

# PROJECTIVE GEOMETRY

Niti Torphe<sup>1</sup>  
Ruchith R<sup>2</sup>  
Saroj Kumar<sup>3</sup>  
Tejaswi K<sup>4</sup>

Supervised by  
Prof. Steven Spallone

Summer 2025

---

<sup>1</sup>[niti.sanjaytorphe@studnets.iiserpune.ac.in](mailto:niti.sanjaytorphe@studnets.iiserpune.ac.in)

<sup>2</sup>[ruchith.r@students.iiserpune.ac.in](mailto:ruchith.r@students.iiserpune.ac.in)

<sup>3</sup>[saroj.kumar@students.iiserpune.ac.in](mailto:saroj.kumar@students.iiserpune.ac.in)

<sup>4</sup>[k.tejaswinarayana@students.iiserpune.ac.in](mailto:k.tejaswinarayana@students.iiserpune.ac.in)

# Contents

<b>1</b>	<b>Conics</b>	<b>2</b>
1.1	Group Laws on Conics . . . . .	2
1.2	Generalizing to any field . . . . .	7
1.3	Finding Pythagorean Triplets . . . . .	11
<b>2</b>	<b>Conics in Characteristic 2 Fields</b>	<b>13</b>
2.1	Classification . . . . .	13
2.2	Conic Groups . . . . .	15
<b>3</b>	<b>Affine Geometry</b>	<b>17</b>
3.1	Affine space . . . . .	17
3.2	Affine frames and coordinates . . . . .	17
3.3	Affine transformation . . . . .	17
3.4	Properties of Affine Transformations . . . . .	18
3.5	Fundamental theorem of Affine Geometry . . . . .	20
<b>4</b>	<b>An Axiomatic Approach to Geometry</b>	<b>22</b>
4.1	First Axiom . . . . .	22
4.2	Second Axiom . . . . .	22
4.3	Third Axiom . . . . .	23
4.4	Fourth Axiom . . . . .	23
4.5	Desargues' Theorem . . . . .	27
<b>5</b>	<b>Projective Geometry</b>	<b>31</b>
5.1	Projective Spaces . . . . .	31
5.2	Fundamental Theorem of Projective Geometry . . . . .	33
5.3	Cross-Ratio . . . . .	37
5.4	Group Law on Cubics . . . . .	38

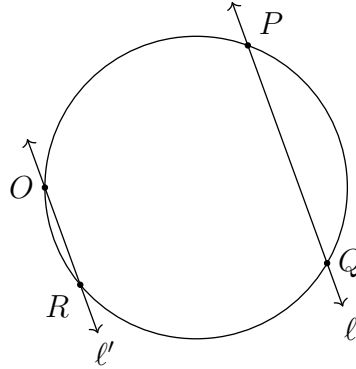
# CHAPTER 1

## Conics

The majority of this chapter is based on the ideas presented in Shirali's article on conic groups [Shi09]. We'll also develop this further with the chapter on conics over characteristic two fields.

### 1.1 Group Laws on Conics

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



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

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

#### A Note on Standard Forms

Throughout this section, we'll only use standard forms of non-degenerate conics i.e. circle, rectangular hyperbola and parabola with equations  $x^2 + y^2 = 1$ ,  $xy = 1$  and  $y = x^2$  respectively. The other non-degenerate conics in their respective classes are affine-congruent (we'll introduce this notion in Chapter 3) to these standard forms [BEG12, § 2.5 Thm. 4].

## Circle

If  $\mathcal{C} = \mathcal{S}$  with equation  $x^2 + y^2 = 1$ , any point  $P \in \mathcal{S}$  has coordinates  $(\cos t, \sin t)$  where  $t \in [0, 2\pi)$  is the angle  $P$  forms with the positive  $x$ -axis in the counter-clockwise direction.

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

$$y'|_{x=t_1} = \left( -\frac{x}{y} \right)_{t=t_1} = \left( -\frac{\cos t}{\sin t} \right)_{t=t_1} = -\cot t_1 = -\cot \left( \frac{t_1 + t_2}{2} \right)$$

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

$$\frac{\sin t_2 - \sin t_1}{\cos t_2 - \cos t_1} = -\frac{\sin \left( \frac{t_2 - t_1}{2} \right) \cos \left( \frac{t_2 + t_1}{2} \right)}{\sin \left( \frac{t_2 - t_1}{2} \right) \sin \left( \frac{t_2 + t_1}{2} \right)} = -\cot \left( \frac{t_2 + t_1}{2} \right)$$

Also note that  $\sin \left( \frac{t_2 - t_1}{2} \right)$  can be cancelled as it's only zero when  $t_2 = t_1 + 2n\pi$  which means  $P = Q$ . So, we don't need to consider the points being same as a separate case. Equating slopes of  $PQ$  and  $OR$ , we get,

$$\begin{aligned} -\cot \left( \frac{t_2 + t_1}{2} \right) &= -\cot \left( \frac{t_3 + t_0}{2} \right) \\ \implies \frac{t_2 + t_1}{2} &= n\pi + \frac{t_3 + t_0}{2} \\ \implies t_3 &= t_2 + t_1 - t_0 - 2n\pi \end{aligned}$$

As shifts of  $2n\pi$  don't affect  $t_3$ , we can ignore that term on the RHS. Thus for any  $P, Q \in \mathcal{S}$  with parameters  $t_1$  and  $t_2$  respectively for circle  $\mathcal{S}$ ,  $P \oplus_O Q = R$  has parameter  $t_3 = t_1 + t_2 - t_0$  where  $t_0$  is the parameter for point  $O$ . Note that we always add or subtract multiples of  $2\pi$  to make sure  $t_3 \in [0, 2\pi)$ .

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

1. **Identity:** For any  $P \in \mathcal{S}$  with parameter  $t$ ,  $P \oplus_O O$  will have parameter

$$t' = t + t_0 - t_0 = t$$

Thus  $O$  acts as the identity element for  $\oplus_O$ .

2. **Inverse:** The point  $Q \in \mathcal{S}$  with parameter  $2t_0 - t$  gives the parameter of  $P \oplus_O Q$  to be

$$t' = t + 2t_0 - t - t_0 = t_0$$

Hence,  $Q$  is the inverse of  $P$ .

3. **Associativity:** For any  $P, Q, R \in \mathcal{S}$  with parameters  $t_1, t_2$  and  $t_3$  respectively,  $P \oplus_O (Q \oplus_O R)$  has parameter

$$t_1 + (t_2 + t_3 - t_0) - t_0 = t_1 + t_2 + t_3 - 2t_0$$

On the other hand,  $(P \oplus_O Q) \oplus_O R$  has parameter

$$(t_1 + t_2 - t_0) + t_3 - t_0 = t_1 + t_2 + t_3 - 2t_0$$

Thus  $\oplus_O$  is associative.

This shows that  $\mathcal{S}$  is a group with  $\oplus_O$ .

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

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

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

Thus  $\varphi$  is a homomorphism.

If  $\varphi(P) = \varphi(Q)$  for some  $P, Q \in \mathcal{S}$  parametrized by  $\theta_1$  and  $\theta_2$  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  $\varphi$  is injective.

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

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

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

## Parabola

If  $\mathcal{C} = \mathcal{P}$  is the parabola with equation  $y = x^2$ , any point on it can be parametrized as  $(t, t^2)$  where  $t \in \mathbb{R}$ .

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

$$y'|_{x=t_1} = (2x)_{x=t_1} = 2t_1 = t_1 + t_2$$

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

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

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

$$t_1 + t_2 = t_0 + t_3 \implies t_3 = t_1 + t_2 - t_0$$

Thus, for any points  $P, Q \in \mathcal{P}$  with parameters  $t_1$  and  $t_2$  respectively for a parabola  $\mathcal{P}$ ,  $P \oplus_O Q = R$  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  $\oplus_O$  satisfies closure for  $\mathcal{P}$ . We'll verify each of the group axioms now.

1. **Identity:** For any  $P \in \mathcal{P}$  with parameter  $t$ ,  $P \oplus_O O$  will have parameter

$$t' = t + t_0 - t_0 = t$$

Thus  $O$  acts as the identity element for  $\oplus_O$ .

2. **Inverse:** The point  $Q \in \mathcal{P}$  with parameter  $2t_0 - t$  gives the parameter of  $P \oplus_O Q$  to be

$$t' = t + 2t_0 - t - t_0 = t_0$$

Hence,  $Q$  is the inverse of  $P$ .

3. **Associativity:** For any  $P, Q, R \in \mathcal{P}$  with parameters  $t_1, t_2$  and  $t_3$  respectively,  $P \oplus_O (Q \oplus_O R)$  has parameter

$$t_1 + (t_2 + t_3 - t_0) - t_0 = t_1 + t_2 + t_3 - 2t_0$$

On the other hand,  $(P \oplus_O Q) \oplus_O R$  has parameter

$$(t_1 + t_2 - t_0) + t_3 - t_0 = t_1 + t_2 + t_3 - 2t_0$$

Thus  $\oplus_O$  is associative.

This shows that  $\mathcal{P}$  is a group with  $\oplus_O$ .

**Theorem 2.**  $\langle \mathcal{P}, \oplus_O \rangle \cong \langle \mathbb{R}, + \rangle$ .

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

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

Thus  $\varphi$  is a homomorphism.

If  $\varphi(P) = \varphi(Q)$  for some  $P, Q \in \mathcal{P}$  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  $\varphi$  is injective.

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

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

Thus  $\varphi$  is surjective. This shows that  $\varphi$  is a bijective homomorphism i.e. an isomorphism from  $\langle \mathcal{P}, \oplus_O \rangle$  to  $\langle \mathbb{R}, + \rangle$ . ■

## Hyperbola

If  $\mathcal{C} = \mathcal{H}$  is the rectangular hyperbola with equation  $xy = 1$ , any point on it can be parametrized as  $(t, t^{-1})$  where  $t \in \mathbb{R}^\times$ .

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

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

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

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

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  $P, Q \in \mathcal{H}$  with parameters  $t_1$  and  $t_2$  respectively for a rectangular hyperbola  $\mathcal{H}$ ,  $P \oplus_O Q = R$  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  $\oplus_O$  satisfies closure for  $\mathcal{H}$ . We'll verify each of the group axioms now.

1. **Identity:** For any  $P \in \mathcal{H}$  with parameter  $t$ ,  $P \oplus_O O$  will have parameter

$$t' = t t_0 t_0^{-1} = t$$

Thus  $O$  acts as the identity element for  $\oplus_O$ .

2. **Inverse:** The point  $Q \in \mathcal{H}$  with parameter  $t_0^2 t^{-1}$  gives the parameter of  $P \oplus_O Q$  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  $P, Q, R \in \mathcal{H}$  with parameters  $t_1, t_2$  and  $t_3$  respectively,  $P \oplus_O (Q \oplus_O R)$  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,  $(P \oplus_O Q) \oplus_O R$  has parameter

$$(t_1 t_2 t_0^{-1})t_3 t_0^{-1} = t_1 t_2 t_3 t_0^{-2}$$

Thus  $\oplus_O$  is associative.

This shows that  $\mathcal{H}$  is a group with  $\oplus_O$ .

**Theorem 3.**  $\langle \mathcal{H}, \oplus_O \rangle \cong \langle \mathbb{R}^\times, \cdot \rangle$ .

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

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

Thus  $\varphi$  is a homomorphism.

If  $\varphi(P) = \varphi(Q)$  for some  $P, Q \in \mathcal{H}$  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  $\varphi$  is injective.

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

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

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

## 1.2 Generalizing to any field

**Note:** Throughout this section, we'll limit ourselves to fields whose characteristic is not 2 as fields with characteristic 2 require a more careful treatment. We'll have a look at these in Chapter 2.

In the previous section, we've considered our conic as the set of points  $(x, y) \in \mathbb{R}^2$  that make  $f(x, y) = 0$  where  $f \in \mathbb{R}[x, y]$  is square-free and has degree 2. We could very well have considered a similar set for any field  $\mathbb{F}$  and we'll now show how a similar operation gives rise to a group structure.

We'll consider  $\mathbb{F}^2$  as a vector space for the rest of this section. Consider a set

$$\mathcal{C} = \{(x, y) \in \mathbb{F}^2 : f(x, y) = 0\}$$

where  $f \in \mathbb{F}[x, y]$  is square-free and has degree 2. Fix an  $\vec{O} = (x_0, y_0) \in \mathcal{C}$ . For any  $\vec{A}, \vec{B} \in \mathcal{C}$  where  $\vec{A} = (a_1, a_2)$  and  $\vec{B} = (b_1, b_2)$ .

Let

$$\vec{c} = \begin{cases} \vec{B} - \vec{A} & \text{if } \vec{A} \neq \vec{B} \\ \left( \frac{\partial f}{\partial y}, -\frac{\partial f}{\partial x} \right)_{(x,y)=\vec{A}} & \text{otherwise} \end{cases}$$

$$\ell = \{ \vec{x} \in \mathbb{F}^2 : \vec{x} = \vec{O} + \lambda \vec{c} \quad \forall \lambda \in \mathbb{F} \}$$

Note that the partial derivative above is a formal derivative since we considered  $f$  to be a polynomial in  $x$  and  $y$ . We aren't really considering any limits here. Clearly,  $\vec{O} \in \mathcal{C} \cap \ell$ . Now,  $|\mathcal{C} \cap \ell|$  can either be 1 or 2 (from the Bézout bound). Define

$$\vec{A} \oplus_O \vec{B} := \begin{cases} \vec{C} & \text{if } \mathcal{C} \cap \ell = \{\vec{O}, \vec{C}\} \\ \vec{O} & \text{if } \mathcal{C} \cap \ell = \{\vec{O}\} \end{cases}$$



## Hyperbola and Parabola

For  $\mathcal{C} = \mathcal{P}$  and  $\mathcal{C} = \mathcal{H}$ , we get  $f(x, y)$  to be  $y - x^2$  and  $xy - 1$  respectively. In both cases, the parametrization we used for  $\mathbb{R}^2$  case works for  $\mathbb{F}^2$  as well. Further, even our formula for the operation extends nicely to  $\mathbb{F}^2$  as the derivation didn't really use any properties special to the vector space  $\mathbb{R}^2$ . So, we have  $\langle \mathcal{P}, \oplus_O \rangle \cong \langle \mathbb{F}, + \rangle$  and  $\langle \mathcal{H}, \oplus_O \rangle \cong \langle \mathbb{F}^\times, \cdot \rangle$ .

## Circle

For  $\mathcal{C} = \mathcal{S}$ , we get  $f(x, y) = x^2 + y^2 - 1$ . This curve has radial symmetry, so we can always apply a rotation to it such that  $\vec{O} = (1, 0)$ . Our goal is to find  $\lambda$  such that  $\vec{O} + \lambda \vec{c} \in \mathcal{S}$ . Suppose  $\vec{c} = (z, w)$ . Any point on  $\mathcal{S}$  must satisfy  $x^2 + y^2 = 1$ . Thus

$$\begin{aligned} (1 + \lambda z)^2 + (0 + \lambda w)^2 &= 1 \\ \implies 1 + \lambda^2(z^2 + w^2) + 2\lambda z &= 1 \\ \implies \lambda^2(z^2 + w^2) + 2\lambda z &= 0 \\ \implies \lambda((z^2 + w^2)\lambda + 2z) &= 0 \\ \implies \lambda = 0 \text{ or } \lambda &= -\frac{2z}{z^2 + w^2} \end{aligned}$$

Since  $P \neq Q$ ,  $(z, w) = (b_1 - a_1, b_2 - a_2)$ . If  $z^2 + w^2 = 0$ , then

$$\begin{aligned} b^2 + a^2 + a^2 + b^2 - 2a_1b_1 - 2a_2b_2 &= 0 \\ \implies a_1b_1 &= 1 - a_2b_2 \\ \implies a_1^2b_1^2 &= 1 + a_2^2b_2^2 - 2a_2b_2 \\ \implies a_1^2b_1^2 &= 1 + (1 - a_1^2)(1 - b_1^2) - 2a_2b_2 \\ \implies 2a_2b_2 &= 1 - a_1^2 + 1 - b_1^2 \\ \implies a_2^2 + b_2^2 - 2a_2b_2 &= 0 \\ \implies (a_2 - b_2)^2 &= 0 \\ \implies a_2 &= b_2 \end{aligned}$$

It is now easy to see that  $a_1^2 = b_1^2$  or  $a_1 = \pm b_1$ . If  $a_1 = b_1$ , then  $P = Q$  which is a contradiction. If  $a_1 = -b_1$ , then  $(z, w) = (2b_1, 0)$  but this means  $4b_1^2 = 0$  or  $b_1 = a_1 = 0$  or  $P = Q$  which is again a contradiction. Hence, we can safely assume  $z^2 + w^2 \neq 0$  when  $P \neq Q$ . The first solution just corresponds to  $\vec{O}$ , hence we take the second one. So,  $\vec{A} \oplus_O \vec{B} = (1 + \lambda z, \lambda w)$ .

If  $\vec{A} \neq \vec{B}$ , then  $\vec{c} = (z, w) = (b_1 - a_1, b_2 - a_2)$ . This means the first coordinate is

$$\begin{aligned} 1 + \lambda z &= \frac{z^2 + w^2 - 2z^2}{z^2 + w^2} \\ &= \frac{1 - b_1^2 - a_1^2 - a_2b_2 + a_1b_1}{1 - a_1b_1 - a_2b_2} \\ &= \frac{(1 - b_1^2 - a_1^2 - a_2b_2 + a_1b_1)(a_1b_1 - a_2b_2)}{(1 - a_1b_1 - a_2b_2)(a_1b_1 - a_2b_2)} \\ &= \frac{(1 - b_1^2 - a_1^2 - a_2b_2 + a_1b_1)(a_1b_1 - a_2b_2)}{1 - b_1^2 - a_1^2 - a_2b_2 + a_1b_1} \\ &= a_1b_1 - a_2b_2 \end{aligned}$$

and the second coordinate is

$$\begin{aligned}
\lambda w &= \frac{-2zw}{z^2 + w^2} \\
&= \frac{-(b_1b_2 + a_1a_2 - a_1b_2 - a_2b_1)}{1 - a_1b_1 - a_2b_2} \\
&= \frac{-(b_1b_2 + a_1a_2 - a_1b_2 - a_2b_1)(a_1b_2 + a_2b_1)}{(1 - a_1b_1 - a_2b_2)(a_1b_2 + a_2b_1)} \\
&= \frac{-(b_1b_2 + a_1a_2 - a_1b_2 - a_2b_1)(a_1b_2 + a_2b_1)}{a_1b_2 + a_2b_1 - b_1b_2 - a_1a_2} \\
&= a_1b_2 + a_2b_1
\end{aligned}$$

If  $\vec{A} = \vec{B}$ , then  $\vec{c} = (z, w) = (2a_2, -2a_1)$ . So,

$$\begin{aligned}
1 + \lambda z &= 1 + \frac{-4a_2(2a_2)}{4a_2^2 + 4a_1^2} = 1 - 2a_2^2 = a_1^2 - a_2^2 \\
\text{and } \lambda w &= \frac{-4a_2(-2a_1)}{4a_2^2 + 4a_1^2} = 2a_1a_2
\end{aligned}$$

Hence,  $\vec{A} \oplus_O \vec{B} = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)$  for any points  $\vec{A}, \vec{B} \in \mathcal{S}$ .

**Theorem 4.** If  $\mathcal{S}$  is defined over  $\mathbb{F}^2$ ,  $\langle \mathcal{S}, \oplus_O \rangle \cong \langle \text{SO}_2(\mathbb{F}), \cdot \rangle$ .

*Proof.* Consider  $\varphi: \mathcal{S} \rightarrow \text{SO}_2(\mathbb{F})$  given by

$$\varphi((a_1, a_2)) = \begin{bmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{bmatrix}$$

It is easy to see that  $\det \varphi((a_1, a_2)) = a_1^2 + a_2^2 = 1$ . Further, the columns are orthogonal to each other as  $-a_1a_2 + a_2a_1 = 0$ .

For any  $(a_1, a_2), (b_1, b_2) \in \mathcal{S}$ ,

$$\begin{aligned}
\varphi((a_1, a_2))\varphi((b_1, b_2)) &= \begin{bmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{bmatrix} \begin{bmatrix} b_1 & -b_2 \\ b_2 & b_1 \end{bmatrix} \\
&= \begin{bmatrix} a_1b_1 - a_2b_2 & -a_1b_2 - a_2b_1 \\ a_1b_2 + a_2b_1 & a_1b_1 - a_2b_2 \end{bmatrix} \\
&= \varphi((a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)) \\
&= \varphi((a_1, a_2) \oplus_O (b_1, b_2))
\end{aligned}$$

Thus  $\varphi$  is a homomorphism.

For any  $(a_1, a_2), (b_1, b_2) \in \mathcal{S}$ ,

$$\varphi((a_1, a_2)) = \varphi((b_1, b_2)) \implies \begin{bmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{bmatrix} = \begin{bmatrix} b_1 & -b_2 \\ b_2 & b_1 \end{bmatrix} \implies (a_1, a_2) = (b_1, b_2)$$

Thus  $\varphi$  is injective.

Consider any  $M \in \text{SO}_2(\mathbb{F})$ , where

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Then, by definition of  $\text{SO}_2(\mathbb{F})$ ,  $ad - bc = 1$  and  $MM^T = I$ . The second condition gives

$$\begin{aligned} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & c \\ b & d \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \implies a^2 + b^2 &= 1 \\ c^2 + d^2 &= 1 \\ ac + bd &= 0 \end{aligned}$$

Using these, we get  $a = d$  and  $b = -c$ . Consider a point  $(a, b) \in \mathbb{F}^2$ . Since  $a^2 + b^2 = 1$ ,  $(a, b) \in \mathcal{S}$ . Further,  $\varphi((a, b)) = M$ . Thus  $\varphi$  is surjective. This shows that  $\varphi$  is a bijective homomorphism i.e. an isomorphism from  $\langle \mathcal{S}, \oplus_O \rangle$  to  $\langle \text{SO}_2(\mathbb{F}), \cdot \rangle$ .  $\blacksquare$

**Theorem 5.** *If  $x^2 + 1 = 0$  has a solution in  $\mathbb{F}$ , then  $\langle \text{SO}_2(\mathbb{F}), \cdot \rangle \cong \langle \mathbb{F}^\times, \cdot \rangle$ .*

*Proof.* Let  $i \in \mathbb{F}$  be a solution to  $x^2 + 1 = 0$ . From the previous proof, we have, for any  $M(a, b) \in \text{SO}_2(\mathbb{F})$ ,

$$M(a, b) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

where  $a, b \in \mathbb{F}$ . The characteristic polynomial of  $M(a, b)$  is  $(a - \lambda)^2 + b^2$  or  $\lambda^2 - 2a\lambda + a^2 + b^2$ . Thus the eigenvalues are  $a \pm ib$ . The corresponding eigenvectors will be  $(1, \mp i)$ . We can then write  $M$  as a diagonal matrix,

$$M'(a, b) = \begin{bmatrix} a + ib & 0 \\ 0 & a - ib \end{bmatrix}$$

For any  $z \in \mathbb{F}^\times$ ,  $\exists a, b \in \mathbb{F}$  such that  $z = a + ib$ . In particular,  $b = -i(z - a)$ . Further,  $a^2 + b^2 = 1$  gives  $z^2 - 2az + 1 = 0$  i.e.  $a = (z^{-1} + z)/2$  and  $b = i(z^{-1} - z)/2$ . Consider the map  $\varphi : \mathbb{F}^\times \rightarrow \text{SO}_2(\mathbb{F})$  given by

$$\varphi(z) = M\left(\frac{z^{-1} + z}{2}, \frac{i(z^{-1} - z)}{2}\right)$$

For any  $z_1, z_2 \in \mathbb{F}^\times$ ,

$$\begin{aligned} \varphi(z_1) &= \varphi(z_2) \\ \implies z_1 z_2^2 - (z_1^2 + 1)z_2 + z_1 &= 0 \text{ and } z_2^{-1} - z_2 = z_1^{-1} - z_1 \\ \implies z_2 = z_1, z_1^{-1} \text{ and } z_2^{-1} - z_2 &= z_1^{-1} - z_1 \\ \implies z_2 &= z_1 \end{aligned}$$

So,  $\varphi$  is injective. Further, for any  $M(a, b) \in \text{SO}_2(\mathbb{F})$ ,  $a + ib \neq 0$  (otherwise,  $a^2 + b^2 = 0$ ). Hence,  $\varphi(a + ib) = M(a, b)$  and  $\varphi$  is surjective.

For any  $z_1, z_2 \in \mathbb{F}^\times$ ,

$$\begin{aligned}\varphi(z_1)\varphi(z_2) &= M\left(\frac{z_1^{-1} + z_1}{2}, \frac{i(z_1^{-1} - z_1)}{2}\right) M\left(\frac{z_2^{-1} + z_2}{2}, \frac{i(z_2^{-1} - z_2)}{2}\right) \\ &= \begin{bmatrix} \frac{(z_1 z_2)^{-1} + z_1 z_2}{2} & \frac{i((z_1 z_2)^{-1} - z_1 z_2)}{2} \\ \frac{-i((z_1 z_2)^{-1} - z_1 z_2)}{2} & \frac{(z_1 z_2)^{-1} + z_1 z_2}{2} \end{bmatrix} \\ &= M\left(\frac{(z_1 z_2)^{-1} + z_1 z_2}{2}, \frac{i((z_1 z_2)^{-1} - z_1 z_2)}{2}\right) \\ &= \varphi(z_1 z_2)\end{aligned}$$

Thus  $\varphi$  is bijective homomorphism i.e. an isomorphism from  $\langle \text{SO}_2(\mathbb{F}), \cdot \rangle$  to  $\langle \mathbb{F}^\times, \cdot \rangle$ . ■

The above theorem can better be understood by noting that applying  $(x, y) \mapsto (x, iy)$  to the equation  $x^2 + y^2 = 1$  results in  $x^2 - y^2 = 1$  which is an equation of a hyperbola. Hence, the group  $\langle \mathbb{F}^\times, \cdot \rangle$  corresponding to hyperbola is actually isomorphic to the group  $\langle \text{SO}_2(\mathbb{F}), \cdot \rangle$  corresponding to the circle if  $x^2 + 1 = 0$  has a solution in  $\mathbb{F}$ .

### 1.3 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 the intersection of  $\ell_t$  and  $\mathcal{C}$ . From  $\ell_t$ , we have  $y = tx - t = t(x - 1)$ . Putting this in  $x^2 + y^2 = 1$ ,

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

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

# CHAPTER 2

## Conics in Characteristic 2 Fields

Given a conic  $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$ , we've classified it by writing it in matrix form as

$$\begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} A & \frac{1}{2}B \\ \frac{1}{2}B & C \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} D & E \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + F = 0$$

and diagonalizing the symmetric matrix to obtain an orthonormal basis within which, the conic only has no  $xy$  term. However, this method no longer works if we're working in  $\mathbb{F}^2$  such that  $\text{ch}(\mathbb{F}) = 2$  as  $1 + 1 = 2 = 0$  and hence, we can't divide by 2.

In this chapter, we'll classify the conics in finite fields with characteristic 2 and investigate the conic groups that arise from them. We'll state the following theorem which will be used heavily throughout the chapter:

**Theorem 6.** *If  $\mathbb{F}$  is a finite field with  $\text{ch}(\mathbb{F}) = 2$ , then  $\forall a \in \mathbb{F} \exists b \in \mathbb{F}$  such that  $b^2 = a$ . We'll write  $b = \sqrt{a}$ .*

*Proof.* Suppose  $|\mathbb{F}| = q$ . Since  $\text{ch}(\mathbb{F}) = 2$ ,  $q$  is even. So,  $|\mathbb{F}^\times| = q - 1$  is odd. As  $\mathbb{F}^\times$  is cyclic for any finite field  $\mathbb{F}$  [DF04, Prop. 9.18], we have  $\mathbb{F}^\times = \langle g \rangle$  for some  $g \in \mathbb{F}^\times$ .

Take any  $a \in \mathbb{F}^\times$ . Then,  $a = g^k$  for some  $k \in \mathbb{Z}/(q-1)\mathbb{Z}$ . Now, 2 has a multiplicative inverse in  $\mathbb{Z}/(q-1)\mathbb{Z}$  since  $q-1$  is odd. Hence,  $\exists b \in \mathbb{F}^\times$  such that  $b = g^{2^{-1}k}$ . It is easy to see that  $b^2 = a$ . ■

## 2.1 Classification

Consider a non-degenerate, non-singular conic in a finite characteristic 2 field  $\mathbb{F}$  given by

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$$

where not all of  $A, B$  and  $C$  are zero.

**Case 1:**  $A \neq 0, B \neq 0$  and  $C \neq 0$

Apply the affine transformation  $(x, y) \mapsto \left(\frac{x}{\sqrt{A}}, \frac{y}{\sqrt{C}}\right)$  and take  $H = \frac{B}{\sqrt{A}\sqrt{C}}$  to get the following form

$$x^2 + Hxy + y^2 + \frac{D}{\sqrt{A}}x + \frac{E}{\sqrt{C}}y + F = 0$$

Further applying the affine transformation  $(x, y) \mapsto \left(x + \frac{E}{H\sqrt{C}}, y + \frac{D}{H\sqrt{A}}\right)$  gives

$$x^2 + Hxy + y^2 + K = 0$$

where  $K = F + \frac{D^2}{H^2A} + \frac{E^2}{H^2C} + \frac{DE}{H\sqrt{A}\sqrt{C}}$ . Now, applying the affine transformation  $(x, y) \mapsto \left(\frac{\sqrt{K}}{H}x, \frac{\sqrt{K}}{H}y\right)$  gives

$$\frac{K}{H^2}x^2 + \frac{K}{H^2}xy + \frac{K}{H^2}y^2 + K = 0$$

We can multiply by  $\frac{H^2}{K}$  since  $K = 0$  will make the conic singular. Thus, taking  $L = H^2$  we have

$$\boxed{x^2 + xy + y^2 + L = 0}$$

where  $L$  can be any non-zero element of  $\mathbb{F}$  due to Theorem 6.

### Case 2: $A = 0, B \neq 0$ and $C \neq 0$

Apply the affine transformation  $(x, y) \mapsto (x, x + y)$  to get

$$(B + C)x^2 + Bxy + Cy^2 + (D + E)x + Ey + F = 0$$

If  $B \neq C$ , we can proceed as Case 1. Otherwise, we have

$$Bxy + By^2 + Dx + Ey + F = 0$$

Applying the affine transformation  $(x, y) \mapsto \left(\frac{x}{\sqrt{B}}, \frac{y}{\sqrt{B}}\right)$  and take  $H = \frac{B}{\sqrt{C}}$  to get the following form

$$xy + y^2 + \frac{D}{\sqrt{B}}x + \frac{E}{\sqrt{B}}y + F = 0$$

Further applying the affine transformation  $(x, y) \mapsto \left(x + \frac{E}{\sqrt{B}}, y + \frac{D}{\sqrt{B}}\right)$  gives

$$xy + y^2 + K = 0$$

where  $K = F + \frac{D^2}{B} + \frac{DE}{B}$ . Now, applying the affine transformation  $(x, y) \mapsto (x + y, y)$  gives

$$xy + K = 0$$

We can now proceed as Case 3.

### Case 3: $A = 0, B \neq 0$ and $C = 0$

Applying the affine transformation  $(x, y) \mapsto \left(x + \frac{E}{B}, y + \frac{D}{B}\right)$  gives

$$Bxy + H = 0$$

where  $H = F + \frac{DE}{B^2}$ . Dividing by  $B$  and taking  $K = \frac{H}{B}$ , we get

$$xy + K = 0$$

Finally, applying the affine transformation  $(x, y) \mapsto (\sqrt{K}x, \sqrt{K}y)$  and dividing by  $K$  ( $K = 0$  implies conic is singular) results in

$$\boxed{xy + 1 = 0}$$

**Case 4:**  $A \neq 0, B = 0$  and  $C \neq 0$

Apply the affine transformation  $(x, y) \mapsto \left(\frac{x}{\sqrt{A}}, \frac{y}{\sqrt{C}}\right)$  to get the following form

$$x^2 + y^2 + \frac{D}{\sqrt{A}}x + \frac{E}{\sqrt{C}}y + F = 0$$

Further applying the affine transformation  $(x, y) \mapsto (x, x + y)$  gives

$$y^2 + Hx + Ky + F = 0$$

where  $H = \left(\frac{D}{\sqrt{A}} + \frac{E}{\sqrt{C}}\right)$  and  $K = \frac{E}{\sqrt{C}}$ . We can proceed as Case 5 from here.

**Case 5:**  $A = 0, B = 0$  and  $C \neq 0$

Applying the affine transformation  $(x, y) \mapsto \left(x, \frac{y}{\sqrt{C}}\right)$  to get the following form

$$y^2 + Dx + \frac{E}{\sqrt{C}}y + F = 0$$

Note that since  $D = 0$  gives a quadratic equation in  $y$ , this case corresponds to a degenerate conic. Hence, we can assume  $D \neq 0$ . So, applying the affine transformation  $(x, y) \mapsto \left(\frac{x}{D} + \frac{Ey}{D\sqrt{C}} + \frac{F}{D}, y\right)$  gives

$$\boxed{y^2 + x = 0}$$

Thus, upto affine congruence there are 3 classes of non-degenerate, non-singular conics in finite fields of characteristic two:

- I.  $y^2 + x = 0$
- II.  $xy + 1 = 0$
- III.  $x^2 + xy + y^2 + L = 0 \quad \forall L \in \mathbb{F}^\times$

From here on, we'll refer to these as Type I, Type II and Type III conics respectively.

Note that Type I and Type II have equations similar to parabola and hyperbola. Further, since  $x^2 + 1 = 0$  has a solution in any field of characteristic two, Theorem 5 gives us that ellipses and hyperbolae will be affine congruent. Hence, all the non-degenerate conics we're used to in  $\mathbb{R}$  are contained in the Type I and Type II cases. Type III, however, is a new class that appears only in the case of characteristic two fields.

## 2.2 Conic Groups

For Type I and Type II conics, we can achieve a similar parametrization as done for any field with characteristic not two in Chapter 1. This gives us the groups corresponding to Type I and Type II conics to be isomorphic to  $\langle \mathbb{F}, + \rangle$  and  $\langle \mathbb{F}^\times, \cdot \rangle$ .

For Type III conics, we have to consider a quadratic field extension  $\mathbb{F}(\alpha)$  as a two dimensional vector space over  $\mathbb{F}$  with an ordered basis  $\{1, \alpha\}$ . Note that such an  $\alpha$  is guaranteed



to exist as the finite field of order  $|\mathbb{F}|^2$  has a subfield isomorphic to  $\mathbb{F}$  since  $|\mathbb{F}| \mid |\mathbb{F}|^2$  [DF04, §14.3]. Suppose  $\alpha$  is the root of the equation  $x^2 + bx + c$  and hence  $\alpha^2 = b\alpha + c$ .

Note that for some fixed  $a = a_1 + a_2\alpha \in \mathbb{F}(\alpha)$ , multiplying any  $x = x_1 + x_2\alpha \in \mathbb{F}(\alpha)$  by  $a$  is an  $\mathbb{F}$ -linear map since

$$\begin{aligned} ax &= (a_1 + a_2\alpha)(x_1 + x_2\alpha) \\ &= a_1x_1 + (a_1x_2 + a_2x_1)\alpha + a_2x_2\alpha^2 \\ &= (a_1 + a_2\alpha)x_1 + (a_2c + a_1\alpha + a_2b\alpha)x_2 \\ &= \begin{bmatrix} a_1 & a_2c \\ a_2 & a_1 + a_2b \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \end{aligned}$$

We'll consider a map  $N: \mathbb{F}(\alpha) \rightarrow \mathbb{F}$  which sends  $z = x + y\alpha \in \mathbb{F}(\alpha)$  to the determinant of the above matrix for multiplying by  $a$  i.e.

$$N(z) = N(x + y\alpha) = \begin{vmatrix} x & cy \\ y & x + by \end{vmatrix} = x(x + by) + cy^2 = x^2 + cy^2 + bxy$$

This map is known as the field norm on  $\mathbb{F}(\alpha)$ . It is easy to see that the equation  $N(z) = k$  for some  $k \in \mathbb{F}^\times$  corresponds to a conic in  $\mathbb{F}^2$  that is Type III (since  $A = 1$ ,  $B = b$  and  $C = c^2$ ). Further,  $N$  can be thought of as a group homomorphism from  $\mathbb{F}(\alpha)^\times$  to  $\mathbb{F}^\times$  since  $N(1) = 1$  and

$$\begin{aligned} N((x + y\alpha)(z + w\alpha)) &= N(xz + yw\alpha^2 + (xw + yz)\alpha) \\ &= N(xz + cyw + (xw + yz + byw)\alpha) \\ &= x^2(z^2 + cw^2 + b zw) + cy^2(z^2 + cw^2 + b zw) \\ &\quad + bxy(z^2 + cw^2 + b zw) \\ &= (x^2 + cy^2 + bxy)(z^2 + cw^2 + b zw) \\ &= N(x + y\alpha)N(z + w\alpha) \end{aligned}$$

For any  $z \in \mathbb{F}(\alpha)$  that satisfies  $N(z) = k$ , every element of the coset  $(\ker N)z$  also satisfies  $N(z) = k$ . In fact, these are the only solutions as cosets are either equal or disjoint. Hence, the order of the conic group of Type III is  $|\ker N|$ .

This is where the investigation ends. There are two main directions to complete this theory – first is classifying the structure of the group of Type III conics – and second is looking at the case of infinite fields with characteristic two.

# CHAPTER 3

## Affine Geometry

Affine spaces extend the concept of vector spaces and linear transformations with the familiar notion of translation. The treatment of affine geometry given here is majorly inspired from Berger's textbook [Ber87]. The more application oriented parts such as properties of affine transformations are taken from Brannan's textbook on geometry [BEG12].

### 3.1 Affine space

**Definition 1.** Given a vector space  $\vec{X}$  over  $\mathbb{F}$ , its set of points  $X$  and an operation  $+: X \times \vec{X} \rightarrow X$  such that  $\forall \vec{v}, \vec{w} \in \vec{X}$  and  $\forall p \in X$ ,

1.  $p + \vec{0} = p$
2.  $p + (\vec{v} + \vec{w}) = (p + \vec{v}) + \vec{w}$
3.  $\theta_p: \vec{X} \rightarrow X$  given by  $\theta_p(\vec{v}) = p + \vec{v}$  is a bijection.

Then  $X$  is called an affine space with underlying vector space  $\vec{X}$ .

Due to the third point above, we have the following definition:

**Definition 2.** Given an affine space  $X$ , for any  $a, b \in X$ ,

$$b - a := \theta_a^{-1}(b)$$

### 3.2 Affine frames and coordinates

**Definition 3.** An  $(n + 1)$ -tuple  $(p_0, \vec{v}_1, \dots, \vec{v}_n)$  where  $p_0 \in X$  and  $\{\vec{v}_1, \dots, \vec{v}_n\}$  is a basis of  $\vec{X}$  is called an affine frame.

Given  $p \in X$  and an affine frame  $(p_0, \vec{v}_1, \dots, \vec{v}_n)$  of  $X$ , if  $p - p_0 = c_1\vec{v}_1 + \dots + c_n\vec{v}_n$ , then  $p$  is said to have coordinates  $(c_1, \dots, c_n)$  in that frame.

### 3.3 Affine transformation

**Definition 4.** Given an affine space  $X$ , a function  $f: X \rightarrow X$  is said to be an affine transformation if  $\exists \vec{f} \in \text{End}(\vec{X}): \vec{f}(b - a) = f(b) - f(a) \forall a, b \in X$ .

*Notation.* We denote the set of affine transformations over  $X$  as  $A(X)$  and the set of invertible affine transformations over  $X$  as  $GA(X)$ .

**Theorem 7.** *Given  $f \in A(X)$ ,  $\vec{f}$  is unique. Further, given some  $p_0 \in X$ ,  $\exists! b \in A$  such that  $f(p) = b + \vec{f}(p - p_0) \forall p \in X$ .*

*Proof.* Suppose  $\vec{f}_1, \vec{f}_2 \in \text{End}(\vec{X})$  such that for any  $a, b \in X$

$$\begin{aligned}\vec{f}_1(b - a) &= f(b) - f(a) \\ \vec{f}_2(b - a) &= f(b) - f(a)\end{aligned}$$

Assume  $\exists \vec{v} \in \vec{X}: \vec{f}_1(\vec{v}) \neq \vec{f}_2(\vec{v})$ . For some  $a \in X$ , we have  $\theta_a(\vec{v}) \in X$  such that  $\theta_a(\vec{v}) - a = \theta_a^{-1}(\theta_a(\vec{v})) = \vec{v}$ . This means

$$\vec{f}_1(\vec{v}) = \vec{f}_1(\theta_a(\vec{v}) - a) = f(\theta_a(\vec{v})) - f(a) = \vec{f}_2(\theta_a(\vec{v}) - a) = \vec{f}_2(\vec{v})$$

This is a contradiction. Hence, our assumption that such a  $\vec{v}$  exists must be wrong and so,  $\vec{f}_1 = \vec{f}_2$ .

Fixing some  $p_0 \in X$ , we have  $\vec{f}(p - p_0) = f(p) - f(p_0) \forall p \in X$ . So,

$$f(p) = f(p_0) + \vec{f}(p - p_0) \forall p \in X$$

Hence,  $b = f(p_0)$ . For some  $b_1, b_2 \in X$  and  $b_1 \neq b_2$ , assume

$$f(p) = b_1 + \vec{f}(p - p_0) \forall p \in X$$

$$f(p) = b_2 + \vec{f}(p - p_0) \forall p \in X$$

Note that

$$b_1 = b_1 + (\vec{f}(p - p_0) - \vec{f}(p - p_0)) = (b_1 + \vec{f}(p - p_0)) - \vec{f}(p - p_0) = f(p) - \vec{f}(p - p_0)$$

$$b_2 = b_2 + (\vec{f}(p - p_0) - \vec{f}(p - p_0)) = (b_2 + \vec{f}(p - p_0)) - \vec{f}(p - p_0) = f(p) - \vec{f}(p - p_0)$$

Hence,  $b_1 = b_2$ . ■

### 3.4 Properties of Affine Transformations

**Definition 5.** Given  $a, b \in X$ , we define the line passing through  $a$  and  $b$  as

$$\ell_{ab} := \{a + t(b - a) : t \in \mathbb{F}\}$$

**Definition 6.** Two lines  $\ell_{ab}$  and  $\ell_{pq}$  are said to be parallel if  $b - a = k(p - q)$  for some  $k \in \mathbb{F}$ . We write this as  $\ell_{ab} \parallel \ell_{pq}$ .

**Theorem 8.** *Consider  $f \in GA(X)$  and  $\ell_{ab}$  for some  $a, b \in X$ . Then,*

$$\exists p, q \in X : f(\ell_{ab}) = \ell_{pq}$$

*Proof.* Fixing  $p_0 = a$  in Theorem 7, we have  $p \in X$  such that

$$f(a + t(b - a)) = p + \vec{f}(t(b - a)) = p + t\vec{f}(b - a) \quad \forall t \in \mathbb{F}$$

Since  $\vec{v} \mapsto p + \vec{v}$  is a bijection, we have  $q \in X$  such that  $q - p = \vec{f}(b - a)$ . Thus

$$f(a + t(b - a)) = p + t(q - p) \quad \forall t \in \mathbb{F}$$

i.e.  $f(\ell_{ab}) = \ell_{pq}$ . ■

The above theorem can be interpreted as the following statement:

*Affine transformations take straight lines to straight lines.*

**Theorem 9.** For any  $f \in \text{GA}(X)$ ,

$$\ell_{ab} \parallel \ell_{pq} \implies f(\ell_{ab}) \parallel f(\ell_{pq})$$

*Proof.* Since  $\ell_{ab} \parallel \ell_{pq}$ , we have  $b - a = k(q - p)$  for some  $k \in \mathbb{F}$ . Using Theorem 7, we can write

$$\begin{aligned} f(\ell_{ab}) &= \{f(a + t(b - a)) : t \in \mathbb{F}\} \\ &= \{c + \vec{f}(a + t(b - a) - p_0) : t \in \mathbb{F}\} \\ &= \{c + \vec{f}((a - p_0) + t(b - a)) : t \in \mathbb{F}\} \\ &= \{c + \vec{f}(a - p_0) + t\vec{f}(b - a) : t \in \mathbb{F}\} \end{aligned}$$

Similarly,  $f(\ell_{pq}) = \{c + \vec{f}(p - p_0) + t\vec{f}(q - p) : t \in \mathbb{F}\}$ . Now,

$$b - a = k(q - p) \implies \vec{f}(b - a) = k\vec{f}(q - p)$$

By definition, this means that  $f(\ell_{ab}) \parallel f(\ell_{pq})$ . ■

The above theorem can be interpreted as the following statement:

*Affine transformations take parallel lines to parallel lines.*

If the underlying vector space  $\vec{X}$  of an affine space  $X$  has a norm  $\|\cdot\|$  defined on it, we have the following theorem:

**Theorem 10.** Given  $f \in \text{GA}(X)$ , a line  $\ell_{ac}$  and any  $b \in \ell_{ac}$  such that  $b \neq a$  and  $b \neq c$ , we have

$$\frac{\|b - a\|}{\|c - b\|} = \frac{\|f(b) - f(a)\|}{\|f(c) - f(b)\|}$$

*Proof.* Since  $b \in \ell_{ac}$ , let  $b = a + t_0(c - a)$ . Now,

$$\frac{\|b - a\|}{\|c - b\|} = \frac{|t_0| \|c - a\|}{|1 - t_0| \|c - a\|} = \left| \frac{t_0}{1 - t_0} \right|$$

Using Theorem 7 with  $p_0 = a$ , we have  $f(x) = p + \vec{f}(x - a)$  for some  $p \in X$ . So,

$$\begin{aligned} f(a) &= p + \vec{f}(a - a) = p \\ f(b) &= p + \vec{f}(a + t_0(c - a) - a) = p + t_0 \vec{f}(c - a) \\ f(c) &= p + \vec{f}(c - a) \end{aligned}$$

Hence,

$$\frac{\|f(b) - f(a)\|}{\|f(c) - f(b)\|} = \frac{|t_0| \|\vec{f}(c - a)\|}{|1 - t_0| \|\vec{f}(c - a)\|} = \left| \frac{t_0}{1 - t_0} \right|$$

■

The above theorem can be interpreted as the following statement:

*Affine transformations preserve the ratio of distances of 3 collinear points.*

### 3.5 Fundamental theorem of Affine Geometry

**Theorem 11.** *If  $A_0, A_1, \dots, A_n, B_0, B_1, \dots, B_n \in X$  such that  $\{A_1 - A_0, \dots, A_n - A_0\}$  and  $\{B_1 - B_0, \dots, B_n - B_0\}$  are linearly independent where  $n = \dim \vec{X}$ , then*

$$\exists! f \in \text{GA}(X): f(A_i) = B_i \ \forall i \in \{0, 1, \dots, n\}$$

*Proof.* Let  $\vec{v}_i = A_i - A_0$  and  $\vec{w}_i = B_i - B_0 \ \forall i \in \{1, 2, \dots, n\}$ . Clearly, both  $\beta_1 = \{\vec{v}_1, \dots, \vec{v}_n\}$  and  $\beta_2 = \{\vec{w}_1, \dots, \vec{w}_n\}$  form a basis for  $\vec{X}$ . In fact, there are unique linear transformations  $\vec{f}_1, \vec{f}_2 \in \text{GL}(\vec{X})$  such that  $\vec{f}_1(\vec{v}_i) = \vec{e}_i$  and  $\vec{f}_2(\vec{w}_i) = \vec{e}_i \ \forall i \in \{1, 2, \dots, n\}$  where  $\{\vec{e}_1, \dots, \vec{e}_n\}$  is the standard basis of  $\vec{X}$ .

Consider the affine transformations  $f_1, f_2 \in \text{GA}(X)$  given by

$$\begin{aligned} f_1(p) &= O + \vec{f}_1(p - A_0) \ \forall p \in X \\ f_2(p) &= O + \vec{f}_2(p - B_0) \ \forall p \in X \end{aligned}$$

Now,  $f_1(A_0) = f_2(B_0) = O$  and  $f_1(A_i) = f_2(B_i) = O + \vec{e}_i \ \forall i \in \{1, 2, \dots, n\}$ . Since  $f_1$  and  $f_2$  are invertible, it is easy to see that  $f = f_2^{-1} f_1$  satisfies  $f(A_i) = B_i \ \forall i \in \{0, 1, \dots, n\}$ .

Next, we need to prove that  $f$  is unique. Suppose there are two affine transformations  $g_1, g_2 \in \text{GA}(X)$  that satisfy  $g_1(A_i) = g_2(A_i) = B_i \ \forall i \in \{0, 1, \dots, n\}$  but  $\exists q_0 \in X$  such that  $g_1(q_0) \neq g_2(q_0)$ .

From Theorem 7, picking  $p_0 = A_0$ ,  $\exists! b_1, b_2 \in X$  such that  $\forall q \in X$

$$\begin{aligned} g_1(p) &= b_1 + \vec{g}_1(p - A_0) \\ g_2(p) &= b_2 + \vec{g}_2(p - A_0) \end{aligned}$$

Since  $g_1(A_0) = g_2(A_0) = B_0$ , we have  $b_1 = b_2$ . Further using

$$g_1(A_i) = g_2(A_i) = B_i \quad \forall i \in \{1, 2, \dots, n\}$$

we get the relations

$$\vec{g}_1(\vec{v}_i) = \vec{g}_2(\vec{v}_i) \quad \forall i \in \{1, 2, \dots, n\}$$

But note that  $\beta_1$  is a basis of  $\vec{X}$ . Thus for any  $\vec{a} \in \vec{X}$ , we have scalars  $c_1, \dots, c_n$  such that  $\vec{a} = c_1\vec{v}_1 + \dots + c_n\vec{v}_n$ . Hence,

$$\vec{g}_1(\vec{a}) = c_1\vec{g}_1(\vec{v}_1) + \dots + c_n\vec{g}_1(\vec{v}_n) = c_1\vec{g}_2(\vec{v}_1) + \dots + c_n\vec{g}_2(\vec{v}_n) = \vec{g}_2(\vec{a}) \quad \forall \vec{a} \in \vec{X}$$

So,  $b_1 = b_2$  and  $\vec{g}_1 = \vec{g}_2$ . But this contradicts that  $\exists q_0 \in X: g_1(q_0) \neq g_2(q_0)$ . Hence,  $g_1 = g_2$ . ■

Intuitively, this theorem says that there exists an affine transformation in  $\text{GA}(X)$  which takes an  $n$ -simplex in an affine space  $X$  with  $\dim \vec{X} = n$  to another  $n$ -simplex in  $X$ . Note that an  $n$ -simplex is a generalization of the concept of triangles and tetrahedra in 2D and 3D respectively. In particular, a triangle is a 2-simplex and a tetrahedron is a 3-simplex. So, if we consider the affine space  $\mathbb{R}^2$ , this theorem says that there is an affine transformation that takes any triangle to any other triangle. We can also state it as

*All triangles in  $\mathbb{R}^2$  are affine-congruent.*

In general, we say two figures are affine-congruent if there is an invertible affine transformation taking one to the other.

# CHAPTER 4

## An Axiomatic Approach to Geometry

The contents of this chapter are adapted Ardin's textbook *Geometric Algebra* [Art57].

### 4.1 First Axiom

**Definition 7.** A plane is a triple  $(\mathcal{P}, \mathcal{L}, I)$ . The set  $\mathcal{P}$  consists of the points, the set  $\mathcal{L}$  consists of the lines, and the inclusion  $I \subseteq \mathcal{P} \times \mathcal{L}$  is an incidence relation.

**Definition 8.** If  $l, m \in \mathcal{L}$  such that either  $l = m$  or  $P I l \implies (P, m) \notin I \forall P \in \mathcal{P}$ , then we say  $l$  and  $m$  are parallel.

**Axiom (1).** For any  $P, Q \in \mathcal{P}$ , there exists a unique  $l \in \mathcal{L}$  such that  $P I l$  and  $Q I l$ . We write  $l = P + Q$ .

For any given  $l, m \in \mathcal{L}$ , if  $\exists! P \in \mathcal{P}$  such that  $P I l$  and  $P I m$ , then  $l \nparallel m$ . If there are two or more such points, say  $P$  and  $Q$ , then  $P I l, Q I l, P I m$ , and  $Q I m$ . By axiom 1,  $l = m$  and hence,  $l \parallel m$ .

Let  $\mathcal{P}_l \subset \mathcal{P}$  be the set of all points on  $l$  that is  $\mathcal{P}_l := \{P \in \mathcal{P} : P I l\}$ .

### 4.2 Second Axiom

**Axiom (2).** For any  $P \in \mathcal{P}$  and  $l \in \mathcal{L}$ , there exists a unique  $m \in \mathcal{L}$  such that  $P I m$ , and  $l \parallel m$ .

**Theorem 12.** *Parallel is an equivalence relation.*

*Proof.* For any  $l \in \mathcal{L}$ ,  $l = l$ , hence  $l \parallel l$ . If  $l, m \in \mathcal{L}$  and  $l \parallel m$ , then  $m \parallel l$ . Assume  $l \parallel m$ , and  $m \parallel n$ . If there exists no  $P \in \mathcal{P}$  such that  $P I l$  and  $P I n$ , then  $l \parallel n$ . Otherwise, if  $\exists P \in \mathcal{P}$  such that  $P I l$  and  $P I n$ , then by axiom 2,  $\exists! r \in \mathcal{L}$  such that  $P I r$ , and  $r \parallel m$ . Hence,  $l = n$  and  $l \parallel n$ . ■

An equivalence class of parallel lines is called a pencil of parallel lines.

**Theorem 13.** *Suppose there exist three distinct pencils  $\pi_1, \pi_2$  and  $\pi_3$  of parallel lines. Then any pencil  $\pi$  contains as many lines as the number of points on any line.*

*Proof.* Let  $l \in \pi_1$ ,  $m \in \pi_2$ . For every  $Q_i \in \mathcal{P}$  such that  $Q_i \text{ I } l$ , by axiom 2, there exists exactly one  $m_i \in \mathcal{L}$  such that  $m \parallel m_i$  and  $P \text{ I } m_i$ . If  $m_i = m_j$ , by axiom 1,  $P_i = P_j$  and therefore  $i = j$ .

For every  $l_i \in \pi_2$ , as  $l \not\parallel l_i$ , there exists exactly one  $P_i \in \mathcal{P}$  such that  $P_i \text{ I } l$  and  $P_i \text{ I } l_i$ . If  $P_i = P_j$ , then by axiom 2, we have a unique  $l_k \in \mathcal{L}$  such that  $P_i \text{ I } l_k$  and  $l_k \parallel m$ . Hence,  $l_i = l_j$  and therefore  $i = j$ .

We found a one-to-one correspondence between the points on  $l$  and the lines in  $\pi_2$ . Hence, for given two distinct pencils, the number of lines in one pencil is equal to the number of points on a line in another pencil. Now, we use the fact that we have 3 distinct pencils of parallel lines. The number of points on a line in  $\pi_3$  is equal to the number of lines in  $\pi_1$  and the number of points on a line in  $\pi_3$  is equal to the number of lines in  $\pi_2$ , hence the number of lines in  $\pi_1$  and  $\pi_2$  is equal and therefore, the number of points on any line in  $\pi_1$ ,  $\pi_2$  and  $\pi_3$  is same.  $\blacksquare$

### 4.3 Third Axiom

**Axiom (3).** There exist three distinct points  $A, B, C \in \mathcal{P}$  such that  $(C, A + B) \notin \text{I}$ . We also say that there exist three non-collinear points.

The smallest structure possible with this geometry is  $\mathbb{Z}_2^2$ .

### 4.4 Fourth Axiom

**Definition 9.** A map  $\sigma: \mathcal{P} \rightarrow \mathcal{P}$  is called a dilatation if for any distinct  $P, Q \in \mathcal{P}$  and  $l' \in \mathcal{L}$  such that  $l' \parallel P + Q$  and  $P' \text{ I } l'$ , we have  $Q' \text{ I } l'$  where  $P' = \sigma P$  and  $Q' = \sigma Q$ .

We can give two examples,

- i.  $\sigma P = P_0 \forall P \in \mathcal{P}$  given a fixed  $P_0 \in \mathcal{P}$ .
- ii.  $\sigma P = P \forall P \in \mathcal{P}$ .

**Theorem 14.** A dilatation  $\sigma$  is uniquely determined by the images  $P', Q'$  of two distinct points  $P$  and  $Q$ . If  $P' = Q'$ , then  $\sigma$  is degenerate and all points are mapped to  $P'$ . Otherwise, if  $P' \neq Q'$ , then  $\sigma$  is one-to-one and onto map.

*Proof.* For  $R \notin \mathcal{P}_{P+Q}$ ,  $R + P \not\parallel R + Q$ . Let  $l' \in \mathcal{L}$  such that  $P' \text{ I } l'$  and  $l' \parallel R + P$ , then by definition,  $R' \text{ I } l'$ . Similarly, let  $l'' \in \mathcal{L}$  such that  $Q' \text{ I } l''$  and  $l'' \parallel Q + P$ , and so,  $R' \text{ I } l''$ . Hence,  $l' \not\parallel l''$  and  $\exists! R' \in \mathcal{P}$  such that  $R' \text{ I } l'$  and  $R' \text{ I } l''$ . Therefore,  $R'$  is uniquely determined.

For  $R \in \mathcal{P}_{P+Q}$ ,  $P \neq R$ . By axiom 3,  $\exists S \notin \mathcal{P}_{P+Q}$ . If  $R \in \mathcal{P}_{P+S}$ , then  $P + Q = P + S$  since  $P, R \in \mathcal{P}_{P+Q}$  and  $P, R \in \mathcal{P}_{P+S}$ . Therefore,  $R \notin \mathcal{P}_{P+S}$ . We uniquely determine  $S'$  using the images  $Q'$  and  $P'$ , and later uniquely determine  $R'$  using the images  $S'$  and  $P'$ .

Suppose  $P' = Q'$ . Then the degenerate map  $\gamma$  which maps every point to  $P'$  has the same effect as  $\sigma$  which sends both  $P$  and  $Q$  to  $P'$ . Hence,  $\sigma = \gamma$  due to uniqueness.

Suppose  $P' \neq Q'$ , and let  $R'$  be a given point. For  $R' \notin \mathcal{P}_{P'+Q'}$ ,  $R' + P' \not\parallel R' + Q'$ . Let  $l_1 \in \mathcal{L}$  such that  $P \text{ I } l_1$  and  $l_1 \parallel R' + P'$  and let  $l_2 \in \mathcal{L}$  such that  $Q \text{ I } l_2$  and  $l_2 \parallel Q' + P'$ .



Then,  $l_1 \nparallel l_2$  and hence,  $\exists! R \in \mathcal{P}$  such that  $R \text{ I } l_1$  and  $R \text{ I } l_2$ . Therefore,  $R$  is uniquely determined.

If  $R \in \mathcal{P}_{P+Q}$ , then  $P \text{ I } l_1$  and  $Q \text{ I } l_2$ , hence  $P + Q = l_1$  or  $P + Q = l_2$ . By definition,  $P' + Q' \parallel P' + R'$  or  $P' + Q' \parallel Q' + R'$ , which contradicts. Hence, with the help of given images of  $P$  and  $Q$  and using the point, we found  $R$ . We conclude that  $R'$  is the image of  $R$ . For  $R' \in \mathcal{P}_{P'+Q'}$ ,  $P \neq R$ . According to axiom 3,  $\exists S' \notin \mathcal{P}_{P'+Q'}$ . If  $R' \in \mathcal{P}_{P'+S'}$ , then  $P' + Q' = P' + S'$  since  $P', R' \in \mathcal{P}_{P'+Q'}$  and  $P', R' \in \mathcal{P}_{P'+S'}$ . Therefore, suppose  $R' \notin \mathcal{P}_{P'+S'}$  and we uniquely determine  $S$  whose image is  $S'$  and prove that we can uniquely find  $R$  whose image is  $R'$  using the images  $P'$  and  $S'$ . ■

**Definition 10.** Let  $\sigma$  be a non-degenerate dilatation and  $P \in \mathcal{P}$ . Any  $l \in \mathcal{L}$  such that  $P \text{ I } l$  and  $\sigma P \text{ I } l$  is called a trace of  $P$ . If  $P = \sigma P$ , then all the lines passing through  $P$  are traces of  $P$ . Otherwise, if  $P \neq \sigma P$ , then the trace of  $P$  is unique and is given by  $P + \sigma P$ . We denote the set of all traces of  $\sigma$  for all  $P \in \mathcal{P}$  as  $\zeta_\sigma$ .

**Theorem 15.** Let  $\sigma$  be a non-degenerate dilatation,  $P \in \mathcal{P}$  and  $l$  be a trace of  $P$ . If  $Q \text{ I } l$ , then  $\sigma Q \text{ I } l$ .

*Proof.* Assume  $Q \neq P$  and take  $l = P + Q$ . Then  $\sigma Q \neq \sigma P$  and by definition,  $\sigma P + \sigma Q \parallel l$ . But  $\sigma P \text{ I } \sigma P + \sigma Q$  and  $\sigma P \text{ I } l$ , hence,  $l = \sigma P + \sigma Q$ . Therefore,  $\sigma Q \text{ I } l$ . ■

**Corollary 1.** The intersection of non-parallel traces is a fixed point.

This leaves us with three possibilities for the traces of non-singular dilatation, which are:

- $\sigma = 1$ , if and only if  $\zeta_\sigma = \mathcal{L}$
- $\sigma \neq 1$  and if  $P_0$  is a fixed point of  $\sigma$ , then  $\zeta_\sigma = \{l = P_0 + P : P \in \mathcal{P}\}$
- $\sigma \neq 1$  and  $\sigma$  fixes no point, then  $\zeta_\sigma = \pi$ , where  $\pi$  is some pencil of parallel lines

**Definition 11.** A non-singular dilatation  $\tau$  is called a translation if either  $\tau = 1$  or  $\tau$  has no fixed point. If  $\tau \neq 1$ , then traces of  $\tau$  form a pencil  $\pi$  of parallel lines which is called the direction of  $\tau$ .

**Theorem 16.** A translation  $\tau$  is uniquely determined by the image  $P'$  of one point  $P$ .

*Proof.* Let  $l \in \zeta_\tau$  such that  $P \text{ I } l$ . For some  $Q \notin \mathcal{P}_l$ , let  $l' \parallel l$  and  $Q \text{ I } l'$ , then  $l' \in \zeta_\tau$  and  $\tau Q \text{ I } l$  since  $\zeta_\tau$  is a pencil. Let  $m, m' \in \mathcal{L}$  such that  $m = P + Q$ ,  $P' \text{ I } m'$  and  $m' \parallel m$ . Then by definition,  $\tau Q \text{ I } m'$ . Since  $l \nparallel m$ , we have  $l' \nparallel m'$ . Since  $\tau Q \text{ I } m'$  and  $\tau Q \text{ I } l'$ , therefore  $\tau Q$  is uniquely determined.

For  $Q \in \mathcal{P}_l$  and  $Q \neq P$ ,  $\exists S \notin \mathcal{P}_l$  by axiom 3. Let  $l'' \parallel l$  such that  $S \text{ I } l''$  and hence,  $l'' \in \zeta_\tau$  and  $\tau S \text{ I } l''$ . Let  $n, n' \in \mathcal{L}$  such that  $n = P + S$ ,  $P' \text{ I } n'$  and  $n' \parallel n$ . Then by definition,  $\tau S \text{ I } n'$ . Since  $l \nparallel n$ , we have  $l' \nparallel n'$ . Since  $\tau S \text{ I } n'$  and  $\tau S \text{ I } l'$ , therefore  $\tau S$  is uniquely determined and using  $\tau S$ , we can uniquely determine  $\tau Q$ . ■

**Theorem 17.** Dilatations form a group  $D$  and translations form a normal subgroup  $T$  of  $D$ . If  $\sigma$  is a dilatation and  $\tau \neq 1$  is a translation, then  $\tau$  and  $\sigma\tau\sigma^{-1}$  have the same direction.

*Proof.* Let  $\sigma_1, \sigma_2$  be two dilatations. Then, their composition is also a dilatation since

$$P + Q \parallel \sigma_2 P + \sigma_2 Q \parallel \sigma_1 \sigma_2 P + \sigma_1 \sigma_2 Q$$

The identity map is a dilatation and since non-degenerate dilatations are one-one and onto,  $\sigma^{-1}$  exists and is a dilatation because

$$\sigma^{-1} P + \sigma^{-1} Q \parallel \sigma \sigma^{-1} P + \sigma \sigma^{-1} Q = P + Q$$

Associativity directly follows from function composition. Hence, dilatations form a group under function composition.

Let  $\tau$  be a translation. Suppose  $\tau^{-1}$  fixes a point  $P$  i.e.  $\tau^{-1} P = P \implies P = \tau P$ . Therefore,  $\tau = 1$  and  $\tau^{-1} = 1$  i.e.  $\tau^{-1}$  fixes no point iff  $\tau \neq 1$ . This proves that  $\tau^{-1}$  is a translation.

Given two translations  $\tau_1$  and  $\tau_2$ , suppose  $\tau_1 \tau_2$  fixes a point. Then,

$$\tau_1 \tau_2 P = P \implies \tau_2 P = \tau_1^{-1} P$$

So,  $\tau_1^{-1} = \tau_2$  and hence,  $\tau_1 \tau_2 = 1$ . Thus  $\tau_1 \tau_2$  fixes no points iff  $\tau_1 \tau_2 \neq 1$ . Therefore, translations form a subgroup of dilatations.

Let  $\sigma$  be a dilatation and  $\tau$  be a translation. Suppose  $\sigma \tau \sigma^{-1}$  fixes a point  $P$ . Then,

$$\sigma \tau \sigma^{-1} P = P \implies \tau \sigma^{-1} P = \sigma^{-1} P$$

i.e.  $\tau$  fixes a point  $\sigma^{-1} P$  and hence  $\tau = 1$ . Thus,  $\sigma \tau \sigma^{-1}$  fixes no points iff  $\sigma \tau \sigma^{-1} \neq 1$  i.e.  $\tau \neq 1$ . So,  $\sigma \tau \sigma^{-1}$  is a translation and hence the subgroup of translations is normal.

Suppose  $\tau \neq 1$  and the pencil  $\pi$  is the direction of  $\tau$ . Then,  $\tau \sigma^{-1} P + \sigma^{-1} P$  is the  $\tau$ -trace of  $\sigma^{-1} P$  and

$$\tau \sigma^{-1} P + \sigma^{-1} P \parallel \sigma \tau \sigma^{-1} P + \sigma \sigma^{-1} P = \sigma \tau \sigma^{-1} P + P$$

This shows  $\sigma \tau \sigma^{-1}$  and  $\tau$  have the same direction. ■

**Theorem 18.** *Identity dilatation along with the translations with same pencil  $\pi$  as their direction form a group.*

*Proof.* For  $\tau \neq 1$ ,  $P + \tau P \parallel \tau P + \tau^{-1} \tau P$ . Hence,  $\tau$  and  $\tau^{-1}$  have the same direction. For  $\tau_1, \tau_2 \neq 1$  such that they have the same direction  $\pi$ . By Theorem 15,  $P, \tau_2 P$  and  $\tau_1 \tau_2 P$  lie on the same line. If  $\tau_1 \tau_2 P = P$ , then  $\tau_1 \tau_2 = 1$  and if  $\tau_1 \tau_2 P \neq P$ , then  $\tau_1 \tau_2$  have the same direction  $\pi$ . ■

**Theorem 19.** *If translations with different directions exist, then  $T$  is a commutative group.*

*Proof.* Suppose  $\tau_1$  and  $\tau_2$  have different directions. Then, the translations  $\tau_1 \tau_2 \tau_1^{-1}$ ,  $\tau_2$  and  $\tau_2^{-1}$  have the same direction. If  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1} \neq 1$ , then  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$  has the same direction as  $\tau_2$ . Further,  $\tau_1, \tau_1^{-1}$  and  $\tau_2 \tau_1^{-1} \tau_2^{-1}$  have the same direction, hence  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1}$  has the same direction as  $\tau_1$ . But  $\tau_1$  and  $\tau_2$  have different directions, hence  $\tau_1 \tau_2 \tau_1^{-1} \tau_2^{-1} = 1$  i.e.  $\tau_1 \tau_2 = \tau_2 \tau_1$ .

Suppose  $\tau_1$  and  $\tau_2$  have the same direction. By assumption, there exists  $\tau_3$  which has a direction different  $\tau_1$  and  $\tau_2$ . Hence,  $\tau_1 \tau_3 = \tau_3 \tau_1$  from above. Now,  $\tau_2 \tau_3$  will have a direction different from  $\tau_1$  otherwise  $\tau_2^{-1} \tau_2 \tau_3 = \tau_3$  will have the same direction as  $\tau_1$ . Thus

$$(\tau_1 \tau_2) \tau_3 = \tau_1 (\tau_2 \tau_3) = (\tau_2 \tau_3) \tau_1 = \tau_2 (\tau_3 \tau_1) = \tau_2 (\tau_1 \tau_3) = (\tau_2 \tau_1) \tau_3$$

Hence,  $\tau_1 \tau_2 = \tau_2 \tau_1$ . ■

**Axiom (4a).** For any  $P, Q \in \mathcal{P}$ , there exists a translation  $\tau_{PQ}$  which moves  $P$  to  $Q$  i.e.  $\tau_{PQ}(P) = Q$ .

**Definition 12.** A map  $\alpha : T \rightarrow T$  is called a trace preserving homomorphism if:

- i. it is a homomorphism of  $T$  i.e.  $(\tau_1 \tau_2)^\alpha = \tau_1^\alpha \tau_2^\alpha$
- ii. it preserves traces i.e. either  $\tau^\alpha = 1$  or  $\tau$  and  $\tau^\alpha$  have the same direction.

We call the set of trace preserving homomorphisms  $k$ .

**Definition 13.** Given  $\alpha, \beta \in k$ , we define  $\alpha + \beta$  and  $\alpha \cdot \beta$  such that

$$\begin{aligned}\tau^{\alpha+\beta} &= \tau^\alpha \tau^\beta \\ \tau^{\alpha \cdot \beta} &= (\tau^\alpha)^\beta = \tau^{\alpha\beta}\end{aligned}$$

We define  $0 \in k$  as the map that sends all translations to the identity dilatation.

**Theorem 20.**  $\langle k, +, \cdot \rangle$  is a ring with identity. [Art57, Thm. 2.9]

**Theorem 21.** Let  $\alpha \in k$ ,  $\alpha \neq 0$  and let  $P \in \mathcal{P}$ . There exists a unique dilatation  $\sigma$  which fixes  $P$  and

$$\tau^\alpha = \sigma \tau \sigma^{-1} \quad \forall \tau \in T$$

*Proof.* Suppose such a  $\sigma$  exists. For any  $Q \in \mathcal{P}$ , and hence by axiom 4(a), we know there exists a  $\tau_{PQ} \in T$  such that  $\tau_{PQ}(P) = (Q)$ . Then  $\tau_{PQ}^\alpha = \sigma \tau_{PQ} \sigma^{-1}$ .

$$\tau_{PQ}^\alpha(P) = \sigma \tau_{PQ} \sigma^{-1}(P) = \sigma \tau_{PQ}(P) = \sigma(Q)$$

Since we know the images of two points, hence it uniquely determines  $\sigma$ . Let  $\alpha \in k$  and  $Q, R \in \mathcal{P}$  such that  $Q \neq R$ . Then,

$$\tau_{QR} \tau_{PQ} = \tau_{PR} \implies \tau_{QR}^\alpha \tau_{PQ}^\alpha = \tau_{PR}^\alpha$$

and

$$\tau_{QR}^\alpha(\tau_{PQ}^\alpha(P)) = \tau_{PR}^\alpha(P) \implies \tau_{QR}^\alpha(\sigma(Q)) = \sigma(R)$$

Now, we need to prove that  $\sigma$  is a dilatation. Let  $l \in \mathcal{L}$  such that  $\sigma(Q) \parallel l$  and  $l \parallel Q + R$ . Hence,  $l \in \zeta_{\tau_{QR}}$  and  $l \in \zeta_{\tau_{QR}^\alpha}$ . By Theorem 15, we have  $\sigma(R) \parallel l$ . So,  $Q + R \parallel \sigma(Q) + \sigma(R)$ . Since we know the images of two points under  $\sigma$ , hence  $\sigma$  is uniquely determined.

Since  $\sigma(P) = \tau_{PP}^\alpha(P) = P$ ,  $\sigma$  fixes  $P$ . If  $\sigma$  is degenerate, then every point is mapped to  $P$  i.e.  $\sigma(Q) = \tau_{PQ}^\alpha(P) = P \implies \tau_{PQ}^\alpha = 1 \quad \forall Q \in \mathcal{P}$ . Therefore,  $\tau^\alpha = 1$ , for all  $\tau \in T$  and hence  $\alpha = 0$ . Thus  $\sigma$  can't be degenerate and

$$\sigma(Q) = \tau_{PQ}^\alpha(P) = \tau_{PQ}^\alpha(\sigma(P)) \implies Q = \sigma^{-1} \tau_{PQ}^\alpha \sigma(P)$$

So,  $\sigma^{-1} \tau_{PQ}^\alpha \sigma$  is a translation which maps  $P$  to  $Q$  and it is uniquely determined as  $\tau_{PQ}$  since translations are uniquely determined by image of one point. Thus

$$\sigma^{-1} \tau_{PQ}^\alpha \sigma = \tau_{PQ} \implies \tau_{PQ}^\alpha = \sigma \tau_{PQ} \sigma^{-1}$$

Since the point  $Q$  was chosen arbitrarily,  $\tau_{PQ}$  can be any translation. Therefore,

$$\tau^\alpha = \sigma \tau \sigma^{-1} \quad \forall \tau \in T$$

■

**Axiom (4b).** If  $\tau_1, \tau_2 \in T$  such that  $\zeta_{\tau_1} = \zeta_{\tau_2}$  and  $\tau_1 \neq 1$ , there exists  $\alpha \in k$  such that  $\tau_2 = \tau_1^\alpha$ .

**Axiom (4b P).** (For a given  $P \in \mathcal{P}$ ) For any  $Q, R \in \mathcal{P}$  such that  $P, Q$  and  $R$  are distinct and collinear, there exists a dilatation  $\sigma$  which fixes  $P$  and maps  $Q$  to  $R$ .

**Theorem 22.** If axiom 4b P holds for some  $P \in \mathcal{P}$ , then axiom 4b is true, and axiom 4b implies 4b P for all  $P \in \mathcal{P}$ .

*Proof.* Assume axiom 4b P is true for a given  $P \in \mathcal{P}$ . Let  $\tau_1, \tau_2 \in T$  such that  $\zeta_{\tau_1} = \zeta_{\tau_2}$ ,  $\tau_1(P) = Q$ , and  $\tau_2(P) = R$ . Let  $\sigma$  be the dilatation for which  $\sigma(P) = P$  and  $\sigma(Q) = R$ . Now,  $\sigma\tau_1\sigma^{-1} \in T$  and  $\sigma\tau_1\sigma^{-1}(P) = \sigma\tau_1(P) = \sigma(Q) = R$ . Hence,  $\sigma\tau_1\sigma^{-1} = \tau_{PR} = \tau_2$ . So, we have  $\alpha \in k$  such that  $\tau^\alpha = \sigma\tau\sigma^{-1}$  and therefore  $\tau_2 = \tau_1^\alpha$ .

Assume axiom 4b is true and let  $P, Q, R \in \mathcal{P}$  be distinct and collinear. Consider  $\tau_1 = \tau_{PQ}$ ,  $\tau_2 = \tau_{PR}$  such that  $\zeta_{\tau_1} = \zeta_{\tau_2}$ . By axiom 4b, there exists a  $\alpha \in k$  such that  $\tau_2 = \tau_1^\alpha$ . From the previous theorem, there exists a dilatation  $\sigma$  for  $\alpha$  such that  $\sigma(P) = P$  and  $\tau^\alpha = \sigma\tau\sigma^{-1}$  for all  $\tau \in T$ . Therefore,

$$\tau_2 = \sigma\tau\sigma^{-1} \implies \tau_2\sigma = \sigma\tau_1$$

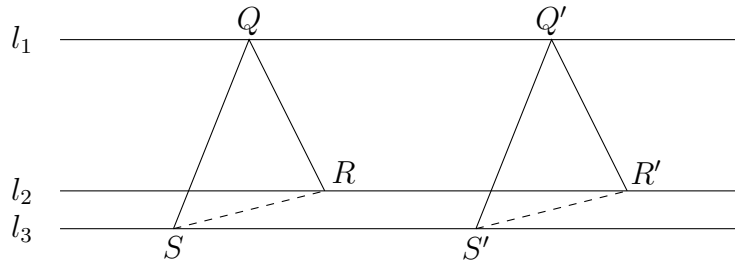
Hence,  $\sigma$  is the desired dilatation. So, axiom 4b P holds for all  $P \in \mathcal{P}$ . ■

## 4.5 Desargues' Theorem

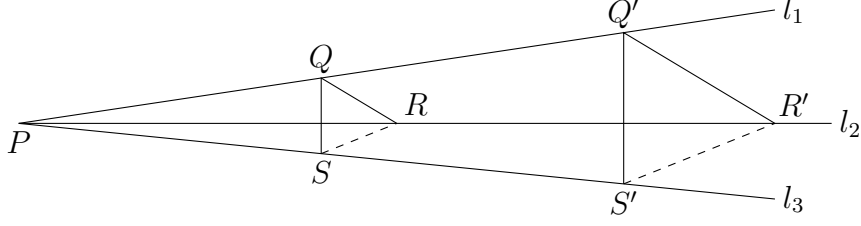
Assuming only the first three axioms hold.

**Theorem 23** (Desargues' Theorem). Let  $l_1, l_2, l_3$  be distinct lines which are either parallel or meet at a point  $P$ . Let  $Q, Q'$  be points on  $l_1$ ;  $R, R'$  points on  $l_2$  and  $S, S'$  points on  $l_3$  which are distinct from  $P$  if the lines meet.

If  $Q + R \parallel Q' + R'$  and  $Q + S \parallel Q' + S'$ ,  
then  $R + S \parallel R' + S'$



**Figure 4.1 :** Desargues' Theorem for case  $D_a$



**Figure 4.2 :** Desargues' Theorem for case **DP**

Let us discuss some trivial cases,

- If  $Q' = Q$ , then  $Q + R = Q' + R'$  and since  $R \text{ I } l_2$ ,  $R' \text{ I } l_2$  and  $R' \text{ I } Q + R$ , hence  $R = R'$  is uniquely determined. Hence, it follows that  $S = S'$ .
- If  $Q, R, S \in \mathcal{P}$  are collinear, then the images  $Q', R'$  and  $S'$  are also collinear.

We will refer to the case when the lines  $l_1, l_2, l_3$  are parallel as **D<sub>a</sub>**, and the case when the lines  $l_1, l_2, l_3$  meet at point  $P$  as **DP**.

**Theorem 24.** *Axiom 4a implies **D<sub>a</sub>** and axiom 4b P implies **DP**.*

*Proof.* To prove **D<sub>a</sub>**, let  $\tau$  be a translation which maps  $Q$  to  $Q'$ . By definition,  $Q' + R' \parallel Q + R \parallel \tau Q + \tau R = Q' + \tau R$ . Therefore,  $Q' + R' = Q' + \tau R$ . Since  $l_2 \parallel Q + Q'$ , we have  $l_2 \in \zeta_\tau$  and  $\tau R \text{ I } l_2$ . Therefore,  $\tau R = R'$ . Similarly, we get  $\tau S = S'$ . Thus,  $R + S \parallel \tau R + \tau S \parallel R' + S'$ .

To prove **DP**, let  $\sigma$  be a dilatation which fixes  $P$  and maps  $Q$  to  $Q'$ . By definition,  $Q' + R' \parallel Q + R \parallel \sigma Q + \sigma R = Q' + \sigma R$ . Therefore  $Q' + R' = Q' + \sigma R$ . Since  $l_2 = P + R$ , we have  $l_2 \in \zeta_\sigma$  and  $\sigma R \text{ I } l_2$ . Therefore,  $\sigma R = R'$ . Similarly, we get  $\sigma S = S'$ . Thus,  $R + S \parallel \sigma R + \sigma S \parallel R' + S'$ . ■

**Theorem 25.** ***D<sub>a</sub>** implies axiom 4a and **DP** axiom 4b P.*

*Proof.* Suppose each line contains only two points. Then by Theorem 13, there are two lines in a given pencil of parallel lines. Hence, only four points exists in a given pencil in our geometry. This resembles the smallest geometry that we know in which first three axioms hold,  $\mathbb{Z}_2^2$ . Let the four points of the geometry be  $A, B, C$  and  $D$ . Then there are six lines, namely  $A + B, A + C, A + D, B + C, B + D$  and  $C + D$ . This geometry satisfies all axioms, including axioms 4a and 4b. Thus from now on, we'll assume that each line contains at least three points and that for any given two lines, there exists a point such that it doesn't lie on either of the lines.

Assuming **D<sub>a</sub>**, let any  $Q, Q' \in \mathcal{P}$  such that  $Q \neq Q'$ . Consider a map  $\eta_Q$  which maps  $Q$  to  $Q'$  and is only defined for any  $R \in \mathcal{P}$  such that  $(R, Q + Q') \notin \mathcal{I}$ . Let  $l \in \mathcal{L}$  such that  $l \parallel Q + Q'$  and  $R \text{ I } l$ . Then  $l \neq Q + Q'$ . Similarly, let  $m \in \mathcal{L}$  such that  $m \parallel Q + R$  and  $Q' \text{ I } m$  which gives  $m \neq Q + R$ . Since  $Q + Q' \not\parallel Q + R$ , we have  $l \not\parallel m$ . Let  $R' \in \mathcal{P}$  such that  $R' \text{ I } l$  and  $R' \text{ I } m$ . Hence,  $R' \neq Q'$  and  $R' \neq R$ . In simpler terms,  $R + R' \parallel Q + Q'$  and  $Q + R \parallel Q' + R'$ , these describe the image  $R'$  of  $R$  under the map  $\eta_Q$ .

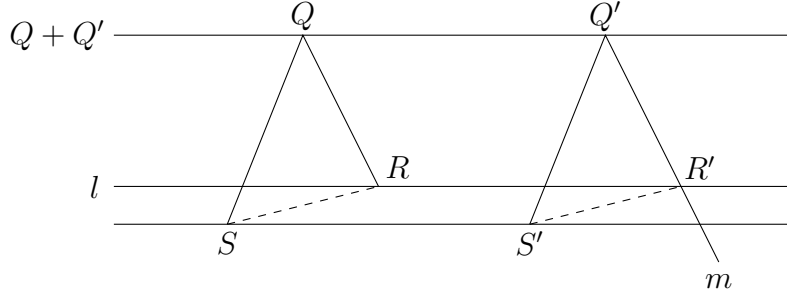


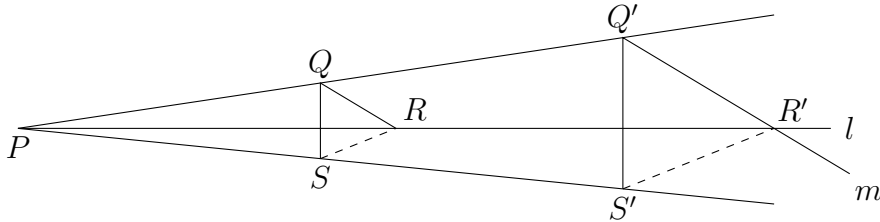
Figure 4.3

Since we have  $R$  and  $R'$ , we can now construct a map  $\eta_R$  which maps  $R$  to  $R'$ . With similar construction, it will send  $Q$  to  $Q'$ . Similarly, we'll find the image of any  $S \in \mathcal{P}$  such that  $(S, R + R') \notin I$ , and  $(S, Q + Q') \notin I$ . Thus  $S + S' \parallel Q + Q' \parallel R + R'$ ,  $Q + R \parallel Q' + R'$  and  $Q + S \parallel Q' + S'$ . So, we can uniquely determine the image  $S'$  under the map  $\eta_Q$ . By **D<sub>a</sub>**,  $R + S \parallel R' + S'$ . Since  $S + S' \parallel R + R'$  and  $R + S \parallel R' + S'$ ,  $S'$  is also an image under the map  $\eta_R$ . Clearly,  $\eta_Q$  and  $\eta_R$  agree on any  $S \in \mathcal{P}$  such that  $(S, R + R') \notin I$ , and  $(S, Q + Q') \notin I$ .

We now have  $S$  and  $S'$ ; we'll construct a map  $\eta_S$ , which maps  $S$  to  $S'$ . With similar construction, it will send  $Q$  to  $Q'$  and  $R$  to  $R'$ . So,  $\eta_Q$ ,  $\eta_R$  and  $\eta_S$  will agree on any  $T \in \mathcal{P}$  such that  $(T, S + S') \notin I$ ,  $(T, R + R') \notin I$  and  $(T, Q + Q') \notin I$ . The desired map  $\tau$  is then a combination of the three maps – for any point  $T$ , the image shall be the image under one of the three maps (for whichever it is defined). This map  $\tau$  has the property that  $\tau(Q) = Q'$ .

Now, we need to show that  $\tau$  is a dilatation. Let any  $U, V \in \mathcal{P}$  such that one of the lines  $Q + Q'$ ,  $R + R'$  or  $S + S'$  doesn't contain  $U$  and  $V$ . Without loss of generality, let us assume that  $Q + Q'$  is such a line, i.e.  $(U, Q + Q') \notin I$  and  $(V, Q + Q') \notin I$ . Hence, we will use the map  $\eta_Q$  to determine the image of  $U$  and  $V$ . For  $U + V \parallel Q + Q'$ , we have  $U' \parallel U + V$ ,  $V' \parallel U + V$  and  $U' + V' = U + V$ . For  $U + V \not\parallel Q + Q'$ , we'll use the same construction as we did to find the images of  $R$  and  $S$  and find images of  $U$  and  $V$  proving that  $U + V \parallel U' + V'$ . Hence,  $\tau$  is a dilatation and therefore a translation as  $\zeta_\tau$  is a pencil of parallel lines.

Assuming **DP**, let any distinct and collinear points  $P, Q, Q' \in \mathcal{P}$ . We'll associate a map  $\nu_Q$  which fixes  $P$ , maps  $Q$  to  $Q'$  and is only defined  $\forall R \in \mathcal{P}$  such that  $(R, Q + Q') \notin I$ . Take  $l = P + R$ , then  $l \neq Q + Q'$ . Let  $m \in \mathcal{L}$  such that  $m \parallel Q + R$ ,  $Q' \parallel m$  and  $m \neq Q + R$ . Since  $P + R \not\parallel Q + R$ , we have  $l \not\parallel m$ . Let  $R' \in \mathcal{P}$  such that  $R' \parallel l$  and  $R' \parallel m$ . Thus  $R' \neq Q'$  and  $R' \neq R$ . In simpler terms,  $P \parallel R + R'$  and  $Q + R \parallel Q' + R'$ , these describe the image  $R'$  of  $R$  under the map  $\nu_Q$ .



Since we have  $R$  and  $R'$ , we can now construct a map  $\nu_R$ , which takes  $R$  to  $R'$ . With the same construction, it will also send  $Q$  to  $Q'$ . Similarly, we'll find the image of any  $S \in \mathcal{P}$

such that  $(S, R+R') \notin I$  and  $(S, Q+Q') \notin I$ . Thus  $(P, Q+Q'), (P, R+R'), (P, S+S') \in I$ ,  $Q+R \parallel Q'+R'$  and  $Q+S \parallel Q'+S'$ . So, we can uniquely determine the image  $S'$  under the map  $\nu_Q$ . By **DP**, we have  $R+S \parallel R'+S'$ . Since  $P \in S+S'$  and  $R+S \parallel R'+S'$ ,  $S'$  is also an image under the map  $\nu_R$ . Clearly,  $\nu_Q$  and  $\nu_R$  agree on  $S \in \mathcal{P}$  such that  $(S, R+R') \notin I$  and  $(S, Q+Q') \notin I$ .

We now have  $S$  and  $S'$ ; we'll construct a map  $\nu_S$ , which maps  $S$  to  $S'$ . With similar construction, it will also send  $Q$  to  $Q'$  and  $R$  to  $R'$ . So,  $\nu_Q$ ,  $\nu_R$  and  $\nu_S$  agree on any  $T \in \mathcal{P}$  such that  $(T, S+S') \notin I$ ,  $(T, R+R') \notin I$  and  $(T, Q+Q') \notin I$ . The desired map  $\sigma$  is then a combination of the three maps: for any point  $T$  the image shall be the image under one of the three maps (for whichever it is defined). This map  $\sigma$  has the property that  $\sigma(Q) = Q'$ .

Now, we need to show that  $\sigma$  is a dilatation. Let any  $U, V \in \mathcal{P}$  such that one of the lines  $Q+Q'$ ,  $R+R'$  or  $S+S'$  doesn't contain  $U$  and  $V$ . Without loss of generality, let us assume that  $Q+Q'$  is such a line i.e.  $(U, Q+Q') \notin I$  and  $(V, Q+Q') \notin I$ . Hence, we will use the map  $\nu_Q$  to determine the image of  $U$  and  $V$ . For  $(P, U+V) \in I$ , we have  $U' \in U+V$ ,  $V' \in U+V$  and  $U'+V' = U+V$ . For  $(P, U+V) \notin I$ , we'll use the same construction as we did to find the images of  $R$  and  $S$  and find images of  $U$  and  $V$  proving that  $U+V \parallel U'+V'$ . Hence  $\sigma$  is the desired dilatation. ■

In the light of the above two theorems, Desargues' theorem is a geometric equivalent of axioms 4a and 4b P.

# CHAPTER 5

## Projective Geometry

The treatment of projective geometry given throughout most of this chapter except the last sections is taken from Audin's textbook [Aud02].

### 5.1 Projective Spaces

**Definition 14.** Let  $\vec{E}$  be a finite dimensional vector space. The *projective space*  $P(\vec{E})$  deduced from  $\vec{E}$  is the set of all 1 dimensional linear subspaces of  $\vec{E}$ .

*Remark.* The dimension of  $P(\vec{E})$  is  $\dim \vec{E} - 1$ . If  $\vec{E}$  consists only of the point 0, it does not contain any lines, and  $P(\vec{E})$  is empty. Thus it shall be implicitly assumed that  $\dim \vec{E} \geq 1$ . If  $\dim \vec{E} = 1$ ,  $\vec{E}$  itself is a line, and thus the set of lines contains a unique element,  $P(\vec{E})$  is a point.

#### 5.1.1 Projective Subspace

A subset  $V$  of  $P(\vec{E})$  is a projective subspace if it is an image of a non-zero vector subspace  $\vec{F}$  of  $\vec{E}$ .

**Proposition 1.** Let  $V$  and  $W$  be two projective subspaces of  $P(\vec{E})$ .

- If  $\dim V + \dim W \geq \dim P(\vec{E})$ , then  $V \cap W$  is not empty.
- Let  $H$  be a hyperplane of  $P(\vec{E})$ , and let  $m$  be a point not in  $H$ . Every line through  $m$  intersects  $H$  at a unique point.

*Proof.* Let  $\vec{F}$  and  $\vec{G}$  be the vector subspaces of  $\vec{E}$  from which  $V$  and  $W$  were deduced, i.e.  $V = P(\vec{F})$ , and  $W = P(\vec{G})$ . The statement can be translated into vector subspaces as

$$\begin{aligned} (\dim \vec{F} - 1) + (\dim \vec{G} - 1) &\geq (\dim \vec{E} - 1) \\ \implies \dim \vec{F} + \dim \vec{G} &\geq \dim \vec{E} + 1 \end{aligned}$$

We can use the linear algebraic properties to further deduce that:

$$\dim \vec{F} + \dim \vec{G} = \dim(\vec{F} + \vec{G}) + \dim(\vec{F} \cap \vec{G}) \leq \dim \vec{E} + \dim(\vec{F} \cap \vec{G})$$

Therefore,

$$\dim(\vec{F} \cap \vec{G}) \geq 1$$



This can be translated back into projective geometry to conclude that  $V \cap W$  is not empty.

Now, to prove the second property, let  $\vec{J}$  be the vector hyperplane of which  $H$  is image of. The point  $m$  is the image of a line  $\ell$  in  $\vec{E}$ , not contained in the hyperplane  $\vec{J}$ . The assertion, translated in terms of linear algebra, is that any plane  $\vec{P}$  containing  $\ell$  meets  $\vec{J}$  along a unique line. Since  $\ell$  is not in  $\vec{J}$ , we have  $\vec{P} + \vec{J} = \vec{E}$ . Hence,

$$\begin{aligned}\dim(\vec{P} \cap \vec{J}) &= \dim \vec{P} + \dim \vec{J} - \dim(\vec{P} + \vec{J}) \\ &= 2 + \dim \vec{E} - 1 - \dim \vec{E} = 1\end{aligned}$$

■

### 5.1.2 Projective Transformation

**Definition 15.** Let  $\vec{E}$  and  $\vec{E}'$  be two vector subspaces, and  $p: \vec{E} \setminus \{0\} \rightarrow P(\vec{E})$  and  $p': \vec{E}' \setminus \{0\} \rightarrow P(\vec{E}')$  be the two projections. A map  $g: P(\vec{E}) \rightarrow P(\vec{E}')$  such that there exists a linear isomorphism  $f: \vec{E} \rightarrow \vec{E}'$  with  $p' \circ f = g \circ p$  is called a *projective transformation*.

**Proposition 2.** *The set of projective transformations from  $P(\vec{E})$  to itself,  $PGL(\vec{E})$ , is a group under composition.*

*Proof.* From the definitions, the projective transformation that descends from identity map of  $\vec{E}$  forms the identity of the group. For any projective transformation  $g$  that descends from a linear isomorphism  $f$ , the transformation  $g'$  that descends from  $f^{-1}$  will act as its inverse. Since functional composition obeys associativity,  $PGL(\vec{E})$  is a group under composition. ■

### 5.1.3 Homogeneous Coordinates and Projective Frames

Given a basis of vector space  $\vec{E}$ , the vectors in  $\vec{E}$  can be described by their coordinates with respect to the basis.

**Definition 16.** A point  $m$  in  $P(\vec{E})$  can be described by the non-zero vector that generates the line  $m$ . In a  $n$ -dimensional projective space  $P(\vec{E})$ , the  $(n+1)$  tuples  $[x_1 : \cdots : x_{n+1}]$  and  $[x'_1 : \cdots : x'_{n+1}]$  represent the same point iff there exists a non-zero scalar  $\lambda$  such that  $x_i = \lambda x'_i$  for all  $i$ .

In a projective space  $P(\vec{E})$  with dimension  $n$ , we actually need  $n+2$  points to uniquely determine the basis of the underlying space  $\vec{E}$ , which will be proved in the next lemma. It will also justify the next definition.

**Definition 17.** If  $\vec{E}$  is a vector space of dimension  $n+1$ , a *projective frame* of  $P(\vec{E})$  is a set of  $n+2$  points  $(m_0, \dots, m_{n+1})$  such that  $m_1, \dots, m_{n+1}$  are the images of the vectors  $\vec{e}_1, \dots, \vec{e}_{n+1}$  in a basis of  $\vec{E}$ , and  $m_0$  is the image of  $\vec{e}_1 + \cdots + \vec{e}_{n+1}$ .

**Lemma 1.** *Let  $(m_0, \dots, m_{n+1})$  be a projective frame of  $P(\vec{E})$ . If the two bases of  $\vec{E}$   $(\vec{e}_1, \dots, \vec{e}_{n+1})$  and  $(\vec{e}'_1, \dots, \vec{e}'_{n+1})$  are such that  $p(\vec{e}_i) = p(\vec{e}'_i) = m_i$  and  $p(\vec{e}_1 + \cdots + \vec{e}_{n+1}) = p(\vec{e}'_1 + \cdots + \vec{e}'_{n+1}) = m_0$ , then they are proportional.*

*Proof.* Consider the points  $m_i$  of  $P(\vec{E})$ . Since the vectors  $\vec{e}_i$  and  $\vec{e}'_i$  both generate the line  $m_i$ ,  $\vec{e}_i = \lambda_i \vec{e}'_i$  for some non-zero  $\lambda_i$ . Using the  $(n+2)$ -th point, we can conclude that

$$(\vec{e}_1 + \cdots + \vec{e}_{n+1}) = \lambda(\vec{e}'_1 + \cdots + \vec{e}'_{n+1})$$

Thus,

$$\lambda_1 \vec{e}_1 + \cdots + \lambda_{n+1} \vec{e}_{n+1} = \lambda(\vec{e}_1 + \cdots + \vec{e}_{n+1})$$

As we are dealing with a basis,  $\lambda_i = \lambda$ . Thus two bases are proportional. ■

**Proposition 3.** *Let  $P(\vec{E})$  and  $P(\vec{E}')$  be two projective spaces of dimension  $n$ . Any projective mapping from  $P(\vec{E})$  to  $P(\vec{E}')$  maps a projective frame of  $P(\vec{E})$  onto a projective frame of  $P(\vec{E}')$ .*

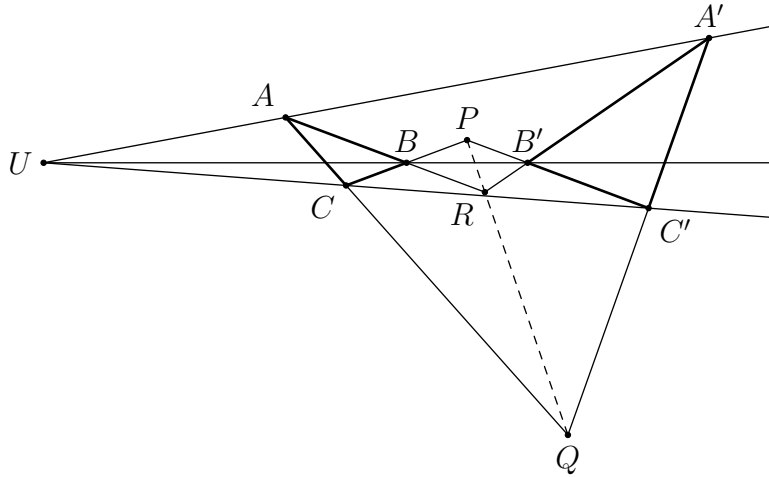
## 5.2 Fundamental Theorem of Projective Geometry

**Theorem 26** (Fundamental Theorem of Projective Geometry). *Let  $(a_1, \dots, a_{n+1})$  and  $(b_1, \dots, b_{n+1})$  be two sets of points in  $P(\mathbb{R}^n)$  such that none of the  $a_i$  and  $b_i$  belong to the projective subspace defined by  $n-1$  of the others in their respective sets. Then there exists a unique projective transformation  $f: P(\mathbb{R}^n) \rightarrow P(\mathbb{R}^n)$  such that,  $f(a_i) = b_i$  for all  $i = 1, \dots, n+1$ .*

*Proof.* The set of points  $(a_i)$  and  $(b_i)$  are both projective frames of  $P(\mathbb{R}^n)$ . Let  $(\vec{e}_1, \dots, \vec{e}_n)$ ,  $(\vec{e}'_1, \dots, \vec{e}'_n) \in \mathbb{R}^n$  be the basis that generate the frames  $(a_i)$  and  $(b_i)$  respectively. We know that there exists a unique isomorphism  $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$  such that  $f(\vec{e}_i) = \vec{e}'_i$ . The projective transformation  $g$  that descends from  $f$  will map the first frame to the second.

To prove the uniqueness: let  $f$  and  $f'$  two such projective transformations. The projective transformation  $g^{-1} \circ g'$  from  $P(\mathbb{R}^n)$  into itself keeps the frame invariant. Thus it is the identity transformation. ■

**Theorem 27** (Desargues' Theorem). *Let  $\triangle ABC$  and  $\triangle A'B'C'$  be triangles in  $\mathbb{R}^2$  such that the lines  $AA'$ ,  $BB'$ , and  $CC'$  meet at point  $U$ . Let  $BC$  and  $B'C'$  meet at  $P$ ,  $CA$  and  $C'A'$  at  $Q$ , and  $AB$  and  $A'B'$  at  $R$ . Then  $P$ ,  $Q$ , and  $R$  are collinear.*



**Figure 5.1 :** Desargues' Theorem

*Proof.* We will prove the theorem for the special case where  $A = [1 : 0 : 0]$ ,  $B = [0 : 1 : 0]$ ,  $C = [0 : 0 : 1]$ , and  $U = [1 : 1 : 1]$ . From the fundamental theorem of projective geometry, we know that it will be congruent to any other configuration. We can use the fact that projective congruence preserves projective properties, to deduce that the theorem holds in general.

The line  $AU$  has the equation  $y = z$ . Since  $A'$  lies on  $AU$ , it must have coordinates  $[a : b : b]$ , where  $b \neq 0$ , since  $A' \neq A$ . We can also write  $A' = [p : 1 : 1]$ , where  $p = a/b$ . Similarly,  $B' = [1 : q : 1]$ , and  $C' = [1 : 1 : r]$ .

Now to find the point  $P$ , we find the equation of the line  $BC$ .

$$\begin{vmatrix} x & y & z \\ 1 & q & 1 \\ 1 & 1 & r \end{vmatrix} = 0 \implies (qr - 1)x - (r - 1)y + (1 - q)z = 0$$

Substituting  $x = 0$  in the equation for the line  $B'C'$ , we get  $(r - 1)y = (1 - q)z$ , which implies  $P = [0 : 1 - q : r - 1]$ . Similarly we find that  $Q = [1 - p : 0 : r - 1]$ , and  $R = [1 - p : q - 1 : 0]$ .

To check the collinearity of  $P$ ,  $Q$ , and  $R$ :

$$\begin{vmatrix} 0 & 1 - q & r - 1 \\ 1 - p & 0 & r - 1 \\ 1 - p & q - 1 & 0 \end{vmatrix} = -(1 - q)(1 - p)(1 - r) + (r - 1)(1 - p)(q - 1) = 0$$

i.e  $P$ ,  $Q$ , and  $R$  are collinear. ■

**Proposition 4.** *There is a unique projective conic through any given set of five points, no three of which are collinear.*

*Proof.* By the fundamental theorem of projective geometry, there exists a projective transformation  $t$  which maps the four out of given five points to the points  $[1 : 0 : 0]$ ,  $[0 : 1 : 0]$ ,  $[0 : 0 : 1]$  and  $[1 : 1 : 1]$ . Let  $[a : b : c]$  be the image of the fifth point under  $t$ . Since projective transformations preserve collinearity, no three of the five points are collinear, and also it can be deduced that  $a$ ,  $b$  and  $c$  are non-zero, since if it were so, it would be collinear with other two points.

Let the conic that passes through these 5 points be of the form

$$Ax^2 + Bxy + Cy^2 + Fxz + Gyz + Hz^2$$

By substituting the points  $[1 : 0 : 0]$ ,  $[0 : 1 : 0]$ , and  $[0 : 0 : 1]$ , the equation can be reduced to the form

$$Bxy + Fxz + Gyz = 0$$

Since the projective conic also passes through  $[1 : 1 : 1]$  and  $[a : b : c]$ , we get the equations

$$B + F + G = 0$$

and

$$Bab + Fac + Gbc = 0$$

Solving these simultaneous equations, we get

$$F = -G \frac{ab - bc}{ab - ac}$$

and

$$B = -G \frac{ac - bc}{ac - ab}$$

It follows that the conic is of the form

$$-G \frac{ac - bc}{ac - ab} xy - G \frac{ab - bc}{ab - ac} xz + Gyz = 0$$

or

$$c(a - b)xy + b(c - a)xz + a(b - c)yz = 0$$

Since the conic is uniquely determined by the fifth point, it follows that it is unique. ■

**Remark. The Standard Projective Conic**

The projective conic  $E = \{[x : y : z] : xy + yz + zx = 0\}$  is called the standard projective conic. It passes through the triangle of reference formed by the points  $[1 : 0 : 0]$ ,  $[0 : 1 : 0]$ , and  $[0 : 0 : 1]$ . This fact can be used to simplify calculations involving projective conics.

All the points on the conic except than  $[1 : 0 : 0]$  can be parameterized as  $[t^2 + t : t + 1 : -t]$ , where  $t \in \mathbb{R}$ . All points on  $\vec{E}$  satisfy  $xy + yz + zx = 0$ . Suppose  $y \neq 0$ , let  $t = x/y$ . Then  $x = ty$ , and so

$$\begin{aligned} (ty)y + yz + z(ty) &= 0 \\ \implies ty + (t + 1)z &= 0 \\ \implies y = -\frac{t + 1}{t}z, x &= -(t + 1)z \end{aligned}$$

Thus the point has homogeneous coordinates  $[-(t + 1)z : -\frac{t+1}{t}z : z]$ , which can be rewritten in the form  $[t(t + 1) : t + 1 : -t]$ . This also happens to hold for the point  $[0 : 0 : 1]$ , where  $y = 0$ .

**Proposition 5.** *Let  $E_1$  and  $E_2$  be non-degenerate conics that pass through the points  $P_1, Q_1, R_1$  and  $P_2, Q_2, R_2$  respectively. Then there exists a projective transformation  $t$  which maps  $E_1$  to  $E_2$  such that  $t(P_1) = P_2$ ,  $t(Q_1) = Q_2$ , and  $t(R_1) = R_2$ .*

*Proof.* We prove this result by proving that for any conic  $E_1$ , there exists a transformation  $t_1$  which maps it to the standard conic  $xy + yz + zx = 0$  such that  $t_1(P_1) = [1 : 0 : 0]$ ,  $t_2(Q_1) = [0 : 1 : 0]$ , and  $t_3(R_1) = [0 : 0 : 1]$  for any  $P_1, Q_1, R_1 \in E$ .

Let  $f$  be a transformation that maps  $P_1$  to  $[1 : 0 : 0]$ ,  $Q_1$  to  $[0 : 1 : 0]$ , and  $R_1$  to  $[0 : 0 : 1]$ . It will map the conic  $E_1$  into a conic  $E'$  of the form

$$Fxy + Gyz + Hzy = 0$$

for some  $F, G, H \in \mathbb{R}$ . Divide the equation by  $FGH$  to rewrite  $E'$  in the form

$$\frac{xy}{GH} + \frac{yz}{FH} + \frac{zx}{FG} = 0$$

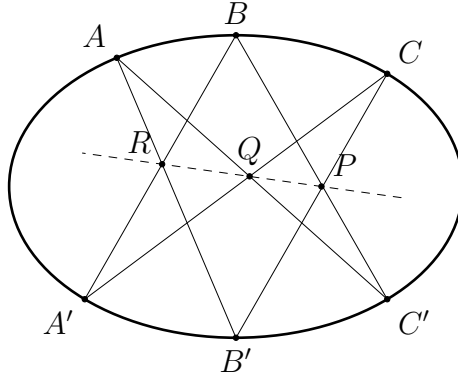
Now, let  $g$  be the transformation of the form  $g([x : y : z]) = A[x : y : z] \forall [x : y : z] \in \mathbb{P}(\mathbb{R}^3)$  where  $A$  is a  $3 \times 3$  matrix such that

$$A = \begin{bmatrix} \frac{1}{H} & 0 & 0 \\ 0 & \frac{1}{G} & 0 \\ 0 & 0 & \frac{1}{F} \end{bmatrix}$$

Then,  $g$  maps  $E'$  to the standard conic  $xy + yz + zx = 0$ , leaving  $P$ ,  $Q$ , and  $R$  unchanged. Let  $t_1 = g \circ f$ . Similarly, let  $t_2$  be the function that maps the conic  $E_2$  to the standard conic such that  $t_2(P_2) = [1 : 0 : 0]$ ,  $t_2(Q_2) = [0 : 1 : 0]$ , and  $t_2(R_2) = [0 : 0 : 1]$  for any  $P_2, Q_2, R_2 \in E_2$ .

The composite function  $t = t_2^{-1} \circ t_1$  maps  $E_1$  to  $E_2$  such that  $t(P_1) = P_2$ ,  $t(Q_1) = Q_2$ , and  $t(R_1) = R_2$ , as required. ■

**Theorem 28** (Pascal's Theorem). *Let  $A, B, C, A', B'$ , and  $C'$  be six distinct points on a non-degenerate projective conic. Let  $BC$  and  $B'C$  intersect at  $P$ ,  $CA'$  and  $C'A$  at  $Q$ , and  $AB'$  at  $R$ . The points  $P, Q$ , and  $R$  are collinear.*



**Figure 5.2 :** When the  $E$  is an ellipse.

*Proof.* We know that any non-degenerate conic can be transformed to the standard conic. Let the conic be in the standard form  $xy + yz + zx = 0$ , with  $A = [1 : 0 : 0]$ ,  $B = [0 : 1 : 0]$ , and  $C = [0 : 0 : 1]$ . Let the point  $A' = [a^2 + a : a + 1 : -a]$ ,  $B' = [b^2 + b : b + 1 : -b]$ , and  $C' = [c^2 + c : c + 1 : -c]$ , for some  $a, b, c \in \mathbb{R}$ .

The line  $BC'$  has the equation  $x = -(c + 1)z$ , and the line  $B'C$  has the equation  $x = by$ . The point  $P$  lies on both of these lines. Hence it has the homogeneous coordinates  $[b(c + 1) : c + 1 : -b]$ . Similarly,  $Q = [a(c + 1) : c + 1 : -c]$ , and  $R = [b(a + 1) : b + 1 : -b]$ .

To check their collinearity, evaluate the determinant:

$$\begin{vmatrix} b(c + 1) & c + 1 & -b \\ a(c + 1) & c + 1 & -c \\ b(a + 1) & b + 1 & -b \end{vmatrix}$$

Which, after some row operations, simplifies to be equal to 0. Hence, the points  $P, Q$ , and  $R$  are collinear. ■

Proof adapted from [BEG12].

### 5.3 Cross-Ratio

**Definition 18.** Let  $a, b, c$  and  $d$  be four points on a projective line  $D$ . There exists a unique map from  $D$  to  $K \cup \{\infty\}$  that maps  $a$  to  $\infty$ ,  $b$  to  $0$ , and  $c$  to  $1$ . The image of  $d$  under this projective mapping is called the *cross-ratio* of the points  $(a, b, c, d)$ , and denoted  $[a, b, c, d]$ .

**Proposition 6.** Let  $a_1, a_2, a_3$ , and  $a_4$  be four points on the line  $D$  (the first three being distinct) and  $a'_1, a'_2, a'_3$ , and  $a'_4$  be four points on another line  $D'$  (satisfying the same assumption). There exists a projective transformation  $f: D \rightarrow D'$  such that  $f(a_i) = a'_i$  iff  $[a_1, a_2, a_3, a_4] = [a'_1, a'_2, a'_3, a'_4]$ .

*Proof.* Assume  $f$  is a projective mapping that sends  $a_i$  to  $a'_i$ . Let  $g$  and  $g'$  be functions such that  $[a_1, a_2, a_3, a_4] = g(a_4)$ , and  $[a'_1, a'_2, a'_3, a'_4] = g'(a'_4)$ .  $g' \circ f$  is a function, which maps  $a_1$  to  $\infty$ ,  $a_2$  to  $0$ , and  $a_3$  to  $1$ . But such function is unique. Hence,  $g = g' \circ f$ , which implies that  $g(a_4) = g'(a'_4)$ . That is,

$$[a_1, a_2, a_3, a_4] = [a'_1, a'_2, a'_3, a'_4]$$

■

*Remark.* **Formulae for cross-ratio**

Let  $a, b$ , and  $c$  be four points on the affine line, the first three being distinct. Then

$$[a, b, c, d] = \frac{(d-b)(c-a)}{(d-a)(c-b)}$$

Also, since the points  $a$  and  $b$  are distinct,  $c$  and  $d$  can be written as

$$\begin{aligned} c &= \alpha a + \beta b \\ d &= \gamma a + \delta b \end{aligned}$$

Then the cross-ratio

$$[a, b, c, d] = \frac{\gamma\beta}{\alpha\delta}$$

**Proposition 7.** If  $a, b, c$ , and  $d$  are four distinct collinear points, then the following equalities hold:

$$\begin{aligned} [a, b, c, d] + [a, c, b, d] &= 1 \\ [b, a, c, d] &= [a, b, c, d]^{-1} \\ [a, b, d, c] &= [a, b, c, d]^{-1} \end{aligned}$$

*Proof.* Let  $f$  be the function that defines the cross-ratio, such that  $[a, b, c, d] = f(d)$ , and let  $f'$  be a function such that  $f'(x) = 1 - f(x) \forall x$ . The composite function  $f' \circ f$  maps  $a$  to  $\infty$ ,  $b$  to  $0$ , and  $c$  to  $1$ . But the function that defines the cross-ratio  $[a, c, b, d]$  also maps  $a$  to  $\infty$ ,  $b$  to  $0$ , and  $c$  to  $1$ . Since such function is unique,

$$\begin{aligned} [a, c, b, d] &= f' \circ f(d) \\ \implies [a, c, b, d] &= 1 - [a, b, c, d] \end{aligned}$$

Let  $g$  be a function such that  $g(x) = \frac{1}{f(x)} \forall x$ . The composite function  $g \circ f$  maps  $a$  to 0,  $b$  to  $\infty$ , and  $c$  to 1. Thus it is the function that defines the cross-ratio  $[b, a, c, d]$ . That is,

$$\begin{aligned} [b, a, c, d] &= g \circ f(d) \\ \implies [b, a, c, d] &= \frac{1}{f(d)} \\ &= [a, b, c, d]^{-1} \end{aligned}$$

Let  $h$  be a function such that  $h(x) = \frac{f(x)}{f(d)} \forall x$ . The composite function  $h \circ f$  maps  $d$  to 1, keeping the images of  $a$  and  $b$  unchanged. Hence, it is the defining function of the cross-ratio  $[a, b, d, c]$ . That is,

$$\begin{aligned} [a, b, d, c] &= h \circ f(c) \\ \implies [a, b, d, c] &= \frac{f(c)}{f(d)} \\ &= [a, b, c, d]^{-1} \end{aligned}$$

■

*Remark.* If  $[a, b, c, d] = k$ , the 24 cross-ratios obtained by permuting the four points take six values in general:

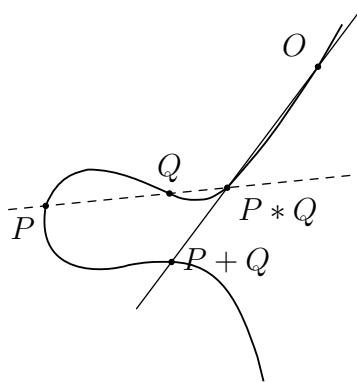
$$k, \quad \frac{1}{k}, \quad 1 - k, \quad 1 - \frac{1}{k}, \quad \frac{1}{1 - k}, \quad \frac{k}{k - 1}$$

## 5.4 Group Law on Cubics

Throughout this section, a projective cubic curve means a non-degenerate, non-singular, non-empty projective cubic curve (i.e. its points are solutions of a cubic polynomial in the coordinates) in a two dimensional projective space. The following proof is adapted from [ST15].

Given a projective cubic curve  $\mathcal{C}$  with a given point  $O$  on it. The addition law is defined as follows:

To add  $P$  and  $Q$ , take the third intersection point  $P * Q$ , join it to  $O$  by a line, and then take the third intersection point to be  $P + Q$ . In other words, set  $P + Q := O * (P * Q)$ . In case of  $P = Q$ , the line passing through  $P$  and  $Q$  is taken to be the tangent to  $\mathcal{C}$  at  $P$ .



**Figure 5.3 :** Group law for cubics

In short, we consider a point to intersect a line twice if it is tangent to the curve and thrice if the point is an inflection point.

Note that

$$P * Q = R \iff Q * R = P \iff R * P = Q$$

Now, we verify that the above addition rule with the set of points on  $\mathcal{C}$  does indeed form a group.

## Closure

First, we see that the set is closed under the operation  $*$ . From Bézout's theorem [ST15, Thm. A.1], we can say that given two points on  $\mathcal{C}$ , there is a third point that intersects with the curve and line through the previous point which proves  $\mathcal{C}$  is closed under  $*$ . Thus, for any two points  $P$  and  $Q$  that lie on  $\mathcal{C}$ ,  $P + Q := O * (P * Q)$  also lies on  $\mathcal{C}$ .

## Identity

For any  $P$ , we have

$$P + O = O * (O * P) = P$$

which shows that  $O$  is the identity element and it belongs to  $\mathcal{C}$ .

## Inverse

Let  $S := O * O$ . For any point  $Q$ , consider  $Q + (Q * S)$  as

$$Q + (Q * S) = O * (Q * (Q * S)) = O * S = O$$

$(Q * S)$  exists if  $S$  exists which is true due to Bézout's theorem [ST15, Thm. A.1]. If  $O$  is an inflection point, then  $S = O$ . Thus, the inverse of  $Q$  is  $(Q * S)$  which lies on  $\mathcal{C}$ .

## Associativity

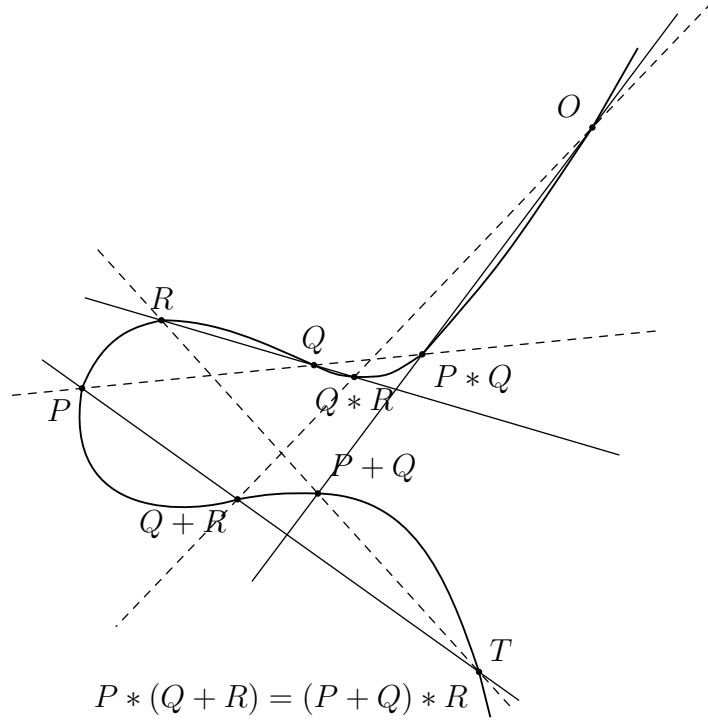
We define the following lines:

$l_1$ : Passes through $Q, R, Q * R$	$m_1$ : Passes through $P, Q, P * Q$
$l_2$ : Passes through $O, P * Q, P + Q$	$m_2$ : Passes through $O, Q * R, Q + R$
$l_3$ : Passes through $P, Q + R$	$m_3$ : Passes through $R, P + R$

Because the curve is in the projective plane, the point of intersection of lines  $l_3$  and  $m_3$  always exists; let that point be  $T$ . Now, we consider the cubic curve obtained by multiplying the equations of  $l_1, l_2$  and  $l_3$  as  $L$ . Similarly, we consider the curve obtained from  $m_1, m_2, m_3$  as  $M$ . They will meet at 9 points due to Bézout's theorem [ST15, Thm. A.1] which are:

$$O, P, Q, R, P * Q, Q * R, P + Q, Q + R, T$$





**Figure 5.4**

But we see that the cubic curve  $\mathcal{C}$  passes through all of these points except  $T$ . From the Cayley-Bacharach theorem [ST15, Thm. A.3], if two cubic curves  $L$  and  $M$  intersect at 9 points and another cubic curve  $\mathcal{C}$  passes through 8 of those points then it passes through the ninth point as well. Hence,  $T$  lies on  $\mathcal{C}$ .

Consider the points of intersection between  $\mathcal{C}$  and  $l_3$ .  $P$  and  $Q + R$  lie on both of them, thus the third point of intersection will be  $P * (Q + R)$ , which happens to be  $T$ .

Similarly, looking at the points of intersection between  $\mathcal{C}$  and  $m_3$ , we see that the point  $T$  also happens to be  $(P + Q) * R$ .

Because they are the same point, we have that:

$$(P + Q) * R = P * (Q + R)$$

From which we can conclude that

$$(P + Q) + R = P + (Q + R)$$

Thus, the points of  $\mathcal{C}$  form a group under the operation  $+$ .

# Bibliography

- [Art57] Emil Artin. *Geometric Algebra*. Interscience Publishers, Inc., 1957.
- [Aud02] Michéle Audin. *Geometry*. Universitext. Springer-Verlag, 2002.
- [BEG12] David A. Brannan, Matthew F. Esplen, and Jeremy J. Gray. *Geometry*. Cambridge University Press, second edition, 2012.
- [Ber87] Marcel Berger. *Geometry I*. Springer-Verlag Berlin Heidelberg, 1987.
- [DF04] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, third edition, 2004.
- [Shi09] Shailesh Shirali. Groups associated with conics. *The Mathematical Gazette*, March 2009.
- [ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer International Publishing Switzerland, second edition, 2015.