Geometry

Tejaswi

Advisor: Dr. Steven Spallone

Summer 2025

Contents

Chapter 1

Some Algebra

1.1 Groups and Fields

Chapter 2

Conics

2.1 Dandelin Spheres

Germinal Pierre Dendelin, a 19th century French-Belgian Professor, discovered this beautiful proof to demonstrate that any plane that cuts through a right circular cone produces a quadratic curve.

Theorem. *When a plane intersects a right circular cone, the curve produced will either be an ellipse, a parabola or a hyperbola.*

Proof. Place a sphere tangent to the intersecting plane π and the cone such that it touches the plane at F, and the cone in a circle C with centre O that lies on a horizontal plane ϵ [1].

Take an aribtrary point P on the curve Q, and extend the line VP from the vertex V of the cone to meet C at point L. Let D be the point on the intersection on the planes π and ϵ such that PD is perpendicular to the line of intersection.(If the planes do not intersect, Q will be a circle)

[1] Assuming that there exists atleast one such sphere

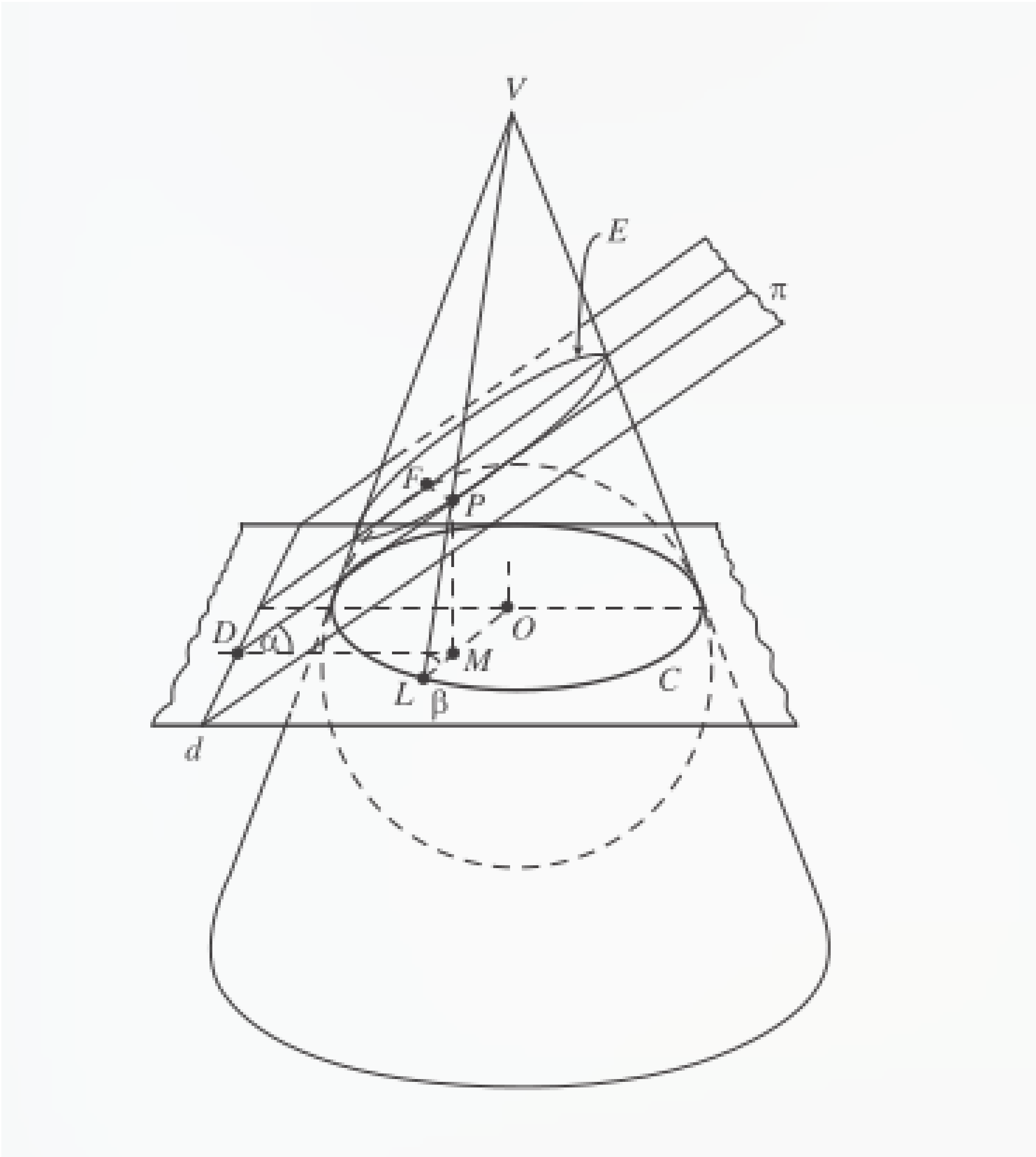

Figure 2.1: When $0 < \alpha < \beta < \frac{\pi}{2}$

Drop a perpendicular PM on OL such that $\triangle PML$ and $\triangle PMD$ are both right angled. Denote $\angle PLM$ as α, and $\angle PDM$ as β.
From the triangles $\triangle PML$ and $\triangle PMD$

$$\begin{aligned} \sin\alpha &= \frac{PM}{PD} \\ \text{and} \quad \sin\beta &= \frac{PM}{PL} \\ \text{i.e.} \quad \frac{PL}{PD} &= \frac{\sin\alpha}{\sin\beta} \end{aligned}$$

Since PL and PF are both tangents from P to the sphere, $PF = PL$. Therfore,

$$\frac{PF}{PD} = \frac{\sin\alpha}{\sin\beta}$$

i.e. $PF = e \cdot PD$, where $e = \sin\alpha / \sin\beta$
It follows from the focus - directrix definition that Q will be an ellipse if $\alpha < \beta$, a parabola if $\alpha = \beta$, or a hyperbola if $\alpha > \beta$. □

2.2 Group Laws on Conics

Consider a conic section C and a point $O \in C$ For any $P, Q \in C$,define a binary operation $\oplus : C \times C \to C$ by $P \oplus Q = R$, where R is such that $l_{PQ} \| l_{OR}$.

Theorem. *Set of points of C forms a group $G(C)$ under the binary operation $\oplus$, with O as the identity element.*

Proof. **Closure:** The line through O parallel to l_{PQ} necessarily meets C again,(counting algebraic multiplicities) since for any quadratic equation with real coeffecient, if one of the roots is real, the other one must be real too.

Existence of Identity Element: The point O serves as the identity element.

Existence of Inverse: Constructively, when Q is such that the line parellel to l_{PQ} that passes through O is tangent to the conic, i.e when $R = O$, we get $P \oplus Q = O$. So, Q serves as the inverse of P.

Associativity: To prove associativity, we'll find algebraic formula for $P \oplus Q$ for standard conics. In the next chapter, we'll prove that any ellipse, hyperbola or parabola is affine congruent to its standard form. This result will generalize the reault to all conics. The following formulae will be valid for any fields with non-two charecteristic.

Let the point P be (p_1, p_2), Q be (q_1, q_2), O be (o_1, o_2), and R be (r_1, r_2), and let the slope of the line l_{PQ} be $\lambda = q_2 - p_2 / q_1 - p_1$, assuming $P \neq Q$, since associativity would be trivial then. Let ℓ be the line through O with slope λ. The coordinates of R will satisfy $\lambda = \frac{r_2 - o_2}{r_1 - o_2} = \frac{q_2 - p_2}{q_1 - p_1}, \Rightarrow r_2 = o_2 + \mu(q_2 - p_2)$ and $r_1 = o_1 + \mu(q_1 - p_1)$ for some $\mu \in \mathbb{F}$.

(i) **Circle**
Without the loss of generality, let $O = (1, 0)$. Since R also lies on C, $r_1^2 + r_2^2 = 1$. i.e.

$$\begin{aligned}
& (1 + \mu(q_1 - p_1))^2 + (0 + \mu(q_2 - p_2))^2 = 1 \\
\Rightarrow \quad & \mu(\mu(q_1 - p_1)^2 + \mu(q_2 - p_2)^2 + 2(q_1 - p_1)) = 0 \\
\Rightarrow \quad & \mu = 0 \text{ or } \mu = -\frac{2(q_1 - p_1)}{(q_1 - p_1)^2 + (q_2 - p_2)^2}
\end{aligned}$$

We assume that $(q_1 - p_1)^2 + (q_2 - p_2)^2 \neq 0$. Because if it was so,

$$\begin{aligned}
& q_1^2 + p_1^2 - 2q_1p_1 + q_2^2 + p_2^2 - 2p_2q_2 = 0 \\
\Rightarrow \quad & 1 - p_1q_1 - p_2q_2 = 0 \\
\Rightarrow \quad & p_1^2q_1^2 = 1 + p_2^2q_2^2 - 2p_2q_2 \\
\Rightarrow \quad & p_1^2q_1^2 = 1 + (1 - p_1^2)(1 - q_1^2) - 2p_2q_2 \\
\Rightarrow \quad & 0 = 2 - p_1^2 - q_1^2 - 2p_2q_2 \\
\Rightarrow \quad & (p_2 - q_2)^2 = 0 \\
\Rightarrow \quad & p_2 = q_2 \text{ and similarly, } p_1 = q_1
\end{aligned}$$

Which is when $P = Q$, which we have assummed not to be true.

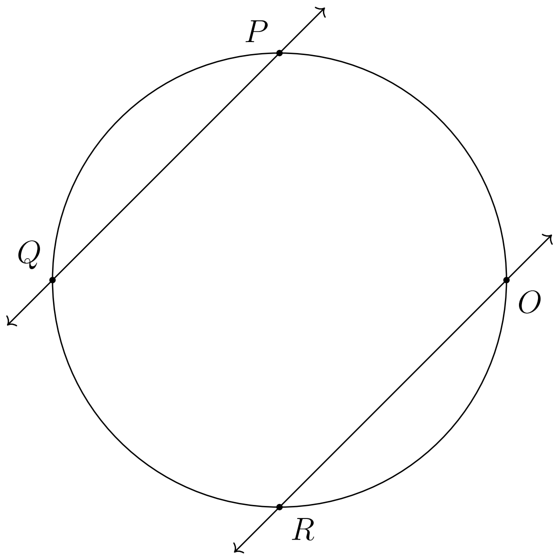

Figure 2.2: $R = P \oplus Q$ when C is a circle.

The $\mu = 0$ solution corresponds to O. Considering the other solution,

$$\begin{aligned}
r_1 &= 1 - \frac{2(q_1 - p_1)^2}{(q_1 - p_1)^2 + (q_2 - p_2)^2} \\
&= \frac{(q_2 - p_2)^2 - (q_1 - p_1)^2}{(q_1 - p_1)^2 + (q_2 - p_2)^2} \\
&= \frac{q_2^2 + p_2^2 - 2p_2q_2 - q_1^2 - p_1^2 + 2p_1q_1}{2(1 - p_1q_1 - p_2q_2)} \\
&= \frac{1 - p_1^2 - q_1^2 + p_1q_1 - p_2q_2}{1 - p_1q_1 - p_2q_2} \\
&= \frac{(p_1q_1 - p_2q_2)(1 - p_1q_1 - p_2q_2)}{1 - p_1q_1 - p_2q_2} \\
&= p_1q_1 - p_2q_2 \\
\text{and, } r_2 &= -\frac{2(q_1 - p_1)(q_2 - p_2)}{(q_1 - p_1)^2 + (q_2 - p_2)^2} \\
&= \frac{p_2q_2 + p_2q_1 - p_1p_2 - q_1q_2}{1 - p_1q_1 - p_2q_2} \\
&= \frac{(p_1q_2 + p_2q_1)(1 - p_1q_1 - p_2q_2)}{1 - p_1q_1 - p_2q_2} \\
&= p_1q_2 + p_2q_1
\end{aligned}$$

$$\Rightarrow R = P \oplus Q = (r_1, r_2) = (p_1q_1 - p_2q_2, p_1q_2 + p_2q_1)$$

Using this formula, it can be proved that $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

(ii) **Parabola**

Without the loss of generality, let $O = (0, 0)$. The points of the standard parabloa can be parameterized as (t, t^2). Let $P = (p, p^2)$, $Q = (q, q^2)$, and $R = (r, r^2)$. Substituting these in λ,

$$\begin{aligned}\lambda &= \frac{r^2}{r} = \frac{q^2 - p^2}{q - p} \Rightarrow r = p + q \\ &\Rightarrow P \oplus Q = (p + q, (p + q)^2)\end{aligned}$$

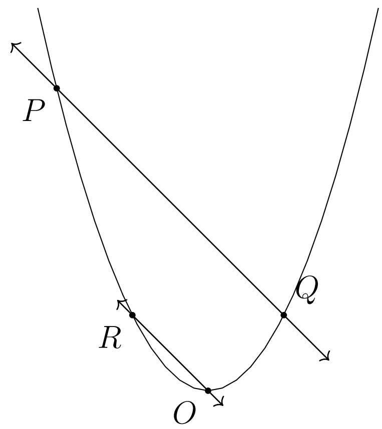

Figure 2.3: $R = P \oplus Q$ when C is a parabola.

Since the parameters just get added, it can be easily proved that
$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$

(iii) **Hyperbola**

Without the loss of generality, let $O = (1, 1)$.The points of the standard hyperbola can be parameterized as $(t, \frac{1}{t})$. Let $P = (p, \frac{w}{p})$, $Q = (q, \frac{1}{q})$, and $R = (r, \frac{1}{r})$. Substituting these in λ,

$$\begin{aligned}\lambda &= \frac{\frac{1}{r} - 1}{r - 1} = \frac{\frac{1}{q} - \frac{1}{p}}{p - q} \Rightarrow r = pq \\ &\Rightarrow P \oplus Q = (pq, \frac{1}{pq})\end{aligned}$$

Since parameters just get multiplied, it can be easily proved that
$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$

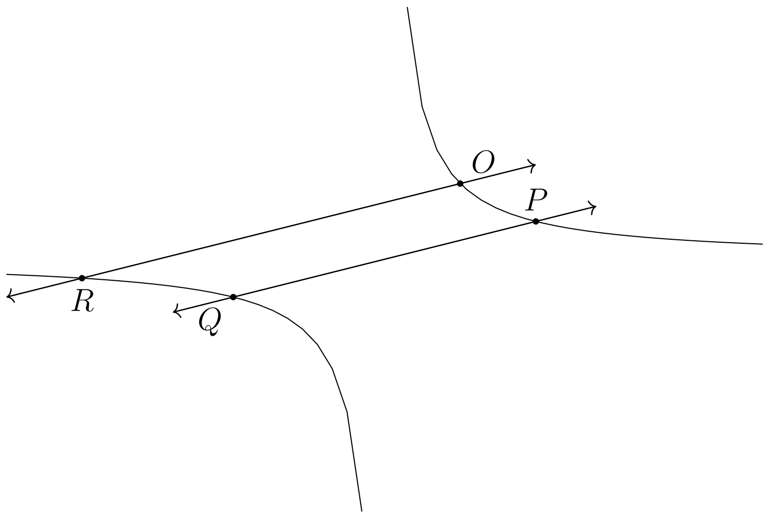

Figure 2.4: $R = P \oplus Q$ when C is a hyperbola.

$\square$

Group laws also hold with a simiilarly defined operation $\oplus$ for elliptic curves, which have notable applications in cryptography.

2.3 Generating solutions for algebraic equations

Chapter 3

Affine Geometry

3.1 Affine Space

A set ε is endowed with the structure of an affine space by a vector space E and a mapping Θ that associates a vector of E with any ordered pair of points in ε,

$$\begin{array}{rcl} \varepsilon \times \varepsilon & \longrightarrow & E \\ (A, B) & \longmapsto & \overrightarrow{AB} \end{array}$$

such that:

- for any point A of ε, the partial map $\Theta_A : B \mapsto \overrightarrow{AB}$ is a bijection from ε to E.

- for any points A, B, and C in ε, we have $\overrightarrow{AB} = \overrightarrow{AC} + \overrightarrow{CB}$.

The vector space E is the direction of ε, or its underlying vector space. The elements of ε are called points, and the dimension of the vector space E is called the dimension of ε.
Some textbooks also define Affine spaces using invertible linear transformations.

Chapter 4

Projective Geometry

4.1 Projective Space