PROJECTIVE GEOMETRY

Saroj Kumar
20231224

supervised by
Dr. Steven Spallone

Summer 2025

Contents

CHAPTER 1
Conics

1.1 Group Laws on Conics

Consider a conic section $\mathcal{C}$ and a point $O \in \mathcal{C}$. For any points $P, Q \in \mathcal{C}$, let ℓ' be the line passing through O such that $\ell' \parallel \ell$ where ℓ is the line joining P and Q. If ℓ' intersects $\mathcal{C}$ at a point other than O, call that point R. Otherwise, take $R = O$. Define a binary operation $\oplus : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ as $P \oplus Q := R$.

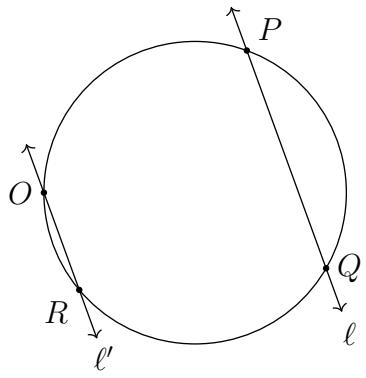

Figure 1.1 : $P \oplus Q$ when $\mathcal{C}$ is a circle.

We'll first find formulae to calculate $P \oplus Q$ and then proceed to prove that $\mathcal{C}$ is a group with $\oplus$.

Ellipse

If $\mathcal{C}$ is an ellipse, consider a coordinate system centred at the centre of the ellipse with its major and minor axes as x and y axes respectively as shown in the figure on the right. Its equation will be $a^{-2}x^2 + b^{-2}y^2 = 1$ in this coordinate system where $a, b \in \mathbb{R}^+$. Any point $P \in \mathcal{C}$ has coordinates $(a\cos\theta, b\sin\theta)$ where $\theta \in [0, 2\pi)$ is the angle P forms with the positive x-axis in the counter-clockwise direction.

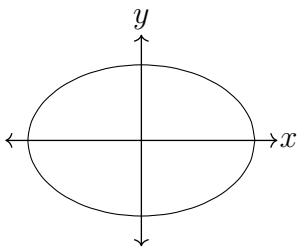

Figure 1.2

Consider points $P, Q, R \in \mathcal{C}$ such that $P \oplus Q = R$ and they form angles θ_1, θ_2 and θ_3 w.r.t. x-axis respectively. Also, let θ_0 be the angle formed by O w.r.t. positive x-axis.

Since $P \oplus Q = R$, we have $OR \parallel PQ$ and hence slope of OR and PQ will be the same. Using their coordinates, this can be written as,

$$\frac{b\sin\theta_3 - b\sin\theta_0}{a\cos\theta_3 - a\cos\theta_0} = \frac{b\sin\theta_2 - b\sin\theta_1}{a\cos\theta_2 - a\cos\theta_1}$$

We can cancel out b/a on both sides. After cross-multiplying and grouping the terms with the same pair of angles, we get

$$\sin(\theta_3 - \theta_2) + \sin(\theta_1 - \theta_3) = \sin(\theta_0 - \theta_2) + \sin(\theta_1 - \theta_0)$$

Using the trigonometric identity $\sin x + \sin y = 2\sin\frac{x+y}{2}\cos\frac{x-y}{2}$, this further simplifies

$$2\sin\left(\frac{\theta_1 - \theta_2}{2}\right)\cos\left(\frac{\theta_1 + \theta_2 - 2\theta_3}{2}\right) = 2\sin\left(\frac{\theta_1 - \theta_2}{2}\right)\cos\left(\frac{\theta_1 + \theta_2 - 2\theta_0}{2}\right)$$

If $P \neq Q$, then $\theta_1 \neq \theta_2$. So, sin won't be zero and hence, we can cancel the 2 and sin, leaving the following relation between the arguments of cos,

$$\frac{\theta_1 + \theta_2}{2} - \theta_3 = 2n\pi \pm \frac{\theta_1 + \theta_2 - 2\theta_0}{2}$$

As shifts of $2n\pi$ don't affect θ_3, we can ignore that term on the RHS. The positive case results in $\theta_3 = \theta_0$ but this just indicates the point O which we know already lies on ℓ' and $\mathcal{C}$. The negative case gives $\theta_3 = \theta_1 + \theta_2 - \theta_0$.

If $P = Q$, then $\theta_1 = \theta_2$. In this case, the slope of line PQ will be the slope of the tangent at P. Equating slope of tangent at P with slope of OR,

$$-\frac{b}{a}\cot\theta_1 = \frac{b\sin\theta_3 - b\sin\theta_0}{a\cos\theta_3 - a\cos\theta_0}$$

Again cancelling out b/a from both sides, cross multiplying and grouping terms with same pairs of angles, we obtain,

$$\cos\theta_1\cos\theta_0 + \sin\theta_1\sin\theta_0 = \cos\theta_1\cos\theta_3 + \sin\theta_1\sin\theta_3$$

The LHS and RHS are just $\cos(\theta_0 - \theta_1)$ and $\cos(\theta_3 - \theta_1)$ respectively. Thus we obtain the following relation for the arguments,

$$\theta_3 - \theta_1 = 2n\pi \pm (\theta_0 - \theta_1)$$

Again, we can ignore shifts by $2n\pi$. The positive case results in $\theta_3 = \theta_0$ which just indicates point O lying on ℓ'. The negative case gives $\theta_3 = 2\theta_1 - \theta_0$ which matches the formula we obtained for $P \neq Q$ case when $\theta_1 = \theta_2$.

Thus for any $P, Q \in \mathcal{C}$ with parameters θ_1 and θ_2 respectively for an ellipse $\mathcal{C}$, $P \oplus Q = R$ has parameter $\theta_3 = \theta_1 + \theta_2 - \theta_0$ where t_0 is the parameter for point O. Note that we always add or subtract multiples of 2π to make sure $\theta_3 \in [0, 2\pi)$.

It is easy to see that $\oplus$ satisfies closure for $\mathcal{C}$. We'll verfiy each of the group axioms now.

1. **Identity:** For any $P \in \mathcal{C}$ with parameter θ, $P \oplus O$ will have parameter $\theta' = \theta + \theta_0 - \theta_0 = \theta$. Thus O acts as the identity element for $\oplus$.

2. **Inverse:** The point Q with parameter $2\theta_0 - \theta$ gives the parameter of $P \oplus Q$ to be $\theta' = \theta + 2\theta_0 - \theta - \theta_0 = \theta_0$. Hence, Q is the inverse of P.

3. **Associativity:** For any $P, Q, R \in \mathcal{C}$ with parameters θ_1, θ_2 and θ_3 respectively, $P \oplus (Q \oplus R)$ has parameter $\theta_1 + (\theta_2 + \theta_3 - \theta_0) - \theta_0$ or $\theta_1 + \theta_2 + \theta_3 - 2\theta_0$. On the other hand, $(P \oplus Q) \oplus R$ has parameter $(\theta_1 + \theta_2 - \theta_0) + \theta_3 - \theta_0$ or $\theta_1 + \theta_2 + \theta_3 - 2\theta_0$. Thus $\oplus$ is associative.

This shows that $\mathcal{C}$ is a group with $\oplus$ for the case where $\mathcal{C}$ is an ellipse.

Theorem 1. *If $\mathcal{C}$ is an ellipse, $\langle \mathcal{C}, \oplus \rangle \cong \langle S^1, \cdot \rangle$ where $S^1 = \{e^{i\theta} \in \mathbb{C} : \theta \in [0, 2\pi)\}$.*

Proof. Consider $\varphi : \mathcal{C} \to S^1$ given by $\varphi((a\cos\theta, b\sin\theta)) = e^{i(\theta - \theta_0)}$. For any points $P, Q \in \mathcal{C}$ parametrized by θ_1 and θ_2 respectively, $P \oplus Q$ has parameter $\theta_1 + \theta_2 - \theta_0$. So,

$$\varphi(P \oplus Q) = e^{i(\theta_1 + \theta_2 - 2\theta_0)} = e^{i(\theta_1 - \theta_0)} e^{i(\theta_2 - \theta_0)} = \varphi(P)\varphi(Q)$$

Thus φ is a homomorphism.

If $\varphi(P) = \varphi(Q)$ for some $P, Q \in \mathcal{C}$ parametrized by θ_1 and θ_2 respectively, then

$$e^{i(\theta_1 - \theta_0)} = e^{i(\theta_2 - \theta_0)} \implies e^{i\theta_1} e^{i\theta_0} = e^{i\theta_2} e^{i\theta_0} \implies e^{i\theta_1} = e^{i\theta_2} \implies \theta_1 = 2n\pi + \theta_2$$

i.e. $P = Q$. Thus φ is injective.

For any $e^{i\theta} \in S^1$, we have the point $P = (a\cos(\theta + \theta_0), b\sin(\theta + \theta_0)) \in \mathcal{C}$ such that

$$\varphi(P) = e^{i(\theta + \theta_0 - \theta_0)} = e^{i\theta}$$

Thus φ is surjective. This shows that φ is a bijective homomorphism i.e. an isomorphism from $\langle \mathcal{C}, \oplus \rangle$ to $\langle S^1, \cdot \rangle$. ■

Parabola

If $\mathcal{C}$ is a parabola, consider a coordinate system with vertex of $\mathcal{C}$ as origin, x-axis as tangent at vertex and y-axis perpendicular to it as shown in the figure on the right. The equation of $\mathcal{C}$ in this coordinate system will be $x^2 = 4ay$ where $a \in \mathbb{R}^+$. Any point on it can be parametrized as $(2at, at^2)$ where $t \in \mathbb{R}$.

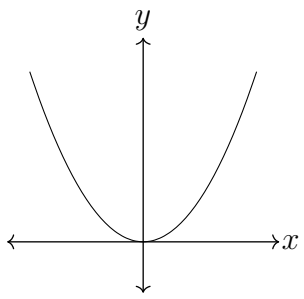

Figure 1.3

Let O, P, Q and R be points with parameters t_0, t_1, t_2 and t_3 respectively such that $P \oplus Q = R$. By definition of $P \oplus Q$, we have $PQ \parallel OR$. Note that if $P = Q$, then slope at P is

$$y'|_{x=2at_1} = \left(\frac{x}{2a}\right)_{x=2at_1} = t_1 = \frac{t_1 + t_2}{2}$$

and if $P \neq Q$, then $t_1 \neq t_2$ and slope of PQ is

$$\frac{at_2^2 - at_1^2}{2at_2 - 2at_1} = \frac{t_1 + t_2}{2}$$

So, we don't need to consider points being same as a separate case. Equating slopes of PQ and OR, we get,

$$\frac{t_1 + t_2}{2} = \frac{t_0 + t_3}{2} \implies t_3 = t_1 + t_2 - t_0$$

Thus, for any points $P, Q \in \mathcal{C}$ with parameters t_1 and t_2 respectively for a parabola $\mathcal{C}$, $P \oplus Q = R$ has parameter $t_3 = t_1 + t_2 - t_0$ where t_0 is the parameter for point O.

It is easy to see that $\oplus$ satisfies closure for $\mathcal{C}$. We'll verfiy each of the group axioms now.

1. **Identity:** For any $P \in \mathcal{C}$ with parameter t, $P \oplus O$ will have parameter $t' = t + t_0 - t_0 = t$. Thus O acts as the identity element for $\oplus$.

2. **Inverse:** The point Q with parameter $2t_0 - t$ gives the parameter of $P \oplus Q$ to be $t' = t + 2t_0 - t - t_0 = t_0$. Hence, Q is the inverse of P.

3. **Associativity:** For any $P, Q, R \in \mathcal{C}$ with parameters t_1, t_2 and t_3 respectively, $P \oplus (Q \oplus R)$ has parameter $t_1 + (t_2 + t_3 - t_0) - t_0$ or $t_1 + t_2 + t_3 - 2t_0$. On the other hand, $(P \oplus Q) \oplus R$ has parameter $(t_1 + t_2 - t_0) + t_3 - t_0$ or $t_1 + t_2 + t_3 - 2t_0$. Thus $\oplus$ is associative.

This shows that $\mathcal{C}$ is a group with $\oplus$ for the case where $\mathcal{C}$ is an parabola.

Theorem 2. *If $\mathcal{C}$ is a parabola, $\langle \mathcal{C}, \oplus \rangle \cong \langle \mathbb{R}, + \rangle$.*

Proof. Consider $\varphi : \mathcal{C} \to \mathbb{R}$ given by $\varphi((2at, at^2)) = t - t_0$. For any points $P, Q \in \mathcal{C}$ parametrized by t_1 and t_2 respectively, $P \oplus Q$ has parameter $t_1 + t_2 - t_0$. So,

$$\varphi(P \oplus Q) = t_1 + t_2 - 2t_0 = (t_1 - t_0) + (t_2 - t_0) = \varphi(P) + \varphi(Q)$$

Thus φ is a homomorphism.

If $\varphi(P) = \varphi(Q)$ for some $P, Q \in \mathcal{C}$ parametrized by t_1 and t_2 respectively, then

$$t_1 - t_0 = t_2 - t_0 \implies t_1 = t_2$$

i.e. $P = Q$. Thus φ is injective.

For any $t \in \mathbb{R}$, we have the point $P = (2a(t + t_0), a(t + t_0)^2) \in \mathcal{C}$ such that

$$\varphi(P) = t + t_0 - t_0 = t$$

Thus φ is surjective. This shows that φ is a bijective homomorphism i.e. an isomorphism from $\langle \mathcal{C}, \oplus \rangle$ to $\langle \mathbb{R}, + \rangle$. ∎

Hyperbola

If $\mathcal{C}$ is a rectangular hyperbola, consider a coordinate system with centre of $\mathcal{C}$ as origin and the asymptotes as x and y axes as shown in the figure on the right. The equation of $\mathcal{C}$ in this coordinate system will be $xy = c^2$ where $c \in \mathbb{R}^+$. Any point on it can be parametrized as (ct, ct^{-1}) where $t \in \mathbb{R}^\times$.

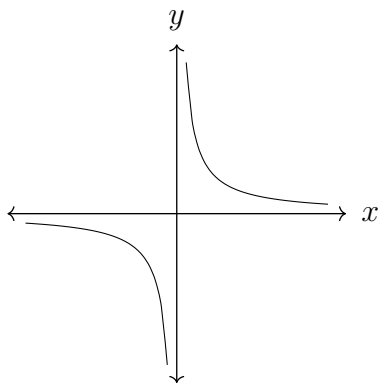

Figure 1.4

Let O, P, Q and R be points with parameters t_0, t_1, t_2 and t_3 respectively such that $P \oplus Q = R$. By definition of $P \oplus Q$, we have $PQ \parallel OR$. Note that if $P = Q$, then slope at P is

$$y'|_{x=ct_1} = \left(-\frac{c^2}{x^2}\right)_{x=ct_1} = -\frac{1}{t_1^2} = -\frac{1}{t_1 t_2}$$

and if $P \neq Q$, then $t_1 \neq t_2$ and slope of PQ is

$$\frac{ct_2^{-1} - ct_1^{-1}}{ct_2 - ct_1} = \frac{t_1 - t_2}{t_1 t_2 (t_2 - t_1)} = -\frac{1}{t_1 t_2}$$

So, we don't need to consider points being same as a separate case. Equating slopes of PQ and OR, we get,

$$-\frac{1}{t_1 t_2} = -\frac{1}{t_0 t_3} \implies t_3 = \frac{t_1 t_2}{t_0}$$

Thus, for any points $P, Q \in \mathcal{C}$ with parameters t_1 and t_2 respectively for a rectangular hyperbola $\mathcal{C}$, $P \oplus Q = R$ has parameter $t_3 = t_1 t_2 t_0^{-1}$ where t_0 is the parameter corresponding to point O.

It is easy to see that $\oplus$ satisfies closure for $\mathcal{C}$. We'll verfiy each of the group axioms now.

1. **Identity:** For any $P \in \mathcal{C}$ with parameter t, $P \oplus O$ will have parameter $t' = tt_0 t_0^{-1} = t$. Thus O acts as the identity element for $\oplus$.

2. **Inverse:** The point Q with parameter $t_0^2 t^{-1}$ gives the parameter of $P \oplus Q$ to be $t' = t(t_0^2 t^{-1}) t_0^{-1} = t_0$. Hence, Q is the inverse of P.

3. **Associativity:** For any $P, Q, R \in \mathcal{C}$ with parameters t_1, t_2 and t_3 respectively, $P \oplus (Q \oplus R)$ has parameter $t_1(t_2 t_3 t_0^{-1}) t_0^{-1} = t_1 t_2 t_3 t_0^{-2}$. On the other hand, $(P \oplus Q) \oplus R$ has parameter $(t_1 t_2 t_0^{-1}) t_3 t_0^{-1} = t_1 t_2 t_3 t_0^{-2}$. Thus $\oplus$ is associative.

This shows that $\mathcal{C}$ is a group with $\oplus$ for the case where $\mathcal{C}$ is an rectangular hyperbola. Although we've shown this for a rectangular hyperbola, we'll later show that any hyperbola can be transformed into a rectangular hyperbola in such a way that intersections with lines and parallelism are preserved. Hence, this result is true for any hyperbola C.

Theorem 3. *If $\mathcal{C}$ is a hyperbola, $\langle \mathcal{C}, \oplus \rangle \cong \langle \mathbb{R}^\times, \cdot \rangle$.*

Proof. Consider $\varphi : \mathcal{C} \to \mathbb{R}^\times$ given by $\varphi((ct, ct^{-1})) = tt_0^{-1}$. For any points $P, Q \in \mathcal{C}$ parametrized by t_1 and t_2 respectively, $P \oplus Q$ has parameter $t_1 t_2 t_0^{-1}$. So,

$$\varphi(P \oplus Q) = t_1 t_2 t_0^{-2} = (t_1 t_0^{-1})(t_2 t_0^{-1}) = \varphi(P)\varphi(Q)$$

Thus φ is a homomorphism.

If $\varphi(P) = \varphi(Q)$ for some $P, Q \in \mathcal{C}$ parametrized by t_1 and t_2 respectively, then

$$t_1 t_0^{-1} = t_2 t_0^{-1} \implies t_1 = t_2$$

i.e. $P = Q$. Thus φ is injective.

For any $t \in \mathbb{R}$, we have the point $P = (c(tt_0), c(tt_0)^{-1}) \in \mathcal{C}$ such that

$$\varphi(P) = tt_0 t_0^{-1} = t$$

Thus φ is surjective. This shows that φ is a bijective homomorphism i.e. an isomorphism from $\langle \mathcal{C}, \oplus \rangle$ to $\langle \mathbb{R}^\times, \cdot \rangle$. ■

1.2 Finding Pythagorean Triplets

Consider the set $\mathcal{C} = \{(x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 1\}$ and $P_0 = (1, 0) \in \mathcal{C}$. For any $t, b \in \mathbb{Q}$, let $\ell_{t,b} = \{(x, y) \in \mathbb{Q} : y = tx + b\}$ such that $P_0 \in \ell_{t,b} \forall\, t, b \in \mathbb{Q}$. This means $0 = t + b$ or $b = -t$. Define $\ell_t := \ell_{t,-t}$. We'll now find intersection of ℓ_t and $\mathcal{C}$. From ℓ_t, we have $y = tx - t = t(x - 1)$. Putting this in $x^2 + y^2 = 1$,

$$x^2 + t^2(x^2 + 1 - 2x) = 1 \implies (1 + t^2)x^2 - 2t^2 x + (t^2 - 1) = 0$$

Applying the quadratic formula, we get

$$x = \frac{t^2 \pm \sqrt{t^4 - (t^2 + 1)(t^2 - 1)}}{t^2 + 1} = \frac{t^2 \pm 1}{1 + t^2}$$

Thus $x = 1$ or $x = (t^2 - 1)/(t^2 + 1)$. $x = 1$ corresponds to $y = 0$ i.e. the point P_0. For $x = (t^2 - 1)/(t^2 + 1)$,

$$y = t\left(\frac{t^2 - 1}{t^2 + 1} - 1\right) = \frac{-2t}{t^2 + 1}$$

Call this point P_t. As $P_t \in \mathcal{C}$,

$$\left(\frac{t^2 - 1}{t^2 + 1}\right)^2 + \left(\frac{-2t}{t^2 + 1}\right)^2 = 1 \implies (t^2 - 1)^2 + (2t)^2 = (t^2 + 1)^2$$

If $t \in \mathbb{Z}$, then $(t^2 - 1)$, $2t$ and $(t^2 + 1)$ will all be in $\mathbb{Z}$. Hence, $(t^2 - 1, 2t, t^2 + 1)$ is a valid Pythagorean triple for all $t \in \mathbb{Z}$.

Note that this does **NOT** generate all Pythagorean triples. E.g. the triple $(5, 12, 13)$ will never be generated by this method as neither 5 nor 12 is one less than a perfect square.

We can adapt a similar strategy to generate rational or integer solutions to equations of the form $ax^2 + by^2 = cz^2$ where $a, b, c \in \mathbb{Q}$.