Projective Geometry

August 17, 2025

Contents

Chapter 1

Conics

Definition. A conic section, a conic, or a quadratic curve is a curve obtained from a cone's surface intersecting a plane.

1.1 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 1.1. *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.

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)

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 $\triangle PMD$

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

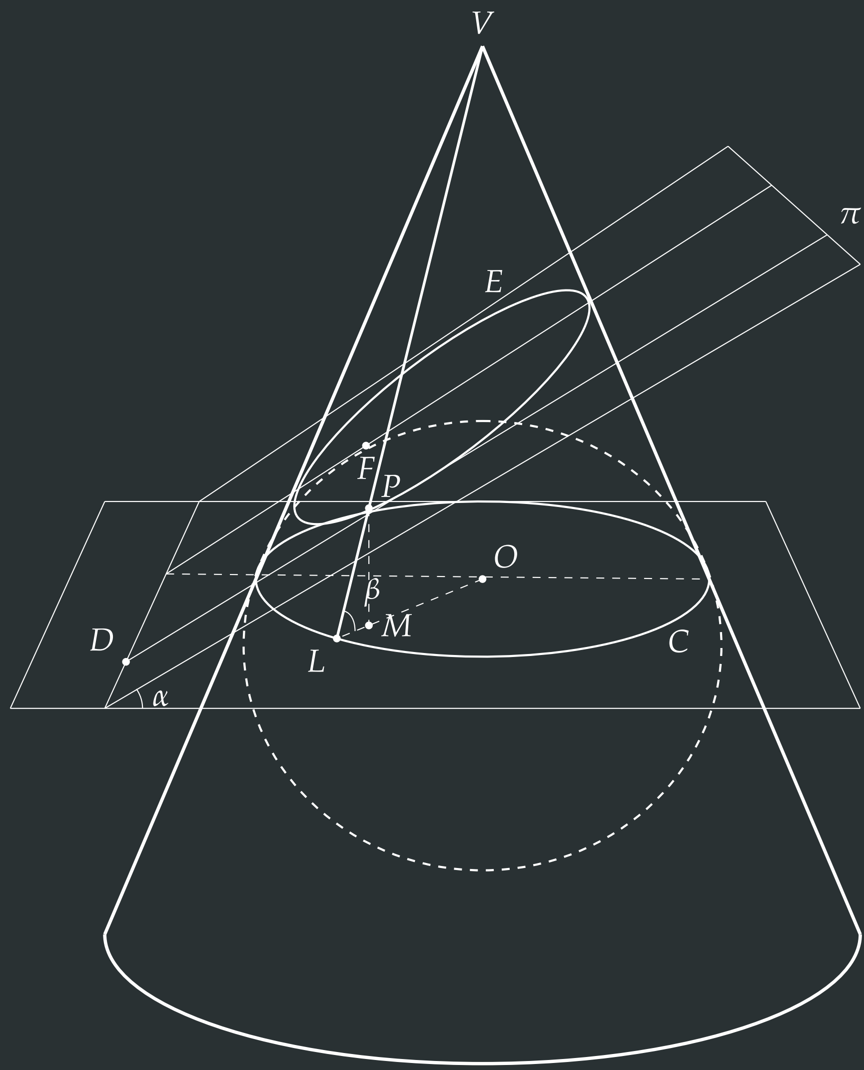

Figure 1.1: When $0 < \alpha < \beta < \frac{\pi}{2}$.

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 $\alpha > \beta$. ■

Proof adapted from [BEG12] with modifications to generalize it for all conics.

1.2 Group Laws on Conics

Consider a conic section $C : \{f(x) = 0, f(x) \in \mathbb{F}[x]\}$, where $deg(f(x)) = 2$, and $ch(\mathbb{F}) \neq 2$, 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 1.2. *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 coeffecients, 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, i.e for the circle $x^2 + y^2 = 1$, for the parabloa $y = x^2$, and for the hyperbola $xy = 1$. In chapter **??**, we'll prove that any ellipse, hyperbola or parabola is affine congruent to its standard form. This result will generalize the result 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 loss of generality, let $O = (1, 0)$. Since R also lies on C, $r_1^2 + r_2^2 = 1$. i.e.

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

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

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

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

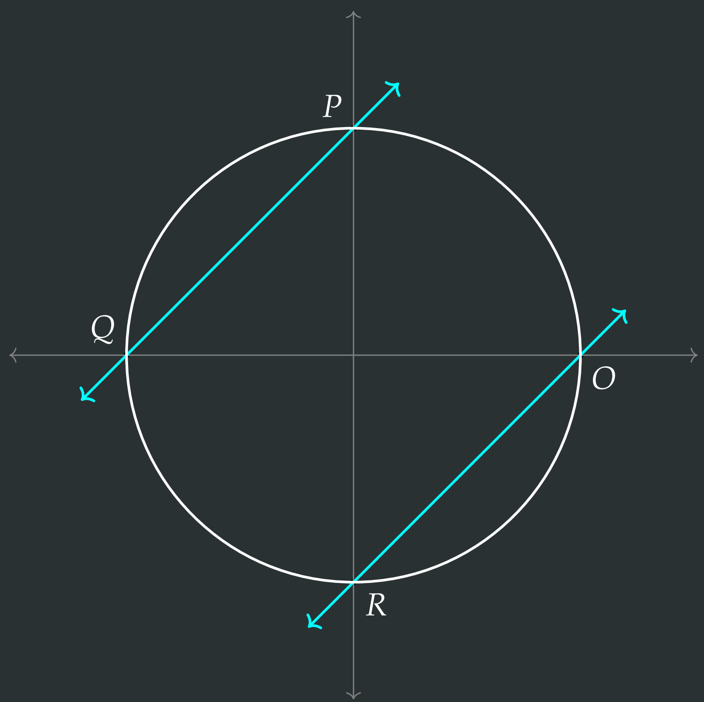

Figure 1.2: $R = P \oplus Q$ when C is a circle.

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

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

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

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

(ii) **Parabola**
Without 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,

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

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

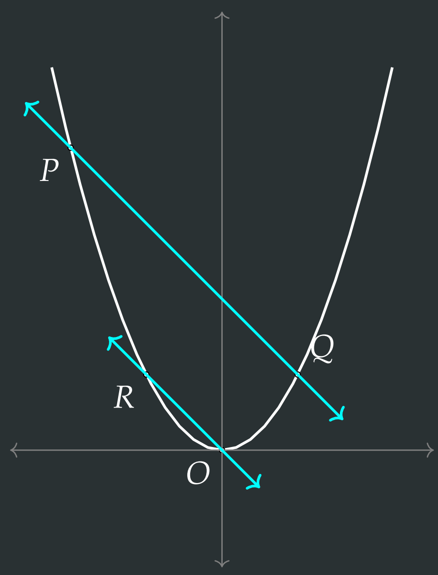

Figure 1.3: $R = P \oplus Q$ when C is the standard parabola.

(iii) **Hyperbola**
Without 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,

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

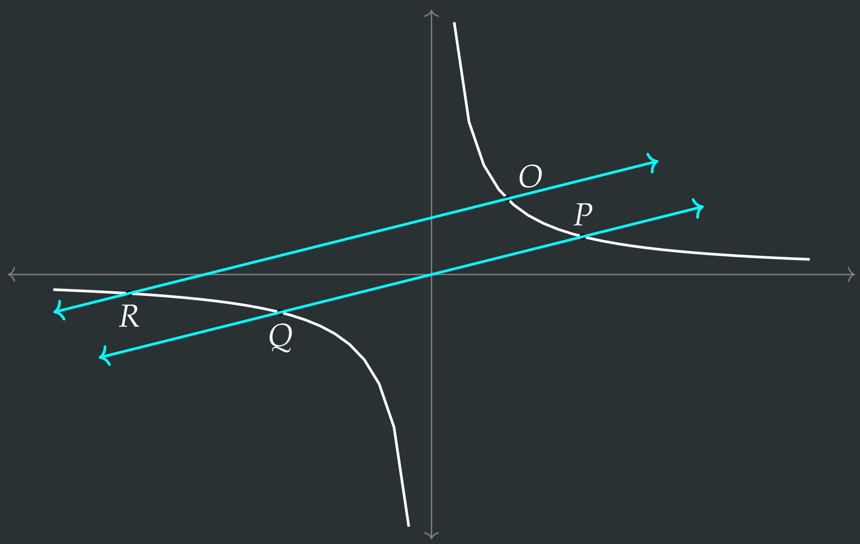

Figure 1.4: $R = P \oplus Q$ when C is the standard hyperbola.

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

■

Proof adapted from [Shi09] with a formula based field independent proof for associativity.

Remark. It can also be proved that the group $\langle C, \oplus \rangle$ is isomorphic to some other well known groups in each case:

- When C is an ellipse, $\langle C, \oplus \rangle \cong \langle S^1, \cdot \rangle$, where $S^1 = \{e^{i\theta} \in \mathbb{C} : \theta \in [0, 2\pi)\}$.
- When C is a parabola, $\langle C, \oplus \rangle \cong \langle \mathbb{R}, + \rangle$.
- When C is a hyperbola, $\langle C, \oplus \rangle \cong \langle \mathbb{R}^\times, \cdot \rangle$.

1.3 Generating Solutions for Diophantine Equations

Consider the conic $C = \{(x, y) \in \mathbb{Q} | x^2 + y^2 = 1\}$, and $P = (1, 0) \in C$. Let l_m be the line with slope $m \in Q$, passing through P and another point $Q = (x, y) \in C$. The coorrdinates of Q can be found by substituting $y = m(x - 1)$.

$$x^2 + m^2(x - 1)^2 - 1 = (1 + m^2)x^2 - 2m^2x - (1 - m^2) = 0$$

using the quadratic formula,

$$x = \frac{m^2 \pm 1}{1 + m^2}$$

using the non-trivial solution, we get $x = \frac{m^2-1}{m^2+1}$ and $y = \frac{-2m}{m^2+1}$. substiting these values in the equation for the conic,

$$(\frac{m^2 - 1}{m^2 + 1})^2 + (\frac{-2m}{m^2 + 1})^2 = 1$$
$$\implies (m^2 - 1)^2 + (2m)^2 = (m^2 + 1)^2$$

This equation will produce integer solutions for $x^2 + y^2 = 1$, though not all of them. Similarly rational or integer solutions for any equations of the form $ax^2 + by^2 = c$, where $a, b, c \in Q$.

Chapter 2

Projective Geometry

2.1 The Projective Space

2.1.1 Projective Spaces

Definition. Let E be a finite dimwnsional vector space. The *projective space* $P(E)$ deduced from E is the set of all 1 dimensional linear subspaces of E. [Aud02]

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

2.1.2 Projective Subspaces

A subset V of $P(E)$ is a projective subspace if it is an image of a nonzero vector subspace F of E.

Proposition 2.1. *Let V and W be two projective subspaces of $P(E)$.*

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

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

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

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

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

Therefore,

$$\dim (F \cap G) \geq 1$$

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

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

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

■

2.1.3 Projective Transformations

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

Proposition 2.2. *The set of projective transformations from $P(E)$ to itself, $PGL(E)$, is a group under composition.*

Proof. From the definitions, the projective transformation that descends from identity map of E forms the identity of the group. For any projective tranformation 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, $PGL(E)$ is a group. ■

2.1.4 Homogeneous Coordinates and Projective Frames

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

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

Remark. Usually, the coordinates for projective spaces are represented as $[x_1 : \ldots : x_{n+1}]$

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

Definition. If E is a vector space of dimension $n+1$, a *projective frame* of $P(E)$ is a set of $n+2$ points $(m_0, \ldots, m_{n+1})$ such that $m_1, \ldots, m_{n+1}$ are the images of the vectors $e_1, \ldots, e_{n+1}$ in a basis of E, and m_0 is the image of $e_1 + \cdots + e_{n+1}$.

Lemma 2.1. *Let $(m_0, \ldots, m_{n+1})$ be a projective frame of $P(E)$. If the two bases of E $(e_1, \ldots, e_{n+1})$ and $(e'_1, \ldots, e'_{n+1})$ are such that $p(e_i) = p(e'_i) = m_i$ and $p(e_1 + \cdots + e_{n+1}) = p(e'_1 + \cdots + e'_{n+1}) = m_0$, then they are proportional.*

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

$$(e_1 + \cdots + e_{n+1}) = \lambda(e'_1 + \cdots + e'_{n+1})$$

Thus,

$$\lambda_1 e_1 + \cdots + \lambda_{n+1} e_{n+1} = \lambda(e_1 + \cdots + e_{n+1})$$

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

2.2 Fundamental Theorem of Projective Geometry

Theorem 2.1 (Fundamental Theorem of Projective Geometry)**.** *Let $(a_1, \ldots, a_{n+2})$ and $(b_1, \ldots, b_{n+2})$ be two sets of points in $\mathbb{RP}^n$ such that none of the a_i and b_i belong to the projective subspace defined by n of the others in their respective sets. Then there exists a unique projective transformation $f : \mathbb{RP}^n \to \mathbb{RP}^n$ such that, $f(a_i) = b_i$ for all $i = 1, \ldots, n+2$.*

Proof. The set of points (a_i) and (b_i) are both projective frames of $\mathbb{R}\mathrm{Pr}^n$. Let $(e_1, \ldots, e_{n+1}), (e'_1, \ldots, e'_{n+1}) \in \mathbb{R}^{n+1}$ be the basis that generate the frames (a_i) and (b_i) respectively. We know that there exists a unique isomorphism $f : \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ such that $f(e_i) = e'_i$. 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 projcetive transformations. The projective transormation $g^{-1} \circ g'$ from $\mathbb{R}\mathrm{Pr}^n$ into itself keeps the frame invariant. Thus it is the identity transformation. ∎

Theorem 2.2 (Desargues's 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 colinear.*

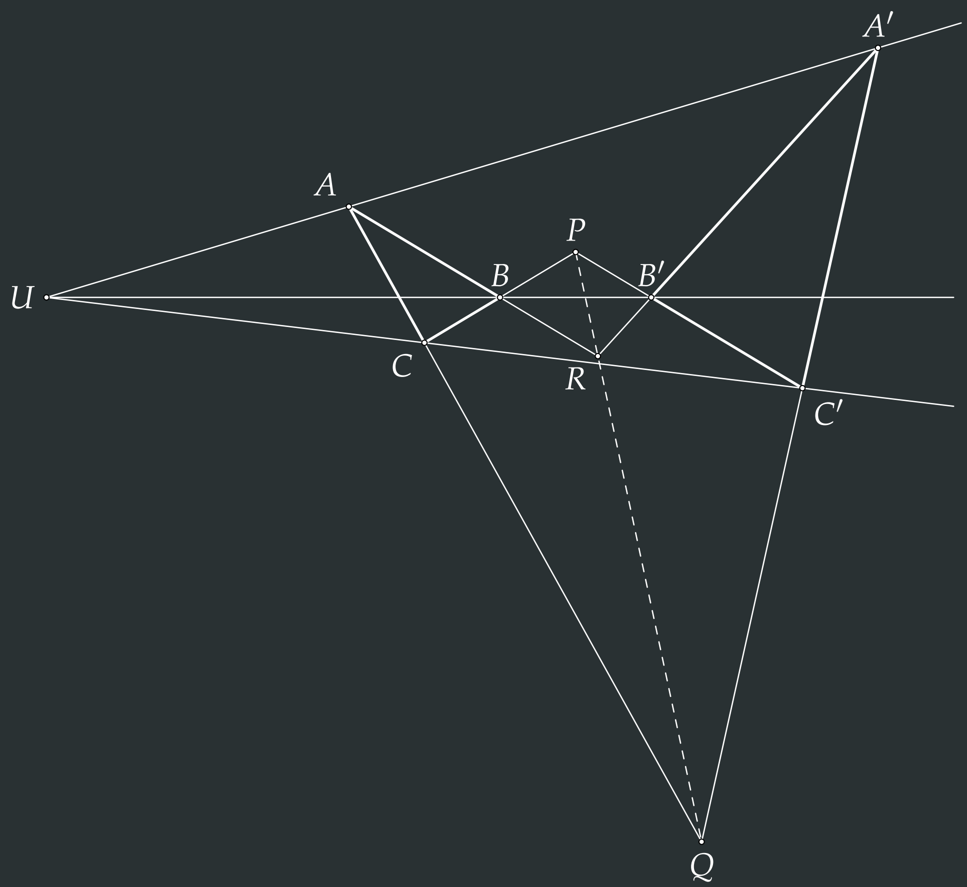

Figure 2.1: P, Q, and R are collinear.

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 projrctive 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 wirte $A' = [p : 1 : 1]$, where $p = a/b$. Similary, $B' = [1 : q : 1]$, and $C' = [1 : 1 : r]$.

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

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

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

To check the colinearity of P, Q, and R:

$$\begin{vmatrix} 0 & 1-q & r-1 \\ 1-p & 0 & r-1 \\ 1-p & q-1 & 0 \end{vmatrix}$$

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

i.e P, Q, and R are colinear. ■

Proposition 2.3. *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 nonzero, 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 porjective concic 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 traingle 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 projcetive 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 E satisfy $xy+yz+zx=0$. Suppose $y\neq 0$, let $t=x/y$. Then $x=ty$, and so

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

Thus the point has homogeneous coordinates $\left[-(t+1)z:-\frac{t+1}{t}z:z\right]$, 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 2.4. *Let E_1 and E_2 be non-degenrate conics that pass through the points P_1, Q_1, R_1 and P_2, Q_2, R_2 respectively. THen ther 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 transormation 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 $g([x : y : z]) = A[x : y : z] \forall [x : y : z] \in \mathbb{R}\,\mathrm{Pr}^3$ where A is a 3×3 matrix such that

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

Then, g maps E' to the standrd 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 2.3 (Pascal's Theorem)**.** *Let A, B, C, A', B', and C' be six distinct points on a non-degenrate 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.*

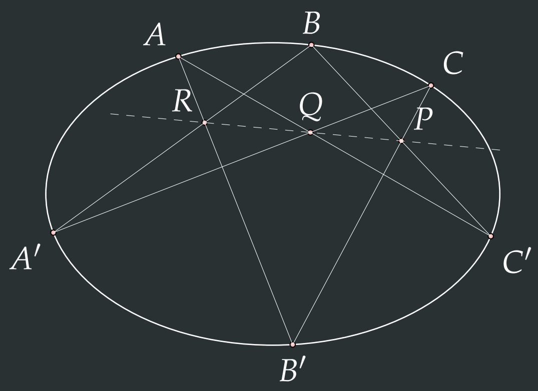

Figure 2.2: When the E is an ellipse.

Proof. We know that any non-degenerate conic can pe 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. ∎

Proofs adapted from [BEG12].

2.3 The Cross-Ratio

Definition. Let a, b, c and d be four points on a projective line D. There exists a unique map $g : D \to K \cup \{\infty\}$ that maps a to ∞, 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 2.5. *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 $f : D \to D'$ 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 ∞, 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. **Formulas 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 2.6. *If a, b, c, and d are four collinear distinct points, then the folloeing 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 ∞, b to 0, and c to 1. But the function that defines the cross-ratio $[a, c, b, d]$ also maps a to ∞, 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 ∞, 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 th eimages 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 the general six values:

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

2.4 Elliptic Curves

Definition. An elliptic curve is a non-empty, non-singular, degree 3 projective curve.

2.4.1 Weierstrass Standard Form

The general equation for a cubic curve C is,

$$
ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0
$$

with atleast one of a, b, c, or d nonzero. Assume that the underlying field is not of charectestic 2 or 3.

If C is nonsingular, it can be proved that it can be projectively transformed into the *Weirestrass form*:

$$
y^2 = x^3 + Ax + B
$$

given, $4A^3 + 27B^2 \neq 0$. It can also be proved that the point at infinity, usually taken as O, is an inflection point. That is, $I_O(l, C) = 3$, where l is the tangent at infinity.

2.4.2 Group Laws on Ellpitic Curves

Similar to the group laws defined for conics in Chapter 1, group law can also be defined on elliptic curves.

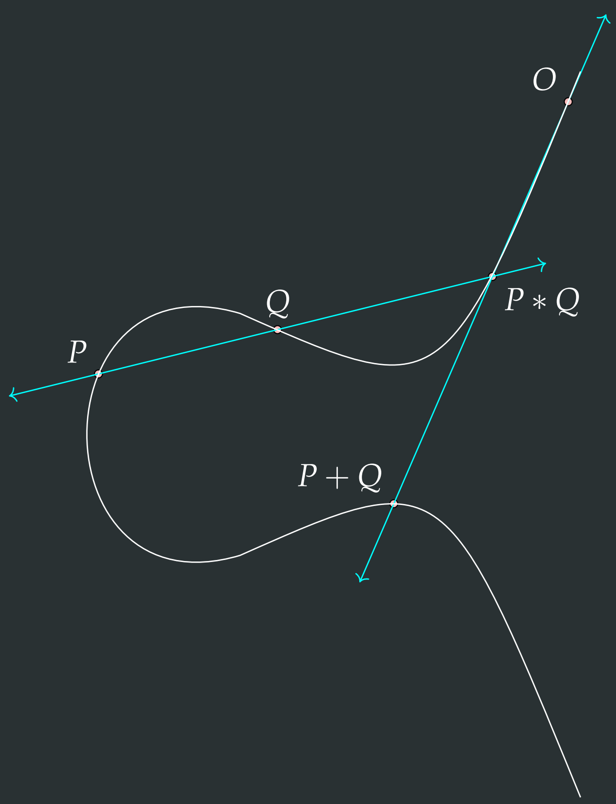

Figure 2.3: Addition Law

Bibliography

[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.

[Shi09] Shailesh Shirali. Groups Associated with Conics. *The Mathematical Gazette*, March 2009.