Projective Geometry

Tejaswi

Advisor: Dr. Steven Spallone

Summer 2025

Contents

Chapter 1

Basic Algebra

1.1 Groups, Rings and Fields

1.1.1 Groups

Definition. A *group* is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

(i) $(a * b) * c = a * (b * c) \forall a, b \in G$,

(ii) $\exists e \in G$, called identity of G, such that $\forall a \in G$ we have $a * e = e * a = a$,

(iii) for each $a \in G$, $\exists a^{-1} \in G$, called inverse of a, such that $a * a^{-1} = a^{-1} * a = e$,

The group is called abelian is $a * b = b * a \forall a, b \in G$. [DF04]

Ex. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are groups under $+$ with $e = 0$, and $a^{-1} = -a$ for all a, and $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, and $\mathbb{C} - \{0\}$ are groups under $\times$ with $e = 1$ and $a^{-1} = \frac{1}{a}$ for all a.

Remark. If G is a group under the opertaion $*$, then

1. the identity of G is unique,

2. for each $a \in G$, a^{-1} is uniquely determined,

3. $(a^{-1})^{-1} = a$ for all $a \in G$,

4. $(a * b)^{-1} = b^{-1} * a^{-1}$,

5. for any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 * a_2 * \ldots * a_n$ is independent of how the expression is bracketed,

6. if $a * u = a * v$, then $u = v$, and if $u * b = v * b$, then $u = v$.

Definition. Let $(G, *)$ and $(H, \diamond)$ be groups. A map $\phi : G \to H$ such that $\phi(x * y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$ is called a *homomorphism.* The map is called an *isomorphism* and G and H are said to be *isomorphic*, written $G \cong H$, if ϕ is a bijective homomorphism. [DF04]

Ex. For any group G, $G \cong G$. The identity map provides an obviuos isomorphism.
- The exponentiation map $exp : \mathbb{R} \to \mathbb{R}^+$ defined by $exp(x) = e^x$, is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

1.1.2 Fields

Definition. A *field* is a set F together with two binary operations $+$ and $\times$ such that $(F, +)$ is an abelian group and $(F - \{0\}, \times)$ is also an an abelian group, and the following distribution law holds: $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in F$. [DF04]

Ex. With usual addition and multiplication, $\mathbb{Q}$ and $\mathbb{R}$ are fields.
- $\mathbb{Z}/p\mathbb{Z}$, where p is a prime, with modular addition and multiplication, is a finite field.

Remark. For any field F if $|F| < \infty$, then $|F| = p^m$ for some prime p and some interger m.

Definition. The *charfecteristic* of a field F, denoted by $ch(F)$, is defined to be the smallest positive integer p such that $p \cdot 1_F = 0$ if such p exists, and defined to be zero otherwise. [DF04]

Remark. The charecteristic of a field F, $ch(F)$, is either 0 or a prime p.

1.1.3 Rings

Definition. A *ring* R is a set together with two binary operations $+$ and $\times$ satisfying the following axioms

(i) $(R, +)$ is an abelian group,

(ii) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

(iii) the distributive laws hold in R: for all $a, b, c \in R$, $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$

The ring R is coommutative if R is commutative. R is said to have an identity if there is an element $1 \in R$ with $1 \times a = a \times 1$ for all $a \in R$. [DF04]

Ex. All fields are obviously rings.
- The simplest rings are *trivial rings*, obtained by taking R to be any abelian group and defining multiplication $\times$ on R by $a \times b = 0$ for all $(a, b) \in R$. *trivial rings* are also commutative, as obviuos from the definition.
- The ring of integers $\mathbb{Z}$ - under usual addition and multiplication is a commutative ring with identity 1.

1.2 Field Extensions

Definition. If K is a field containing the subfield F, then K is said to be an *extension* of F, denoted K/F. The field F is sometimes called the base field of the extension. [DF04]

Definition. The *prime subfield* of a field F is the subfield of F generated by its multiplicative identity 1_F. It is isomorphic to either $\mathbb{Q}$(if $ch(F) = 0$), or to $\mathbb{F}_p$(if $ch(F) = p$). [DF04]

Remark. Every field F is an extension of its prime subfield.

Definition. The *degree* of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F. [DF04]

An important class of field extensions are those obtained by trying to solve equations over a field F. Famously, Gauss extended $\mathbb{R}$ in an attempt to solve the equation $x^2 + 1 = 0$. The new field generated by adjoining the roots of the equation i and $-i$ to $\mathbb{R}$ is $\mathbb{C}$. Given any field F and a polynomial $p(x) \in F[x]$, one can similarly extend it to form a field K, containing solution to the equation $p(x) = 0$.

Chapter 2

Conics

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

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, assuming such sphere exists.

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 $\triangle PMD$

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

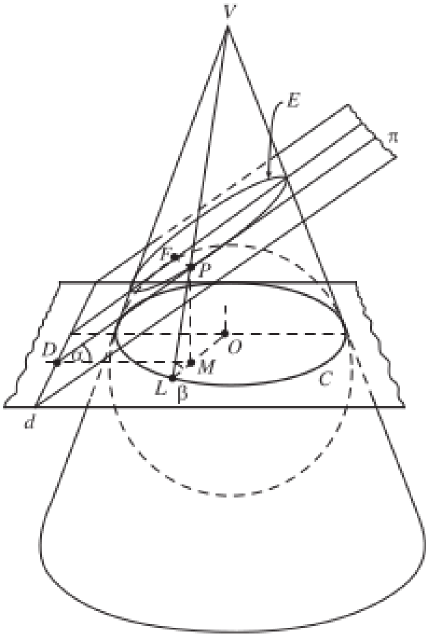

Figure 2.1: When $0 < \alpha < \beta < \frac{\pi}{2}$. Figure from [BEG12]

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.

2.2 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. *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 3, 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.

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

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

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

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

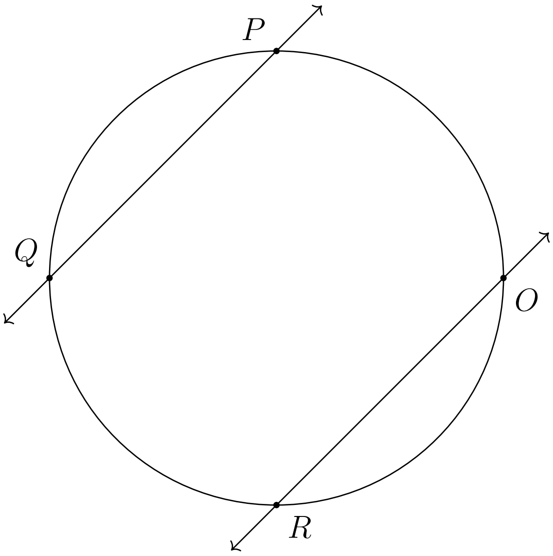

Figure 2.2: $R = P \oplus Q$ when C is a circle.

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

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

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

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
$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$

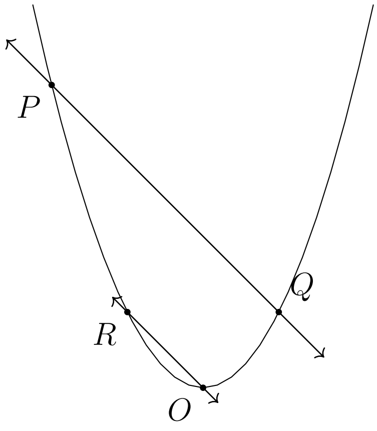

Figure 2.3: $R = P \oplus Q$ when C is a parabola.

(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,

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

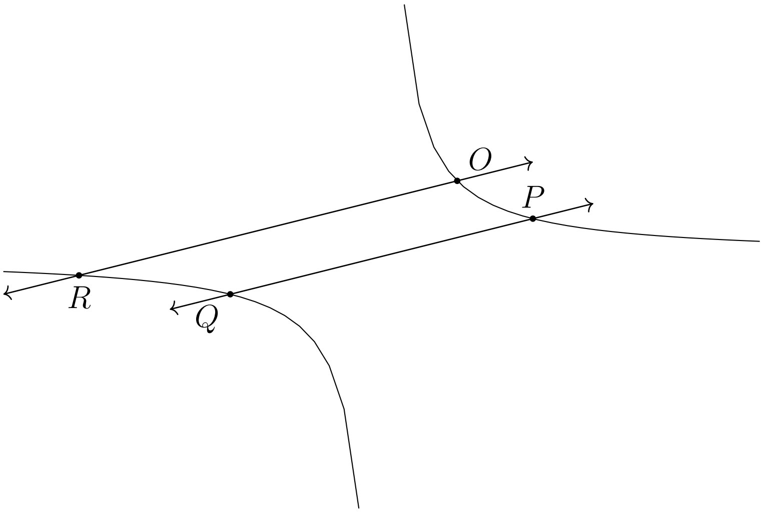

Figure 2.4: $R = P \oplus Q$ when C is a hyperbola.

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, $\langle C, \oplus \rangle \cong \langle \mathbb{R}^\times, \cdot \rangle$.

2.3 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 $a, b, c \in Q$.

2.4 Conics in Fields of Charecteristic 2

Chapter 3

Affine Geometry

3.1 Axiomatic Construction of Affine Space

3.2 The Affine Space

Definition. 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. [Aud02]

3.2.1 Affine Transfromations

3.3 Fundamental Theorem of Affine Geometry

3.4 Affine Congruence of Conics

Chapter 4

Projective Geometry

4.1 The Projective Space

4.1.1 Constructing the Projective Plane

4.1.2 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.

4.1.3 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. *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

$$\begin{array}{rc} & (\dim F - 1) + (\dim G - 1) \geq (\dim E - 1) \\ \Longrightarrow & \dim F + \dim G \geq \dim E + 1 \end{array}$$

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,

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

■

4.1.4 Projective Transformations

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

4.1.5 Homogeneous Coordinates and Projective Frames

Given a basis of vector space E, the vectors in E can be descirbed 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.

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. *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. ■

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

Proof. ■

4.2 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. *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,

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

■

4.3 Fundamental Theorem of Projective Geometry

Theorem (Fundamental Theorem of Projective Geometry)**.** *Let $a_1, \dots, a_{n+2}$ and $b_1, \dots, b_{n+2}$ be two sets of points in $\mathbb{RP}^n$. Then there exists a unique projective transformation $f : \mathbb{RP}^n \to \mathbb{RP}^n$ such that, $f(a_i) = b_i$ for all $i = 1, \dots, n+2$. [AAS17]*

Theorem (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.*

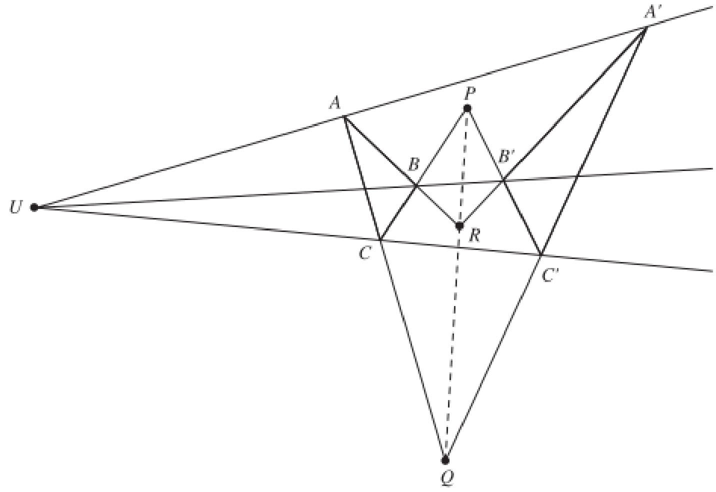

Figure 4.1: Figure from [BEG12].

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. ■

Proof adapted from [BEG12].

Proposition. *There is a unique projective conic through any given set of five points.*

Proof. ■

Proof adapted from [BEG12].

Remark. **The Standard Projective Conic**

Proposition. *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 adapted from [BEG12].

Theorem (Pascal's Theorem)**.**

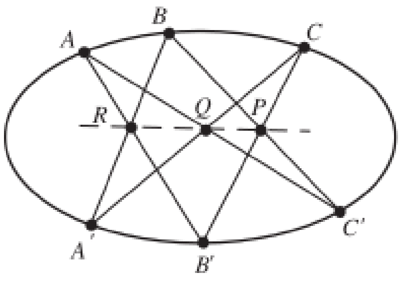

Figure 4.2: Figure from [BEG12].

Proof. ∎

Proof adapted from [BEG12].

4.4 Elliptic Curves

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

4.4.1 Group Laws on Elliptic Curves

Bibliography

[AAS17] Shiri Artstein-Avidan and Boaz A. Slomka. Fundamental Theorems of Affine and Projective Geometry Revisited. *Communications in Contemporary Mathematics*, 19, 2017.

[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.

[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.

[Spa] Steven Spallone. Introduction to Curves.