(F(y,z))^{-1} \\
F_1(y,z)p(F(y,z)) &= p(y) \\
\log(F(y,z)) &= \log(y) + h(z)
\end{aligned}$$

By symmetry between y, z we see that the constant of integration $h(z)$ must be $\log(z)$.

□