Projective Geometry

Richard Earl

Trinity Term 2025

LECTURE LAYOUT

1-2: Projective Spaces (as $\mathbb{P}(V)$ of a vector space V). Homogeneous Co-ordinates. Linear Subspaces.
3-4: Projective Transformations. General Position. Desargues Theorem. Cross-ratio.
5: Dual Spaces. Duality.
6-7: Symmetric Bilinear Forms. Conics. Singular conics, singular points. Projective equivalence of non-singular conics.
7-8: Correspondence between $\mathbb{P}^1$ and a non-singular conic. Simple applications to Diophantine Equations.

SUGGESTED READING

1) N.J. Hitchin, Maths Institute notes on Projective Geometry, found at

http://people.maths.ox.ac.uk/hitchin/hitchinnotes/hitchinnotes.html

2) M. Reid and B. Szendrői, Geometry and topology, Cambridge University Press, 2005 (Chapter 5).

3) R. Casse, Projective Geometry, An Introduction, Oxford University Press (2006)

Further Reading:

4) A. Beutelspachter and U. Rosenbaum, Projective Geometry, Cambridge (1998)

1. INTRODUCTION

We will start by considering a theorem that is not actually part of this course – namely *Bézout's Theorem* – but a clean and general result which readily motivates the worth of projective geometry. (For those interested, the theorem is part of the Part B course *Algebraic Curves*.)

Bezout's Theorem is a first significant result in *algebraic geometry*. There as many different types of geometry as there are different properties of interest to geometers. Differential geometry, for example, is interested in smooth objects (spaces and maps) to which calculus can be applied. Riemannian geometry is focused on metric properties. Algebraic geometry is unsurprisingly interested in objects that can be described using algebraic language, and proved using the theorems of algebra.

So, for example, curves defined by polynomials such as $x^2+xy+y^2 = 1$ would be of interest to an algebraic geometer whereas the curve with equation $y = e^x$ would not be. Bézout's Theorem addresses a natural first question: how many times do two curves, defined by polynomials of degrees m and n, intersect?

If we begin with $m = n = 1$ then we are talking about two lines. These typically meet in a point but we recognize that this wouldn't be the case if the lines are parallel. If $m = 1$ and $n = 2$, so that we're considering a line and a conic, then there can be as many as two intersections. We appreciate that there may be no intersections – with $y = 0$ and $y = x^2 + 1$ – but that can be circumvented by working with complex numbers, and we can see that the answer might be just one – with $y = 0$ and $y = x^2$ – but we could think of this as a double contact or repeated root in some sense. But we are still left with cases like $y = x$ and $(y - x)^2 = 1$ which appear to have no intersection, or $y = 0$ and $y^2 = x$ which has one 'single contact' intersection. Consider the $m = n = 2$ case and you'll find the number of intersections can be $0, 1, 2, 3, 4$.

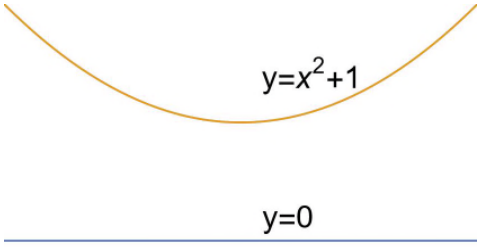

Fig. 1a – no real intersections

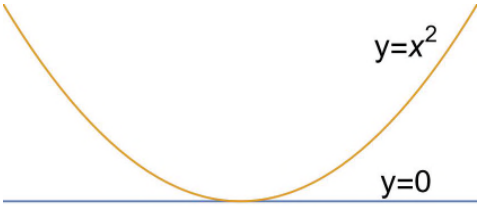

Fig. 1b – one double contact

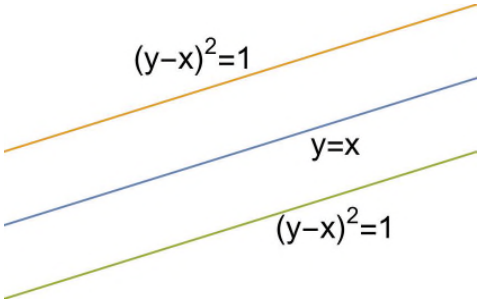

Fig 1c. – no intersections

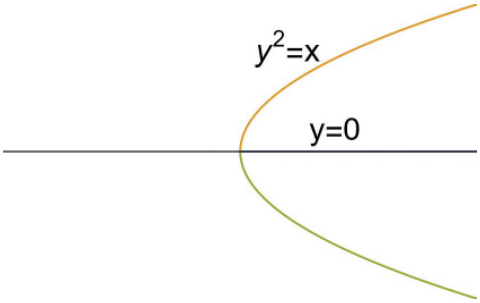

Fig. 1d. – one single contact

Perhaps, then, the best we can do is to say that the two curves meet in at most mn points. Even the use of complex numbers and appreciation of multiple contacts cannot completely resolve the issue. It turns out, though, that all we are missing is the notion of *points at infinity.* Once we properly introduce the notion of parallel lines meeting at a point at infinity then Bézout's Theorem states that the two curves have mn intersections, counting multiple contacts, using complex numbers, and including points at infinity.

So given two parallel lines, we will agree that they meet at some idealized point at infinity. As lines should only meet once this point at infinity lies in both directions. Given a third parallel line, it will meet each of these two lines in a point at infinity, and so in fact at the same point at infinity. So to each family of parallel lines there is a single point at infinity. Put another way there is a point at infinity for each gradient m; that is, the lines $y = mx + c$ all meet in the same point at infinity. And we need to remember to allow $m = \infty$ as a possible gradient, relating to the family of parallel vertical lines. These points at infinity make the *line at infinity.*

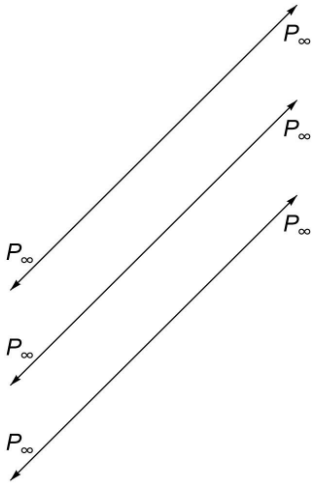

Fig. 2 – parallel lines

Note though that these 'points at infinity' aren't special in any way, or rather we've only made them special by our choice of where to put our affine xy-axes. The family of parallel lines passing through a point at infinity, properly judged from infinity, would not look any different from the family of lines passing through the origin.

If we return to our earlier examples, when Bézout appeared not to hold:

- $y = 0$, $y^2 = x$. The parabola and line meet a second time at the point at infinity at the 'end' of the x-axis
- $y = x$, $(y - x)^2 = 1$. The two lines $y = x \pm 1$ both meet $y = x$ at a point at infinity in the same way that $y = 0$ and $y^2 = x^2$ meet at the origin.

1.1 The Projective Plane

We need, then, a rigorous, formal way of introducing these points at infinity if we are to prove geometric results involving them. For fixed m, the lines $y = mx + c$ all meet at a point at infinity. This point at infinity is where the points (x, mx) move to as $x \to \pm\infty$. So it's the ratio of x and y that is important here. Somehow we want to include all the points (x, y) of the standard affine plane $\mathbb{R}^2$ and a line at infinity including the points $(\infty, m\infty)$ where $m \in \mathbb{R} \cup \{\infty\}$.

We cannot make easy meaning of $(\infty, m\infty)$ but if we recognize this ∞ as the consequence of some erroneous division by zero, then we can describe our 'extended' plane using **homogeneous co-ordinates,** first introduced by Möbius in 1827.

Definition 1 *Given real x_0, x_1, x_2, not all zero, then we write $[x_0 \colon x_1 \colon x_2]$ for the equivalence class of $(x_0, x_1, x_2) \in \mathbb{R}^3 \backslash \{\mathbf{0}\}$ under the equivalence relation*

$$(x_0, x_1, x_2) \sim (\lambda x_0, \lambda x_1, \lambda x_2) \qquad \textit{where } \lambda \neq 0.$$

How does this help us with the previous discussion? Well if $x_0 \neq 0$ then we may divide by x_0 (i.e. set $\lambda = 1/x_0$) to see that such equivalence classes can be represented as $[1 \colon x \colon y]$ where $x = x_1/x_0$ and $y = x_2/x_0$. These are 'most' of the equivalence classes and $[1 \colon x \colon y]$ can be identified with the point $(x, y) \in \mathbb{R}^2$. And the remaining equivalence classes, when $x_0 = 0$ are $[0 \colon 1 \colon m]$ when $x_1 \neq 0$ which corresponds to the point at infinity $(\infty, m\infty)$, and finally $[0 \colon 0 \colon 1]$ which corresponds to $m = \infty$' the point at infinity of the vertical lines.

If we return to the earlier 'problematic' examples we see now that

- $y = 0$, $y^2 = x$. The parabola and line meet a second time at $[0 \colon 1 \colon 0]$.
- $y = x$, $(y - x)^2 = 1$. The two lines $y = x \pm 1$ both meet $y = x$ at $[0 \colon 1 \colon 1]$.

Whilst here, and remembering that $x = x_1/x_0$ and $y = x_2/x_0$, we can see that the affine lines $y = mx + c$ would become

$$x_2 = mx_1 + cx_0$$

and that this line passes through the point at infinity $[0 \colon 1 \colon m]$. Further the parabola $y^2 = x$ would become $x_2^2 = x_0 x_1$ and we see this does indeed pass through the point $[0 \colon 1 \colon 0]$.

The variables x_1/x_0 and x_2/x_0 are known as **inhomogeneous co-ordinates.**

2. PROJECTIVE SPACES

In this chapter we define the basic objects of study in this course, projective spaces. Looking to generalize the earlier discussion we consider projective spaces over any field $\mathbb{F}$, not just $\mathbb{R}$ or $\mathbb{C}$. Further we will consider finite-dimensional spaces over $\mathbb{F}$ so that we can also better appreciate the effect on a projective space of a change of basis.

So throughout V will denote a finite-dimensional vector space over a field $\mathbb{F}$. We shall denote by $\mathbb{F}^*$ the multiplicative group of non-zero elements of $\mathbb{F}$.

Definition 2 *The **projective space** $\mathbb{P}(V)$ consists of the equivalence classes $[v]$, where $v \in V, v \neq 0_V$, under the equivalence relation $v \sim \lambda v$ for all $\lambda \in \mathbb{F}^*$.*

Note that $\mathbb{P}(V)$ can equally be identified as the set of 1-dimensional subspaces of V. Or, in the language of group actions, we might write

$$\mathbb{P}(V) = \frac{V \backslash \{0_V\}}{\mathbb{F}^*},$$

where $\mathbb{F}^*$ acts by scalar multiplication.

Remark 3 *Note that, currently, a projective space is simply a set. It has no particular algebraic structure. We will shortly discuss the topology of some projective spaces.*

Definition 4 *We define the **dimension** of $\mathbb{P}(V)$ as $\dim V - 1$. This reflects our intuition that factoring out the $\mathbb{F}^*$ action has lowered the dimension by one.*

We will use the notation $\mathbb{P}^d$ to denote a projective space of dimension d and will write $\mathbb{FP}^d$ if we wish to highlight the underlying field.

*If $\dim \mathbb{P}(V) = 1$ then $\mathbb{P}(V)$ is called a **projective line**, and if $\dim \mathbb{P}(V) = 2$ then $\mathbb{P}(V)$ is called a **projective plane**.*

Example 5 *(a) The real projective line $\mathbb{RP}^1$ is*

$$\frac{\mathbb{R}^2 - \{(0,0)\}}{\mathbb{R}^*}.$$

As a quotient topological space this is the circle. It is straightforwardly homeomorphic to $S^1/\{\pm 1\}$ which in turn is homeomorphic to

$$\frac{\textit{upper semi-circle}}{-1 \sim 1} \cong S^1.$$

(b) The complex projective line $\mathbb{CP}^1$ is

$$\frac{\mathbb{C}^2 - \{(0,0)\}}{\mathbb{C}^*}.$$

As a quotient topological space this is the sphere, the Riemann sphere most naturally, as we can identify $z \in \mathbb{C}$ with $[1\colon z]$ and ∞ as $[0\colon 1]$.

(c) The real projective plane $\mathbb{RP}^2$ was the subject of the discussion in the previous chapter. Topologically it is $S^2/\{\pm 1\}$, a spherical shell with antipodal points identified, or equivalently a single hemisphere with diametrically opposite boundary points identified. By flattening the hemisphere into a disc we can see this is homeomorphic to a closed disc with diametrically opposite boundary points identified, as in Figure 3.

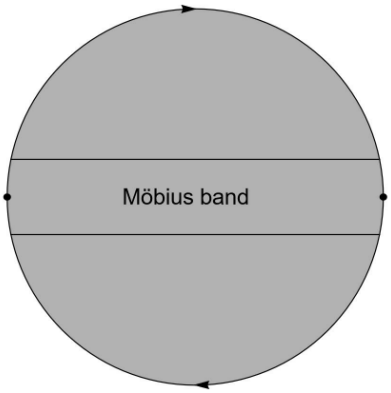

Fig. 3 – real projective plane

$\mathbb{RP}^2$ is compact as S^2 is compact. Note that the region between the two horizontal lines is a Möbius band. Consequently $\mathbb{RP}^2$ is not orientable.

Definition 6 *If U is a subspace of V, then $\mathbb{P}(U)$ is a subset of $\mathbb{P}(V)$ called a **linear subspace**. In particular, if $\dim U = 2$, we obtain a **projective line** (usually just referred to as a line) in $\mathbb{P}(V)$. If $\dim U = 3$, we obtain a **projective plane**. If $\dim U = \dim V - 1$, then we call $\mathbb{P}(U)$ a **hyperplane.***

Proposition 7 *Through any 2 distinct points in $\mathbb{P}(V)$, there is a unique projective line.*

Proof Let $[u] \neq [v]$ in $\mathbb{P}(V)$, so u, v are linearly independent. The unique line containing $[u], [v]$ is now $\mathbb{P}(\langle u, v\rangle)$. Certainly this is a projective line and if $\mathbb{P}(U)$ were another such line with $\dim U = 2$ then we'd have $u, v \in U$ and so $U = \langle u, v\rangle$. ■

We can immediately see that intersection properties are nicer in a projective plane than in the Euclidean plane.

Proposition 8 *In a projective plane, any two distinct projective lines meet in a unique point.*

Proof We can write the projective plane as $\mathbb{P}(V)$ for a 3-dimensional vector space V and the projective lines as $\mathbb{P}(U_1), \mathbb{P}(U_2)$ for two distinct 2-dimensional subspaces U_1 and U_2 of V.

Now recall the dimension formula

$$\dim(U_1 + U_2) + \dim(U_1 \cap U_2) = \dim(U_1) + \dim(U_2).$$

As U_1, U_2 are distinct 2-dimensional subspaces, the sum $U_1 + U_2$ strictly contains U_1 and hence is of dimension greater than 2, so is the full 3-dimensional space V. Hence the formula shows $U_1 \cap U_2$ is 1-dimensional, and this represents the unique point in projective space where $\mathbb{P}(U_1)$ meets $\mathbb{P}(U_2)$. ■

2.1 Homogeneous Co-ordinates.

Say that $\dim V = n+1$ and $v_0, \ldots, v_n$ is a basis for V. Then any $v \in V$ can be uniquely written

$$v = x_0 v_0 + x_1 v_1 + \cdots + x_n v_n$$

and so $[v]$ can be given the **homogeneous co-ordinates**

$$[v] = [x_0 \colon x_1 \colon \cdots \colon x_n],$$

which are unique up to multiplication by a non-zero scalar. Recall that not all of $x_0, \ldots, x_n$ can be zero.

Example 9 *Let $\mathbb{P}(V)$ be a projective line and P_0, P_1, P_2 be three distinct points in $\mathbb{P}(V)$. Then there is a basis for V with respect to which*

$$P_0 = [1 \colon 0], \qquad P_1 = [1 \colon 1], \qquad P_2 = [0 \colon 1].$$

Note that the inhomogeneous co-ordinates of P_0, P_1, P_2 are $0, 1, \infty$ respectively.

Solution Say that $P_0 = [v_0]$ and $P_1 = [v_1]$. As $P_0 \neq P_1$ then v_0, v_1 are linearly independent and hence a basis of V. So, if $P_2 = [v_2]$ we may write

$$v_2 = \alpha_0 v_0 + \alpha_1 v_1$$

and as P_0, P_1, P_2 are distinct then neither α_0 nor α_1 are zero. So with respect to the basis $\{\alpha_0 v_0, \alpha_1 v_1\}$ for V it's the case that P_0, P_1, P_2 respectively have the homogeneous co-ordinates above. ■

Remark 10 *This result may seem familiar from the study of Möbius transformations, where we saw three distinct points of the extended complex plane can be mapped to $0, 1, \infty$ by a unique Möbius transformation. We shall see in due course that the Möbius transformations are the projective transformations of $\mathbb{CP}^1$.*

Example 11 *Consider the line in affine space $\mathbb{R}^2$ with equation $y = 2x$. We can complete this to a projective line in $\mathbb{RP}^2$ by embedding $\mathbb{R}^2$ in $\mathbb{RP}^2$ via $(x, y) \mapsto [1 \colon x \colon y]$. Recall that $x = x_1/x_0$ and $y = x_2/x_0$ so that in terms of homogeneous co-ordinates $[x_0 \colon x_1 \colon x_2]$, the projective line has equation $x_2 - 2x_1 = 0$.*

Example 12 *Write down the equation of the line connecting the points $[1 \colon 2 \colon 0]$ and $[0 \colon 1 \colon 1]$ in $\mathbb{P}(\mathbb{F}^3)$. What is its equation in inhomogeneous co-ordinates? What is its point at infinity?*

Solution Let x_0, x_1, x_2 be the homogeneous co-ordinates in $\mathbb{F}^3$. A (projective) line has the form $\mathbb{P}(U)$ where U is a 2-dimensional subspace of $\mathbb{F}^3$ and such subspaces have an equation of the form

$$a_0 x_0 + a_1 x_1 + a_2 x_2 = 0.$$

So we have $a_0 + 2a_1 = 0$ and $a_1 + a_2 = 0$, so that the (projective) line has equation

$$-2a_1x_0 + a_1x_1 - a_1x_2 = 0.$$

Or, as such equations are unique only up to multiplication by a non-zero scalar, then we can write this as

$$2x_0 - x_1 + x_2 = 0.$$

In terms of inhomogeneous co-ordinates $x = x_1/x_0$ and $y = x_2/x_0$, this is the line $2 - x + y = 0$ and its point at infinity (when $x_0 = 0$) is $[0\colon 1\colon 1]$. ■

Example 13 *What projective conic does the hyperbola $xy = 1$ correspond to in $\mathbb{P}^2$? What are its points at infinity? What are the points at infinity of the parabola $y^2 = x$?*

Solution Recalling that $x = x_1/x_0$ and $y = x_2/x_0$ then the projectivized version of the hyperbola has equation $x_1x_2 = x_0^2$. Note that its two points at infinity are $[0\colon 1\colon 0]$ and $[0\colon 0\colon 1]$, respectively the points at infinity of the x-axis and y-axis, the hyperbola's asymptotes. The parabola $y^2 = x$ has projectivized equation $x_2^2 = x_1x_0$ which has point at infinity $[0\colon 1\colon 0]$. ■

Generally, we may decompose n-dimensional projective space $\mathbb{FP}^n = \mathbb{P}(\mathbb{F}^{n+1})$ as the union of 2 sets

$$S_\infty = \{[x_0\colon \ldots : x_n] \mid x_0 = 0 : x_i \text{ not all } 0\}$$
$$S_{aff} = \{[x_0\colon \ldots : x_n] \mid x_0 \neq 0\}$$

Clearly S_∞ may be identified with projective space $\mathbb{FP}^{n-1}$ of dimension one lower. In S_{aff}, every point may be written as $[1\colon t_1\colon \ldots : t_n]$ where $t_i = x_i/x_0$, and this sets up an identification of S_{aff} with $\mathbb{F}^n$. So we have a disjoint union

$$\mathbb{FP}^n = \mathbb{F}^n \cup \mathbb{FP}^{n-1}. \tag{2.1}$$

Intuitively, we are adding some points at infinity – in fact a **hyperplane at infinity** $\mathbb{FP}^{n-1}$– to the **affine space** $\mathbb{F}^n$ to obtain the projective space $\mathbb{FP}^n$. As we mentioned in the introduction, this ensures that projective space has nicer properties than affine space, especially as regards intersection properties. For example, going back to Proposition 8, we can see that parallel lines in affine space $\mathbb{F}^2$ generate projective lines in $\mathbb{FP}^2$ that meet in the $\mathbb{FP}^1$ at infinity. Likewise distinct projective planes in $\mathbb{P}^3$ meet in a projective line.

It is important to realise that the decomposition (2.1) is not canonical. There is nothing special or different about the points at infinity. They are deemed such only by our choice of where to place an affine space $\mathbb{F}^n$ within the projective space $\mathbb{FP}^n$. We could , for example, choose any other co-ordinate x_i and decompose projective space according to whether x_i is zero or non-zero.

In fact, it is often useful to consider the subsets $\mathcal{U}_i$ of $\mathbb{FP}^n$ given by

$$\mathcal{U}_i = \{[x_0, \ldots, x_n] \mid x_i \neq 0\}$$

The $\mathcal{U}_i$ cover $\mathbb{FP}^n$, as every point in $\mathbb{FP}^n$ has *some* co-ordinate x_i non-zero. As above, each $\mathcal{U}_i$ may be identified with $\mathbb{F}^n$. So we have covered projective space by open sets each with an identification with affine space. If $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ this endows $\mathbb{RP}^n$ and $\mathbb{CP}^n$ with the structure of an n-dimensional **manifold** and n-dimensional **complex manifold** respectively.

Remark 14 *(Off-syllabus) If we take the field $\mathbb{F}$ to be $\mathbb{R}$ or $\mathbb{C}$ then in fact we can put a topology on projective space, related to the Euclidean topology on $\mathbb{R}^n$ or $\mathbb{C}^n$.*

For $\mathbb{R}^{n+1}$, this proceeds by observing that Definition 2 is equivalent to saying that

$$\mathbb{RP}^n = \frac{\{v \in S^n \subset \mathbb{R}^{n+1}\}}{v \sim -v}$$

(where S^n is the unit sphere in $\mathbb{R}^{n+1}$), because every non-zero vector $v = (x_1, \ldots, x_n) \in \mathbb{R}^{n+1}$ may be scaled by $\mathbb{R}^*$ to an element of norm one, which is unique up to replacing v by $-v$. So we have exhibited real projective space as the quotient of the sphere by a $\mathbb{Z}_2$ action. We can thus endow real projective space with the quotient topology, which is compact (as the sphere is a compact subset of Euclidean space) and Hausdorff (as it is the quotient of a Hausdorff space by the action of a finite (and hence compact) group). Similar ideas may be used to topologize complex projective space.

Real and complex projective spaces may thus be viewed as compactifications of the corresponding affine spaces. In particular, the projective lines over these fields are the one-point compactifications of $\mathbb{R}$ and $\mathbb{C}$ respectively. In the complex case, we may view the projective line as the Riemann sphere and in the real case we obtain the circle (Example 5).

*For general fields $\mathbb{F}$, we do not have an analogue of the Euclidean topology on $\mathbb{F}^n$, so these ideas are not applicable. In algebraic geometry there is a standard topology for projective spaces over general fields, the **Zariski topology**, but it has very different properties – in particular it has fewer open sets and is not Hausdorff. (This is covered more in the Part C Algebraic Geometry course.)*

More generally we can see that subsets of projective space can be defined by the zero sets of homogeneous polynomials. We say a polynomial $P(x)$ is **homogeneous** of degree j if there exists a positive integer j such that $P(\lambda x) = \lambda^j P(x)$ for all x. (Equivalently, all the terms in $P(x)$ are of total degree j). For example, $x_0x_1^2 + x_0x_1x_2 + x_2^3$ is homogeneous of degree 3, but $x_0 + x_1x_2$ is not homogeneous.

Homogeneity is the condition that ensures that the equation $P(x) = 0$ is well-defined on projective space. A **projective algebraic variety** is a subset of projective space defined by a system of homogeneous polynomial equations. If the equations are all of degree 1 we define the linear subspaces. We shall later investigate the case of *quadrics*, which are defined by a single homogeneous quadratic polynomial; in a projective plane quadrics are referred to as *conics*.

2.2 Axiomatization of Projective Planes (Off-syllabus)

Alternatively an axiomatic approach can be taken to introducing projective planes. In this approach, a projective plane consists of collections $\mathcal{P}$ of points and $\mathcal{L}$ of lines satisfying:

- given two distinct points, there is a unique line containing them.
- any two lines have at least one point in common.

- any line contains at least three points.
- there are at least two lines.

The above actually provides a somewhat more general notion of what it is to be a projective plane. The smallest projective plane is the order 2 *Fano plane* (named after the Italian mathematician Gino Fano (1871-1952)) which is often represented as below:

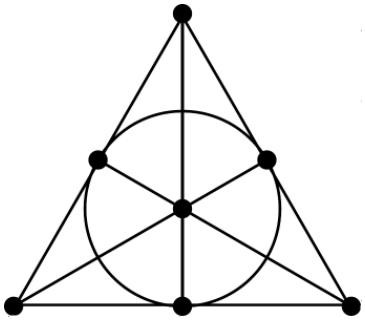

Fig. 4 – Fano plane

Here the dots are points and the line segments/circle are lines. This is the same as $\mathbb{F}_2\mathbb{P}^2$. The *order* of a projective plane is one less than the number of points in any projective line.

However there are four non-isomorphic projective planes of order 9, the usual $\mathbb{F}_9\mathbb{P}^2$ and three further planes in which Desargues' Theorem does not hold (see later). The only *known* finite projective planes have an order which is the power of a prime. There is no projective plane of order 10, but this is only known to be true using lengthy computer elimination and it is still an open problem as to whether there is a projective plane of order 12.

3. PROJECTIVE TRANSFORMATIONS

Whenever we introduce a class of mathematical objects, we are always interested in the transformations between them. For example with groups we consider homomorphisms, with topological spaces we consider continuous maps, and with vector spaces linear maps.

We have defined projective spaces in terms of quotients of vector spaces. It is therefore natural to consider maps of projective spaces induced by linear maps of vector spaces. The obvious definition is

$$\tau\colon [v] \mapsto [Tv]$$

where $[v]$ is the point of projective space represented by $v \in V\backslash\{0\}$.

There are two potential problems we must consider first. One, as always with defining maps on quotient spaces, is to check that the map is well-defined. That is, we must check that if $[v] = [w]$ then $[Tv] = [Tw]$. In our situation this is clear from the linearity of T, and the fact that $[v] = [w]$ if and only if v is a non-zero scalar multiple of w. The second problem is that only non-zero vectors represent points of projective space, so we need Tv to be non-zero whenever v is, that is, we need T to be injective.

Definition 15 *If $T : V \to W$ is an injective linear transformation, we define the associated* ***projective linear transformation*** *by*

$$\tau\colon v \mapsto [Tv]$$

We will generally be interested in the case when $V = W$, so that T is invertible.

Note that any non-zero scalar multiple of T represents the same projective transformation as does T. In fact, the assignment $T \mapsto \tau$ defines a homomorphism from $GL(V)$, the group of invertible linear transformations of V, onto the group of projective linear transformations of $\mathbb{P}(V)$. The kernel of this map is the (normal) subgroup of scalar invertible linear transformations, that is, non-zero scalar multiples of the identity. Therefore, using the first isomorphism theorem for groups, we can make the definition.

Definition 16 *The group of projective linear transformations of $\mathbb{P}(V)$ is*

$$PGL(V) = \frac{GL(V)}{\{\lambda I \mid \lambda \in \mathbb{F}^*\}}.$$

More concretely, if we identify V with $\mathbb{F}^{n+1}$ by choosing a basis, then we write the group $PGL(V)$ as $PGL(n+1, \mathbb{F})$, the quotient of the group of $(n+1) \times (n+1)$ invertible matrices over $\mathbb{F}$ by the subgroup of non-zero scalar matrices.

Of course we can write projective transformations in terms of homogeneous co-ordinates. We illustrate this in the case of the projective line.

Example 17 *Consider an invertible linear map $T\colon \mathbb{F}^2 \to \mathbb{F}^2$ given by $T(x,y) = (ax+by, cx+dy)$ with $ad-bc \neq 0$.*

Working on an affine patch $y \neq 0$, we can rewrite the associated projective linear transformation of $\mathbb{FP}^1$ as

$$\left[\frac{x}{y}\colon 1\right] \mapsto \left[\frac{ax+by}{cx+dy}\colon 1\right],$$

so in terms of the inhomogeneous co-ordinate $t = \frac{x}{y}$ then T is the map

$$t \mapsto \frac{at+b}{ct+d}.$$

*In the case $\mathbb{F} = \mathbb{C}$, we have encountered these transformations before: they are the **Möbius transformations** of the Riemann sphere $\mathbb{CP}^1$. (The point at infinity ∞ in the Riemann sphere is here identified with $[1,0]$).*

Example 18 *Find the order of the group $PGL(2,\mathbb{F})$ where $\mathbb{F}$ is a finite field with q elements.*

Solution A representative of an element of $PGL(2,\mathbb{F})$ is an invertible matrix and so its columns form a basis for $\mathbb{F}^2$. The first column can therefore be any vector in $\mathbb{F}^2\backslash\{0\}$, and there are q^2-1 such vectors. Now the second column needs to be independent of the first column. As $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ then there are $q-1$ vectors that are dependent on the first vector and so q^2-q independent vectors. The number of invertible matrices over $\mathbb{F}$ is then $(q^2-1)(q^2-q)$. However each transformation in $PGL(2,\mathbb{F})$ is represented by $q-1$ invertible matrices (which are scalar multiples of one another). Finally we have

$$|PGL(2,\mathbb{F})| = \frac{(q^2-1)(q^2-q)}{(q-1)} = (q-1)q(q+1).$$

■

We may recall from complex analysis the result that given an ordered triple of distinct points in the Riemann sphere, there is a unique Möbius transformation sending the triple to $(0,1,\infty)$. Hence the group $PGL(2,\mathbb{C})$ of Möbius transformations acts transitively on the set of ordered triples of distinct points in the projective line.

What does the condition that the points are distinct mean in terms of projective geometry? Well, two points in projective space are equal if and only if their representative vectors are proportional, which for two vectors is equivalent to saying they are dependent. This motivates the following definition.

Definition 19 *In an n-dimensional projective space $\mathbb{FP}^n$, we say that $n+2$ points are* in ***general position*** *if each subset of $n+1$ of these points has linearly independent representative vectors*

So in the $n=1$ case, this just says we have a triple of distinct points. And four points are in general position in $\mathbb{P}^2$ if no three are collinear.

We now prove the following theorem, which generalises the above result about Möbius transformations.

Theorem 20 *(**General position theorem**) Let $X_0, X_1, \ldots, X_{n+1}$ and $Y_0, Y_1, \ldots, Y_{n+1}$ be two $(n+2)$-tuples of points in n-dimensional projective space, such that each $(n+2)$-tuple is in general position. Then there exists a unique projective linear transformation τ such that $\tau(X_i) = Y_i$ for each i.*

Proof Let $X_i = [v_i]$ for $i = 0, \ldots, n+1$, that is, v_i is a representative vector for X_i. The general position hypothesis implies that $v_0, \ldots, v_n$ form a basis for the vector space. For the last point X_{n+1}, we have

$$v_{n+1} = \sum_{i=0}^{n} \lambda_i v_i$$

for some scalars λ_i.

Now, all the λ_i are non-zero, a(for if one is zero then we get a dependency relation between v_{n+1} and n of the other v_i. So we may in fact replace v_i by $\lambda_i v_i$ and take

$$v_{n+1} = \sum_{i=0}^{n} v_i$$

Again using general position, this representation of v_{n+1} is unique.

Similarly we can take $Y_i = [w_i]$ for $i = 0, \ldots, n+1$, with $w_{n+1} = \sum_{i=0}^{n} w_i$, where $w_0, \ldots, w_n$ is a basis.

Now there exists a linear transformation T with $T(v_i) = w_i$ for $i = 0, \ldots, n$. Linearity and the formulae for v_{n+1}, w_{n+1} also imply $T(v_{n+1}) = w_{n+1}$, as required.

If S is another linear transformation inducing a projective transformation with the required property, then $Sv_i = \mu_i w_i$ for $i = 0, \ldots, n+1$, where μ_i are non-zero scalars. Now

$$\mu_{n+1} w_{n+1} = S v_{n+1} = \sum_{i=0}^{n} S v_i = \sum_{i=0}^{n} \mu_i w_i,$$

so $w_{n+1} = \sum_{i=0}^{n} (\mu_i / \mu_{n+1}) w_i$ and by uniqueness of this representation we see all the μ_i are equal. Hence $S = \mu T$ and they induce the same projective map. ■

Remark 21 *The general position theorem might also be appreciated as follows: given $n+2$ points $X_0, \ldots, X_{n+1}$ in general position in an n-dimensional projective space $\mathbb{P}(V)$ then there is a basis for V with respect to which the $n+2$ points have co-ordinates*

$$[1\colon 0\colon \cdots \colon 0], \quad [0\colon 1\colon \cdots \colon 0], \quad \ldots \quad [0\colon 0\colon \cdots \colon 1], \quad [1\colon 1\colon \cdots \colon 1].$$

This follows as, given any basis, the points with the above co-ordinates are in general position, and so the projective map found in the previous theorem might instead be viewed as a change of basis map.

Example 22 *In the projective plane, four points are in general position if and only if no 3 are collinear. So we see that any two such quadruples in the plane are projectively equivalent. In the projective line, the ordered quadruples*

$$[1\colon 0], [0\colon 1], [1\colon 1], [1\colon 2], \qquad [1\colon 0], [0\colon 1], [1\colon 1], [1\colon 3],$$

are not projectively equivalent. The only projective transformation mapping the first three points of the first quadruple to the first three points of the second quadruple is the identity, and it clearly does not pair up the fourth points. We will meet the cross-ratio in the next chapter which explains which quadruples in a projective line are equivalent.

As an application of the general position theorem, we prove a celebrated classical result of projective geometry, *Desargues' Theorem*. (Girard Desargues 1591-1661 was a French mathematician and pioneer of projective geometry.)

Theorem 23 ***(Desargues, 1648)*** *Let O, A, A', B, B', C, C' be seven distinct points in a projective space such that the lines AA', BB' and CC' are distinct and concurrent at O. Then the points of intersection*

$$P = BC \cap B'C', \qquad Q = CA \cap C'A', \qquad R = AB \cap A'B',$$

are collinear.

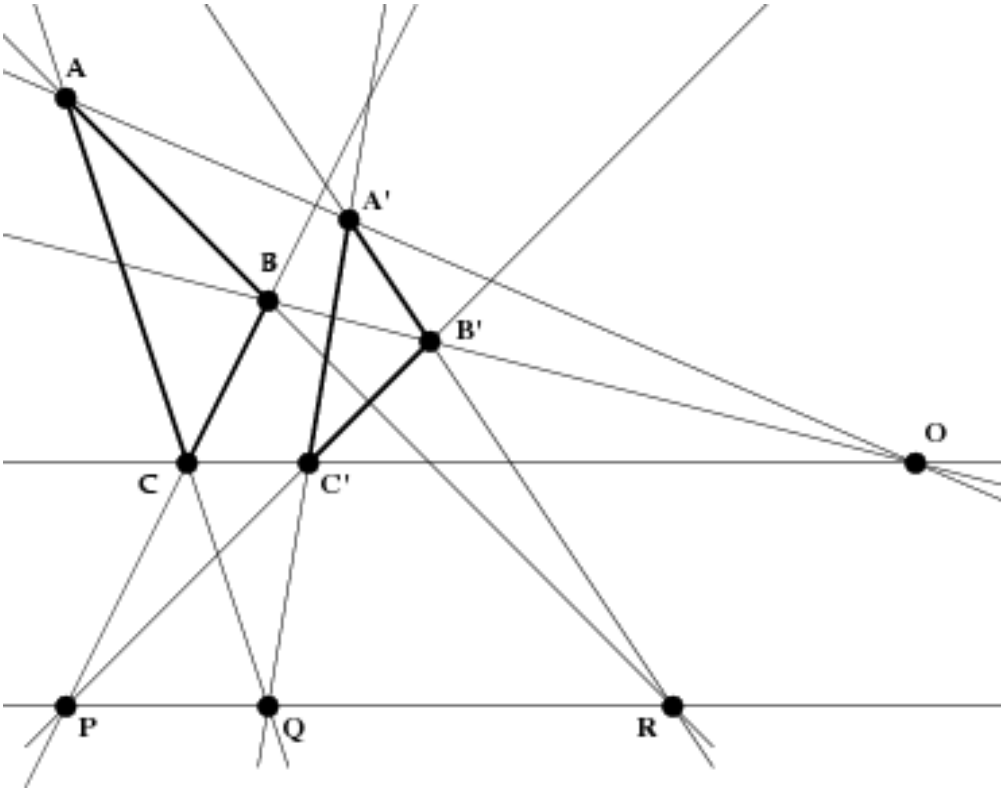

Fig.5 – Desargues' Theorem

Proof Fix a representative vector x for O. As O, A, A' are distinct, and so in general position, then we can choose representative vectors a, a' such that

$$x = a + a'$$

and likewise we can choose representative vectors b, b', c, c' such that $x = b + b'$ and $x = c + c'$. These equations imply $a - b = b' - a' = r$. As $a - b \in \langle a, b \rangle$ is a representative vector for

a point on the line AB and $a' - b'$ similarly represents a point on the line $A'B'$ then r is a representative vector of $R = AB \cap A'B'$. Similarly $b - c$ and $c - a$ are representative vectors for $P = BC \cap B'C'$ and $Q = CA \cap C'A'$ respectively. But then

$$p + q + r = (b - c) + (c - a) + (a - b) = 0$$

so that these three representative vectors are linearly dependent. Hence the points they represent are collinear. ■

The Theorem of Pappus is another classical result. It may be viewed as a version of Pascal's theorem (Theorem 52) for a degenerate conic. Again it employs general position arguments.

Theorem 24 ***(Pappus, 4th century)*** *Let A, B, C and A', B', C' be two collinear triples of distinct points in the projective plane. Then the three points*

$$P = AB' \cap A'B, \qquad Q = CA' \cap C'A \qquad R = BC' \cap B'C,$$

are collinear.

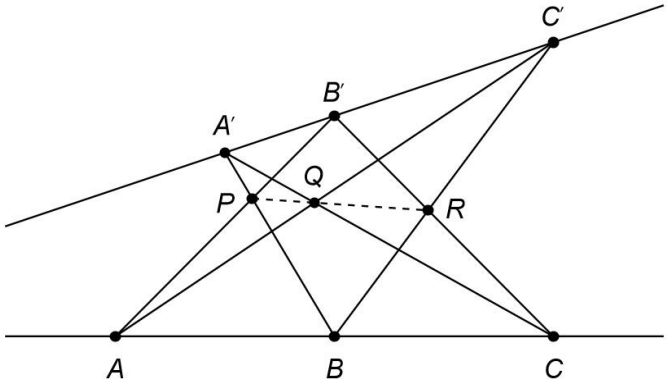

Fig.6 – Pappus' Theorem

Proof Exercise 8 on problem sheet 1. ■

Remark 25 *(Off-syllabus) Recall earlier, §2.2, that we gave a list of four axioms for what it is to be a projective plane. In a similar fashion projective spaces of higher dimensions than two can be axiomatized. It turns out that any projective space of dimension at least three is Desarguesian in that Desargues' Theorem necessarily holds in them. Hilbert was the first to appreciate that (axiomatized) projective planes need not be Desarguesian. It turns out that Desargues' theorem holds in a projective plane P if and only if $P = \mathbb{P}(V)$ where V is a 'vector space' over a division ring – a division ring satisfies all the axioms of a field other than the commutativity of multiplication, an example being the quaternions. In turn a Desarguesian projective plane can be expressed as a projective space of a vector space over a field if and only if Pappus' Theoem holds.*

4. CROSS-RATIO

Let us return to the case of the projective line. We know that any two ordered triples of distinct points are equivalent under the action of the projective linear group. What can we say about ordered quadruples? It turns out that there is a single numerical invariant which distinguishes orbits of ordered quadruples of distinct points in the projective line under the projective group.

Definition 26 *Let $x_i = [\xi_i \colon \eta_i]$, where $i = 0, \ldots, 3$, be four distinct points in the projective line $\mathbb{FP}^1$. The **cross-ratio** of the ordered quadruple is*

$$(x_0x_1 : x_2x_3) = \frac{(x_2 - x_0)(x_3 - x_1)}{(x_3 - x_0)(x_2 - x_1)} = \frac{(\xi_0\eta_2 - \xi_2\eta_0)(\xi_1\eta_3 - \xi_3\eta_1)}{(\xi_0\eta_3 - \xi_3\eta_0)(\xi_1\eta_2 - \xi_2\eta_1)}, \tag{4.1}$$

where the x_i are inhomogeneous co-ordinates and so care is need if any are 0 or ∞. (Modern use of the cross-ratio dates to 1806 by Lazare Carnot, but Pappus was making implicit use of the cross-ratio in the fourth century.)

We can observe that if we scale any pair (ξ_i, η_i) then the numerator and denominator both scale by the same factor, so the quotient on the right hand side is unchanged. The cross-ratio is therefore well-defined. Moreover, under projective transformations

$$\begin{pmatrix} \xi_i & \xi_j \\ \eta_i & \eta_j \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \xi_i & \xi_j \\ \eta_i & \eta_j \end{pmatrix}$$

by the determinant product rule we see that each bracket $\xi_i\eta_j - \xi_j\eta_i$ scales by the (non-zero!) determinant $ad - bc$, and hence the cross-ratio is invariant under a projective transformation. Thus we have shown:

Proposition 27 *The cross-ratio is a projective invariant.*

So any 2 quadruples that are projectively equivalent must have the same cross-ratio. What about the converse? We would like to show that any two quadruples with the same cross-ratio are projectively equivalent. Stated like that, it seems like an involved calculation, but we can greatly simplify it using the general position theorem. As a result of that theorem, we may assume x_0, x_1, x_2 to be the points $[1 \colon 0], [0 \colon 1], [1 \colon 1]$. Then

$$(x_0x_1 : x_2x_3) = \frac{(1.1 - 0.1)(0.\eta_3 - \xi_3.1)}{(1.\eta_3 - 0.\xi_3)(0.1 - 1.1)} = \frac{\xi_3}{\eta_3}$$

As the points are distinct, we may write $x_3 = [\lambda \colon 1]$ for $\lambda \neq 0, 1$, and now the cross-ratio is λ. So any quadruple of distinct points is projectively equivalent to the quadruple $[1 \colon 0], [0 \colon 1], [1 \colon 1], [\lambda \colon 1]$, where λ is the cross-ratio. We have therefore proved the following result.

Theorem 28 *Two ordered quadruples of distinct points in the projective line are projectively equivalent if and only if their cross-ratios are equal.*

Remark 29 *(Off-syllabus) Notice that the cross-ratio in (4.1) does not take the values* 0, 1 *or* ∞*. The cross-ratio thus sets up a bijection between*

- *ordered quadruples of distinct points in* $\mathbb{FP}^1$ *modulo the action of the projective linear group* $PGL(2,\mathbb{F})$*, and*
- *the projective line* $\mathbb{FP}^1$ *with points* $0, 1, \infty$ *removed.*

Take $\mathbb{F} = \mathbb{C}$ *now. Note that as* x_2 *coincides with* x_0 *or* x_3 *coincides with* x_1 *then the cross-ratio approaches* 0*. Likewise as* x_3 *coincides with* x_0 *or* x_2 *coincides with* x_1 *then the cross-ratio approaches* ∞*. Finally as* x_3 *coincides with* x_2 *or* x_1 *coincides with* x_0 *the cross-ratio approaches* 1*. Thus, in some sense all of* $\mathbb{CP}^1$ *can be used to represent orbits of quadruples, though we have found* $0, 1, \infty$ *each correspond to two orbits and no point of* $\mathbb{CP}^1$ *corresponds to an orbit with more than two points coinciding.*

The question of how this correspondence might be completed to include the points $0, 1, \infty$ *by allowing members of the quadruple to coincide suitably is a subtle one that leads into the branch of algebraic geometry known as Geometric Invariant Theory. In the above example, considering all ordered quadruples, the cross-ratios other that* $0, 1, \infty$ *parameterize the 'stable' orbits,* $0, 1, \infty$ *are the 'semistable' orbits, and the remaining 'unstable' orbits (where two or more points coincide) are omitted.*

We conclude by remarking that the cross-ratio has some interesting symmetries.

Theorem 30 *The cross-ratio obeys the following equations:*

$$(x_0x_1 \colon x_2x_3) = (x_1x_0 \colon x_3x_2) = (x_2x_3 \colon x_0x_1),$$
$$(x_0x_1 \colon x_2x_3) = (x_1x_0 \colon x_2x_3)^{-1},$$
$$(x_0x_2 \colon x_1x_3) = 1 - (x_0x_1 \colon x_2x_3).$$

Proof Each of these identities is routine. We shall prove these using inhomogeneous coordinates for ease of notation.

(a) That

$$\frac{(x_2 - x_0)(x_3 - x_1)}{(x_3 - x_0)(x_2 - x_1)} = \frac{(x_3 - x_1)(x_2 - x_0)}{(x_2 - x_1)(x_3 - x_0)} = \frac{(x_0 - x_2)(x_1 - x_3)}{(x_1 - x_2)(x_0 - x_3)}$$

are trivial identities.

(b) Likewise

$$\frac{(x_2 - x_0)(x_3 - x_1)}{(x_3 - x_0)(x_2 - x_1)} = \left(\frac{(x_2 - x_1)(x_3 - x_0)}{(x_3 - x_1)(x_2 - x_0)}\right)^{-1}$$

is an immediate identity.

(c) Finally

$$\begin{aligned}(x_0x_2 \colon x_1x_3) + (x_0x_1 \colon x_2x_3) &= \frac{(x_1 - x_0)(x_3 - x_2)}{(x_3 - x_0)(x_1 - x_2)} + \frac{(x_2 - x_0)(x_3 - x_1)}{(x_3 - x_0)(x_2 - x_1)} \\ &= \frac{(x_1 - x_0)(x_3 - x_2) - (x_2 - x_0)(x_3 - x_1)}{(x_3 - x_0)(x_1 - x_2)} \\ &= \frac{x_1x_3 + x_0x_2 - x_2x_3 - x_0x_1}{(x_3 - x_0)(x_1 - x_2)} = 1.\end{aligned}$$

■

Example 31 *(1997 B3 #8) Let p_1, p_2, p_3, p_4 be distinct points in $\mathbb{CP}^1$ with $(p_1p_2 \colon p_3p_4) = \alpha$. Suppose that for each permutation $\sigma \in S_4$ we have*

$$\left(p_{\sigma(1)}p_{\sigma(2)} : p_{\sigma(3)}p_{\sigma(4)}\right) = \begin{cases} \alpha & \text{if } \sigma \text{ is even,} \\ \overline{\alpha} & \text{if } \sigma \text{ is odd.} \end{cases}$$

Show that α can take one of only two possible values, which you should find. Identify the subgroup of $PGL(2, \mathbb{C})$ which preserves the set $\{p_1, p_2, p_3, p_4\}$.

Remark 32 *In general, given distinct points $(p_1p_2 \colon p_3p_4) = \lambda$, then the permuted cross-ratio $\left(p_{\sigma(1)}p_{\sigma(2)} : p_{\sigma(3)}p_{\sigma(4)}\right)$ can take 6 values, namely*

$$\lambda, \qquad 1-\lambda, \qquad \frac{1}{\lambda}, \qquad \frac{\lambda-1}{\lambda}, \qquad \frac{1}{1-\lambda}, \qquad \frac{\lambda}{\lambda-1},$$

in light of the cross-ratio identities given in the previous theorem. For such general λ the only σ which fix the cross-ratio are the Klein 4-group

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}.$$

However, for certain special values of λ, such at α, the 6 cross-ratios above will not be distinct and a larger subgroup of S_4 will preserve the cross-ratio and so the set $\{p_1, p_2, p_3, p_4\}$.

Solution As (12) is odd then

$$\alpha = (p_1p_2 \colon p_3p_4) = (p_2p_1 \colon p_3p_4)^{-1} = \overline{\alpha}^{-1}$$

and as (23) is odd then

$$\alpha = (p_1p_2 \colon p_3p_4) = 1 - (p_1p_3 \colon p_2p_4) = 1 - \overline{\alpha}.$$

Hence $|\alpha| = 1$ and $\operatorname{Re}\alpha = \frac{1}{2}$. This means

$$\alpha = \frac{1 \pm \sqrt{3}i}{2}.$$

For these two values of α the subgroup of $PGL(2, \mathbb{C})$ fixing the set $\{p_1, p_2, p_3, p_4\}$ is isomorphic to A_4. Given τ which fixes the set, inducing a permuation σ of the points, we have

$$\alpha = (\tau(p_1)\tau(p_2) : \tau(p_3)\tau(p_4)) = \left(p_{\sigma(1)}p_{\sigma(2)} : p_{\sigma(3)}p_{\sigma(4)}\right)$$

and so σ must be even. Conversely given such even σ then the cross-ratios $\left(p_{\sigma(1)}p_{\sigma(2)} : p_{\sigma(3)}p_{\sigma(4)}\right)$ and $(p_1p_2 \colon p_3p_4)$are equal and so there is a unique transformation τ effecting this permutation. ■

5. DUALITY

We shall now apply some more linear algebra theory to projective geometry. We recall that for any vector space V over $\mathbb{F}$ we can associate the *dual space* V^* of linear maps (functionals) $f : V \to \mathbb{F}$. In the finite-dimensional case (which we are only concerned with in these notes), V and V^* are isomorphic, since they are of equal dimension; however this isomorphism depends on a choice of basis and so is not canonical. However, the double dual V^{**}, that is the dual of V^*, *is* canonically isomorphic to V. Explicitly, the map

$$\phi\colon V \to V^{**}$$

defined by

$$(\phi(v))(f) = f(v) \quad \text{for } f \in V^*,\ v \in V$$

is a canonical isomorphism between V and V^{**}.

We then have an inclusion-reversing correspondence between subspaces of V and subspaces of V^*, given by associating to $U \leqslant V$ its *annihilator*

$$U^\circ = \{f \in V^* \mid f(u) = 0 \text{ for all } u \in U\}$$

We recall the following results from Part A Linear Algebra.

Proposition 33 *For subspaces U, U_1, U_2 of V we have*
(a) if $U_1 \leqslant U_2$ then $U_2^\circ \leqslant U_1^\circ$: that is, taking the annihilator reverses inclusion.
(b) $(U_1 + U_2)^\circ = U_1^\circ \cap U_2^\circ$.
(c) $(U_1 \cap U_2)^\circ = U_1^\circ + U_2^\circ$.
(d) $\dim U + \dim U^\circ = \dim V$.
(e) $(U^\circ)^\circ = \phi(U)$.

The last statement (e) follows from the obvious fact that $\phi(U) \leqslant (U^\circ)^\circ$, and the dimension formula (d).

We shall use the canonical isomorphism ϕ to identify spaces with their double duals, and subspaces with their double annihilators, without further comment.

Turning to projective spaces, we obtain an inclusion-reversing **duality correspondence** between linear subspaces of $\mathbb{P}(V)$ and linear subspaces of $\mathbb{P}(V^*)$, given by associating $\mathbb{P}(U^\circ)$ with $\mathbb{P}(U)$.

In particular, points of $\mathbb{P}(V^*)$ correspond to hyperplanes in $\mathbb{P}(V)$, represented by n-dimensional subspaces of V if $\dim V = n + 1$. This is of course just the assignment to $[f]$, where $f \in V^*\backslash\{0\}$, of the hyperplane $\mathbb{P}(\ker f)$ in $\mathbb{P}(V)$. In terms of homogeneous co-ordinates, the point $[a_0\colon \ldots : a_n]$ in $\mathbb{P}(V^*)$ corresponds to the hyperplane with equation $a_0x_0 + \cdots + a_nx_n = 0$ in $\mathbb{P}(V)$ (note that scaling the a_i does not alter the hyperplane). Conversely, hyperplanes in $\mathbb{P}(V^*)$ correspond to points in $\mathbb{P}(V^{**}) = \mathbb{P}(V)$.

In general, if $\mathbb{P}(U)$ is an m-dimensional linear subspace of $\mathbb{P}^n = \mathbb{P}(V)$, then U has dimension $m + 1$, so U° has dimension $(n + 1) - (m + 1) = n - m$, and hence $\mathbb{P}(U^\circ)$ is a linear subspace

of $\mathbb{P}(V^*)$ of dimension $n-m-1$. Specifically, in $\mathbb{P}^2$ points dualize to lines and vice versa; in $\mathbb{P}^3$ points dualize to planes and vice versa, and lines to lines.

For the projective plane, the duality interchanges points and lines. If $[x], [y]$ are 2 points on a line L then the lines $[x^\circ], [y^\circ]$ meet at the point $[L^\circ]$. More generally a set of collinear points corresponds under duality to a set of concurrent lines. We can interpret $[x^\circ]$ as the locus in the dual plane parameterizing lines through x in the original plane.

To more formally present these facts: we have $L = \mathbb{P}(\langle x, y\rangle) = \mathbb{P}(\langle x\rangle + \langle y\rangle)$. This has dual

$$\mathbb{P}(\langle x, y\rangle^\circ) = \mathbb{P}((\langle x\rangle + \langle y\rangle)^\circ) = \mathbb{P}(\langle x\rangle^\circ \cap \langle y\rangle^\circ).$$

Notice in fact for the projective plane that Proposition 7 and Proposition 8 are dual to each other, in the sense that we get one from the other via duality. In general each theorem in projective geometry will have a dual version. Moreover once having proved a theorem in all projective spaces $\mathbb{P}(V)$ then this theorem applies equally well to dual projective spaces $\mathbb{P}(V^*)$ and so the dual theorem is a free consequence of proving the original theorem. The dual of the theorem *two distinct points lie on a unique line* has (in general) the dual theorem *two distinct hyperplanes each contain a unique linear subspace of dimension* $\dim \mathbb{P}(V) - 2$.

Example 34 *The dual of Desargues' Theorem in the plane is as follows:*

Let $\pi, \alpha, \alpha', \beta, \beta', \gamma, \gamma'$ be seven distinct lines in a projective plane such that the points

$$\alpha \cap \alpha',\ \beta \cap \beta',\ \gamma \cap \gamma'$$

are distinct and all lie on π. Then the three lines joining $\alpha \cap \beta$ and $\alpha' \cap \beta'$, joining $\beta \cap \gamma$ and $\beta' \cap \gamma'$, and joining $\gamma \cap \alpha$ and $\gamma' \cap \alpha'$, are concurrent.

Example 35 *Give a projective plane $\mathbb{P}^2$, we can define four lines to be in general position if no three of them are concurrent. This is equivalent to the four points they represent in $(\mathbb{P}^2)^*$ being in general position.*

Under duality a line $\alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 = 0$ in $\mathbb{P}^2$ corresponds to the point $[\alpha_0 \colon \alpha_1 \colon \alpha_2]$ in the dual space $\mathbb{P}^{2*}$. So by the general position theorem, four lines in $\mathbb{P}^2$ which are in general position can be assumed to have the equations

$$x_0 = 0, \qquad x_1 = 0, \qquad x_2 = 0, \qquad x_0 + x_1 + x_2 = 0$$

without any loss of generality.

Example 36 *(1998 B3 #5)*

(a) Let $\mathbb{P}(V)$ be a projective plane. Suppose that $p_1, \ldots, p_6$ are distinct points in $\mathbb{P}(V)$ and $l_1, \ldots, l_4$ are distinct lines in $\mathbb{P}(V)$, such that each line l_j contains exactly 3 of the points p_i. Show that no p_i is contained in 3 of the lines l_j, and hence (or otherwise) prove that each point p_i is the intersection of exactly two of l_1, l_2, l_3 and l_4.

(b) Let $q_1, \ldots, q_4$ be the points in $\mathbb{P}(V^*)$ dual to the lines $l_1, \ldots, l_4$ in $\mathbb{P}(V)$. By considering the dual statement (or otherwise), prove that $q_1, \ldots, q_4$ are in general position in $\mathbb{P}(V^*)$. Explain briefly how you could use this fact to show that the group G of projective transformations of $\mathbb{P}(V)$ preserving the set $\{p_1, \ldots, p_6\}$ is isomorphic to the group S_4.

Solution (a) Without loss of generality suppose, for a contradiction, that p_1 lies on each of l_1, l_2, l_3. By a possible relabelling we might then assume that the other two points on l_1 are p_2, p_3. The two other points on l_2 must be different as $l_1 \neq l_2$, call them p_4, p_5, but we then run out of points to put on l_3. A contradiction.

Suppose for a contradiction that p_1 lies only on line l_1 and none of l_2, l_3, l_4. We can label the points on l_2 as p_2, p_3, p_4. As $l_3 \neq l_2$ only one of these points may lie on l_3, so say p_5 and p_6 lie on l_3 and then we have no points to assign to l_4. A contradiction.

Consequently each point p_i lies on precisely two lines as required.

(b) $q_1, \ldots, q_4$ not being in general position in $\mathbb{P}(V^*)$ means that three of the points are collinear. The dual statement is that three of $l_1, \ldots, l_4$ are concurrent. Their intersection cannot be one of the p_i by (a) but then we have to assign nine points to these three lines alone – a contradiction. Given any permutation σ of the q_i there is a unique projective transformation of $\mathbb{P}(V^*)$ effecting that permutation on the q_i as they are in general position (and so is then any reordering of them). Thus the group of transformations in $PGL(V^*)$ preserving $q_1, \ldots, q_4$ is isomorphic to S_4. Necessarily the dual of that map preserves the set $\{l_1, l_2, l_3, l_4\}$ and so preserves the set of intersections $\{p_1, \ldots, p_6\}$. ■

6. BILINEAR FORMS AND QUADRICS

The next piece of algebra we consider in the context of projective geometry is the theory of bilinear forms. **Throughout this section, we will assume that** $\mathrm{char}\mathbb{F} \neq 2$.

Definition 37 *A **symmetric bilinear form,** on a vector space V over a field $\mathbb{F}$, is a map $B\colon V \times V \to \mathbb{F}$ such that*
(i) $B(v,w) = B(w,v)$
(ii) B is linear in v (and hence, by (i), also in w)
If an addition we have the property
(iii) if $B(v,w) = 0$ for all w then $v = 0$,
*then we say the form is **nondegenerate** or **nonsingular**.*

More concretely, if we choose a basis $e_0, \ldots, e_n$ then a bilinear form is given by

$$B(v,w) = v^T M w$$

for the symmetric matrix M such that $[M]_{ij} = B(e_i, e_j)$. Nondegeneracy of the form B is equivalent to invertibility of the matrix M. Symmetric matrices form a vector space of dimension $\frac{1}{2}\dim V(\dim V + 1)$, so we can form linear combinations of bilinear forms.

Remark 38 *In Part A Linear Algebra we focused particularly on inner products. Over $\mathbb{R}$, these are symmetric bilinear forms which satisfy the extra condition of positive definiteness (that is $B(v,v) > 0$ for $v \neq 0$). Over $\mathbb{C}$, positive definiteness requires the form to be conjugate symmetric, rather than symmetric, and sesquilinear, rather than bilinear – that is, the form is linear in one variable and conjugate linear in the other. We shall focus instead on bilinear forms and drop the positive definiteness property. In fact, for most purposes nondegeneracy is a good replacement for positive definiteness. In particular, nondegeneracy is actually equivalent to the statement that the map from V to V^* defined by $v \mapsto B(v,.)$ is an isomorphism.*

Any bilinear form is determined (if the characteristic of $\mathbb{F}$ does no equal 2), by the associated **quadratic form**

$$Q(v) = B(v,v),$$

for we can recover B via the **polarization identity**

$$B(v,w) = \frac{1}{4}(B(v+w, v+w) - B(v-w, v-w)) = \frac{1}{4}(Q(v+w) - Q(v-w)).$$

And over $\mathbb{R}$ or $\mathbb{C}$ we can diagonalise quadratic forms.

Theorem 39 *If $v \mapsto Q(v) = B(v,v)$ is a quadratic form defined on a vector space, then*
(i) if $\mathbb{F} = \mathbb{C}$, there is a basis $e_0, \ldots, e_n$ with respect to which

$$Q(v) = \lambda_0^2 + \cdots + \lambda_r^2$$

where $v = \sum_{i=0}^{n} \lambda_i e_i$ *and where* $r+1$ *is the rank of* B.

(ii) if $\mathbb{F} = \mathbb{R}$*, there is a basis* $e_0, \ldots, e_n$ *with respect to which*

$$Q(v) = \lambda_0^2 + \cdots + \lambda_r^2 - \lambda_{r+1}^2 - \cdots - \lambda_{r+s}^2$$

where $v = \sum_{i=0}^{n} \lambda_i e_i$ *and where* $r+s+1$ *is the rank of* B.

Proof Write $B(v,v) = v^T X v = \sum_{i,j} X_{ij} v_i v_j$ in some basis, where X is a symmetric matrix. If $X = 0$ then there is nothing to prove. Otherwise, we can assume that some X_{ii} is non-zero; this is because if $X_{ij} \neq 0$ where $i \neq j$ we can introduce new variables

$$y_i = \frac{1}{2}(v_i + v_j), \qquad y_j = \frac{1}{2}(v_i - v_j)$$

and now $v_i v_j = y_i^2 - y_j^2$.

Now we complete the square.

$$\frac{1}{X_{ii}} \left(\sum_j X_{ij} v_j \right)^2 = X_{ii} v_i^2 + 2 \sum_{j \neq i} X_{ij} v_j v_i + \text{terms involving the other } v_j.$$

So, by introducing the new variable $\tilde{y}_i = \sum X_{ij} v_j$, we can put B into the form

$$B(v,v) = \frac{1}{X_{ii}} \tilde{y}_i^2 + \text{terms involving the other } v_j.$$

Now we repeat the process until we have diagonalised B to $\mathrm{diag}(\beta_0, \ldots, \beta_n)$: rescaling the variables appropriately by now setting for non-zero β_i

$$y_i \mapsto \sqrt{\beta_i} y_i \quad \text{over } \mathbb{C} \qquad \text{and} \qquad y_i \mapsto \sqrt{|\beta_i|} y_i \quad \text{over } \mathbb{R},$$

now brings it into the desired forms. Note that over $\mathbb{R}$ we cannot change the sign of the coefficient of y_i^2 by rescaling. ■

Remark 40 *Note that over* $\mathbb{R}$ *we might simplify this argument by beginning with the spectral theorem, but that the spectral theorem would not help with the complex case as we are interested in symmetric rather than conjugate symmetric (i.e. Hermitian) forms.*

Notice that the form is nondegenerate exactly when $r = n$ (in the complex case) and $r + s = n$ (in the real case).

Example 41 *Consider the form on* $\mathbb{R}^3$.

$$x_0 x_1 + x_1 x_2 + x_2 x_0.$$

We change variables to

$$y_0 = \frac{1}{2}(x_0 + x_1), \quad y_1 = \frac{1}{2}(x_0 - x_1), \quad y_2 = x_2$$

to generate some non-zero diagonal terms. The form is now

$$y_0^2 - y_1^2 + 2y_2y_0.$$

We complete the square, writing this as

$$(y_0 + y_2)^2 - y_2^2 - y_1^2$$

so on putting $z_0 = y_0 + y_2$ *and* $z_1 = y_1,\ z_2 = y_2$ *we get the required form*

$$z_0^2 - z_1^2 - z_2^2$$

over the reals. If we work over $\mathbb{C}$*, then scaling* z_1, z_2 *by* i *brings us into the standard form of a nondegenerate quadratic form over* $\mathbb{C}$*.*

We have seen that linear subspaces of projective space $\mathbb{P}(V)$ are projectivisations of subspaces of V, and hence are determined by systems of homogeneous linear equations. The next simplest subsets of projective space defined by polynomial equations are the *quadrics*, which are defined by the vanishing of a quadratic form.

Definition 42 *A* ***quadric*** *is the locus of points in a projective space defined by an equation* $Q(v) = 0$*, where* $v \mapsto Q(v) = B(v, v)$ *is a (not identically zero) quadratic form.*

In the case that the projective space is a projective plane then quadrics are more typically referred to as ***conics.***

We remark that this does indeed define a subset of projective space, as $Q(v)$ *is homogeneous of degree 2 in* v*.*

Example 43 *In* $\mathbb{RP}^2$ *consider the conic defined by the quadratic form*

$$Q(x_0, x_1, x_2) = x_0^2 + x_1^2 - x_2^2.$$

In inhomogeneous co-ordinates $x = x_1/x_0, y = x_2/x_0$ *this could be considered as the hyperbola*

$$1 + x^2 - y^2 = 0.$$

This has points at infinity $[0\colon 1\colon 1]$ *and* $[0\colon 1\colon -1]$ *at the end of the asymptotes.*

We might instead have considered the conic using the inhomogeneous co-ordinates $x = x_0/x_2$*,* $y = x_1/x_2$ *and then we would be considering the circle with equation*

$$x^2 + y^2 - 1 = 0$$

which has no points at infinity.

Example 44 *Find a projective transformation which takes the parabola* $y^2 = x$ *to the circle* $x^2 + y^2 = 1$*. (Here we are using inhomogeneous co-ordinates* $x = x_1/x_0, y = x_2/x_0$*.)*

Solution In homogeneous co-ordinates these conics (call them C_1, C_2) are defined by the equation $x_2^2 = x_1 x_0$ and $x_1^2 + x_2^2 - x_0^2 = 0$ and so by the matrices

$$B_1 = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B_2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Consider the effect of a projective transformation $[T]$ on the first conic. Then

$$\begin{aligned} [\mathbf{x}] \in [T]\,(C_1) \quad &\iff \quad \left[T^{-1}\right][\mathbf{x}] \in C_1 \\ &\iff \quad (T^{-1}\mathbf{x})^T B_1 T^{-1}\mathbf{x} = 0. \\ &\iff \quad \mathbf{x}^T (T^{-1})^T B_1 T^{-1}\mathbf{x} = 0. \end{aligned}$$

And if we want T to map C_1 to C_2 then we need

$$\mathbf{x}^T (T^{-1})^T B_1 T^{-1}\mathbf{x} = 0 \quad \iff \quad \mathbf{x}^T B_2 \mathbf{x} = 0,$$

so it is sufficient to have

$$(T^{-1})^T B_1 T^{-1} = B_2$$

or equivalently that

$$B_1 = T^T B_2 T.$$

Now the matrix B_1 is symmetric and has eigenvalues $\pm 1/2, 1$. So there is an orthogonal matrix P such that

$$P^T B_1 P = \mathrm{diag}(-1/2, 1/2, 1).$$

If we now take $Q = \mathrm{diag}(\sqrt{2}, \sqrt{2}, 1)$ then we have

$$Q^T P^T B_1 P Q = \mathrm{diag}(-1, 1, 1) = B_2.$$

So we might choose $T = (PQ)^{-1}$. Calculating P gives

$$P = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and then

$$T = (PQ)^{-1} = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

■

Proposition 45 *We assume* $\mathrm{char}\mathbb{F} \neq 2$. *If a quadric contains three distinct, collinear points then it contains the entire line.*

Proof We may choose representative vectors $\mathbf{x}$ and $\mathbf{y}$ so that the points are $[\mathbf{x}]$, $[\mathbf{y}]$, $[\mathbf{x}+\mathbf{y}]$. Then we have

$$B(\mathbf{x},\mathbf{x}) = 0 = B(\mathbf{y},\mathbf{y})$$

and

$$0 = B(\mathbf{x}+\mathbf{y},\mathbf{x}+\mathbf{y}) = B(\mathbf{x},\mathbf{x}) + 2B(\mathbf{x},\mathbf{y}) + B(\mathbf{y},\mathbf{y})$$

so that $B(\mathbf{x},\mathbf{y}) = 0$ as well as $2 \neq 0$. Then for any point $[\alpha\mathbf{x}+\beta\mathbf{y}]$ of the line we have

$$B(\alpha\mathbf{x}+\beta\mathbf{y},\alpha\mathbf{x}+\beta\mathbf{y}) = \alpha^2 B(\mathbf{x},\mathbf{x}) + 2\alpha\beta B(\mathbf{x},\mathbf{y}) + \beta^2 B(\mathbf{y},\mathbf{y}) = 0$$

as required. ■

Definition 46 *We say a quadric is* ***nonsingular*** *if the associated symmetric bilinear form is nondegenerate. On choosing a basis, this is equivalent to the symmetric matrix defining the form being invertible.*

Example 47 *Over $\mathbb{C}$, our diagonalization theorem tells us that a conic can be put into one of the following three forms:*

(i) $z_0^2 + z_1^2 + z_2^2 = 0$;

(ii) $z_0^2 + z_1^2 = 0$;

(iii) $z_0^2 = 0$.

Case (i) is the general case, when the conic is nonsingular. The remaining two cases are the two kinds of singular conics. Case (ii) is a pair of distinct lines – on putting the conic in the above form $z_0^2 + z_1^2 = 0$ we see the lines are $z_0 - iz_1 = 0$ and $z_0 + iz_1 = 0$, which meet at the point $[0\colon 0\colon 1]$ in the plane. Case (iii) is the most degenerate – it is a double line, i.e. a line with multiplicity two. We can think of Cases (ii) and (iii) as singular limits or degenerations of the generic nonsingular conics.

In fact generally, for conics, but not higher dimensional quadrics, we have:

Proposition 48 *A conic in $\mathbb{FP}^2$ which contains a line is singular.*

Proof Take two points on the line in the conic and a point off the line. If we choose representative vectors e_0, e_1, e_2 for these three points, they form a basis and say that $X = (X_{ij})$ is a symmetric matrix over $\mathbb{F}$ representing the conic. Points on the line have representative vectors $\alpha e_0 + \beta e_1$ so that

$$(\alpha e_0 + \beta e_1)^T X (\alpha e_0 + \beta e_1) = 0$$

for all α, β. But this means that X has the form

$$X = \begin{pmatrix} 0 & 0 & X_{02} \\ 0 & 0 & X_{12} \\ X_{02} & X_{12} & X_{22} \end{pmatrix}$$

which is a singular matrix. ■

Proposition 49 *Non-empty, nonsingular conics in $\mathbb{RP}^2$ are projectively equivalent.*

Proof By our earlier theorem any conic's equation can be put in the form

$$x_0^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2 = 0.$$

As $r+s$ is the rank and the conic is non-singular then $r+s+1 = 3$ and so we are left considering the possibilities:

$$\begin{aligned} x_0^2 + x_1^2 + x_2^2 &= 0 \\ x_0^2 + x_1^2 - x_2^2 &= 0 \\ x_0^2 - x_1^2 - x_2^2 &= 0 \\ -x_0^2 - x_1^2 - x_2^2 &= 0. \end{aligned}$$

The first and last are empty conics (as we're working over $\mathbb{R}$, and there is no point $[0\colon 0\colon 0]$) and the second two are clearly projectively equivalent (by permuting x_0, x_1, x_2 accordingly). ■

Remark 50 *We might then view an ellipse as a conic which does not intersect the line at infinity, a parabola as a conic which is tangential to the line at infinity, and a hyperbola as a conic which intersects the line at infinity in two points.*

Proposition 51 *Through each point P of a non-singular conic C in $\mathbb{FP}^2$ there is a unique line which meets the conic only once. This line is called the* ***tangent line*** *to C at P.*

Proof Say that the conic is represented by the invertible symmetric matrix X with respect to some basis and say that $P = [\mathbf{x}]$. We then have that $X\mathbf{x} \neq \mathbf{0}$ as X is invertible and $\mathbf{x}^T X\mathbf{x} = 0$ as P lies on the conic.

A line in $\mathbb{FP}^2$ has the form $\mathbb{P}(\langle \mathbf{x}, \mathbf{y}\rangle)$ where $\mathbf{y}$ is independent of $\mathbf{x}$. This line will meet the conic at points satisfying

$$0 = (\alpha\mathbf{x} + \beta\mathbf{y})^T X(\alpha\mathbf{x} + \beta\mathbf{y}) = 2\alpha\beta\mathbf{y}^T X\mathbf{x} + \beta^2\mathbf{y}^T X\mathbf{y}.$$

For the line to meet the conic only at P (when $\beta = 0$) we must have that

$$2\lambda\mathbf{y}^T X\mathbf{x} + \mathbf{y}^T X\mathbf{y} \neq 0 \qquad \text{for all scalars } \lambda \in \mathbb{F}.$$

This is only possible if $\mathbf{y}^T X\mathbf{x} = 0$ and $\mathbf{y}^T X\mathbf{y} \neq 0$. The plane of vectors $\mathbf{y}$ perpendicular to $X\mathbf{x}$ uniquely specifies a plane in $\mathbb{F}^3$ and so uniquely specifies a line in $\mathbb{FP}^2$. ■

Pappus' Theorem might be viewed as a special case of the following theorem as applying to singular conics.

Theorem 52 ***(Pascal's Mystic Hexagon, 1640)*** *Let A, B, C, A', B', C' be six distinct points on a non-singular conic. Then the intersections*

$$P = AB' \cap A'B, \qquad Q = AC' \cap A'C, \qquad R = BC' \cap B'C,$$

are collinear.

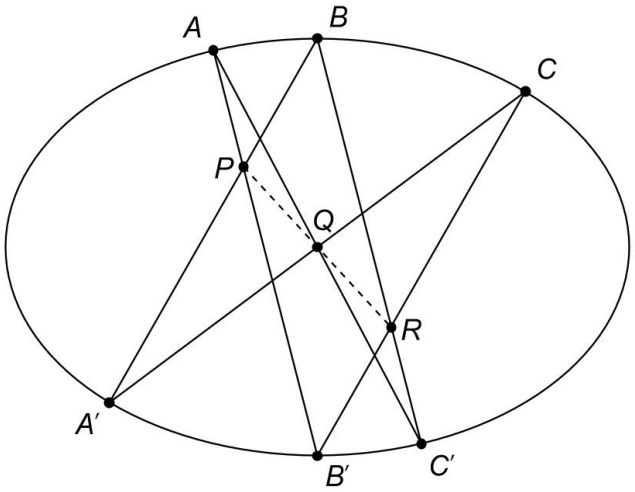

Fig. 7 – Pascal's Theorem

Proof The conic contains no line and hence the points A, B, A', B' are in general position. So we may assume them to have homogeneous co-ordinates

$$A = [1\colon 0\colon 0]\,, \qquad B = [0\colon 1\colon 0]\,, \qquad A' = [0\colon 0\colon 1]\,, \qquad B' = [1\colon 1\colon 1]\,.$$

Let $C = [x\colon y\colon z]$ and $C' = [X\colon Y\colon Z]$, noting that x, y, z, X, Y, Z are necessarily non-zero or else three points will be collinear. We then have

$$\begin{aligned} P &= AB' \cap A'B = \{x_1 = x_2\} \cap \{x_0 = 0\} = [0\colon 1\colon 1]\,, \\ Q &= AC' \cap A'C = \{Zx_1 = Yx_2\} \cap \{yx_0 = xx_1\} = [xY : yY : yZ]\,, \\ R &= BC' \cap B'C = \{Zx_0 = Xx_2\} \cap \{(z-y)x_0 + (x-z)x_1 + (y-x)x_2 = 0\} \\ &= [(x-z)X\colon (x-y)Z + (y-z)X\colon (x-z)Z]\,. \end{aligned}$$

Now the conic is represented by the symmetric matrix

$$\begin{pmatrix} 0 & \alpha & \beta \\ \alpha & 0 & -\alpha-\beta \\ \beta & -\alpha-\beta & 0 \end{pmatrix},$$

for some α, β, in order to pass through A, B, A', B'. As C also lies on the conic, we also have that

$$\alpha xy + \beta xz - (\alpha+\beta)yz = 0,$$

so that

$$\frac{\alpha}{\beta} = \frac{z(y-x)}{y(x-z)}.$$

As C' similarly lies on the conic then

$$\frac{z(y-x)}{y(x-z)} = \frac{Z(Y-X)}{Y(X-Z)}.$$

Multiplying up, and grouping the XY, YZ, ZX terms, this is equivalent to

$$z(y-x)XY + x\,(z-y)\,YZ + y(x-z)ZX = 0.$$

Now the three points P, Q, R are collinear precisely when

$$\Delta = \begin{vmatrix} 0 & 1 & 1 \\ xY & yY & yZ \\ (x-z)X & (x-y)Z + (y-z)X & (x-z)Z \end{vmatrix} = 0.$$

Note

$$\begin{aligned} \Delta &= \begin{vmatrix} 0 & 0 & 1 \\ xY & y(Y-Z) & yZ \\ (x-z)X & (x-y)Z + (y-z)X - (x-z)Z & (x-z)Z \end{vmatrix} \\ &= xY\,[(x-y)Z + (y-z)X - (x-z)Z] - yX(x-z)\,(Y-Z) \\ &= x(x-y)YZ + x(y-z)YX - x(x-z)YZ - yXY(x-z) + yXZ\,(x-z) \\ &= x(z-y)YZ + z\,(y-x)\,XY + y\,(x-z)\,XZ \\ &= 0, \end{aligned}$$

using the earlier condition. ■

Remark 53 *Given 5 points in a projective plane, no three of which are collinear, there is a unique nonsingular conic through the points (Sheet 2, Exercise 3). The converse of Pascal's theorem applies to 6 points, specificically: 6 points A, B, C, A', B', C', no three of which lie on a line, all lie on a conic if the intersections P, Q, R are collinear.*

Definition 54 *The **singular points** of a quadric $Q(\mathbf{v}) = \mathbf{v}^T X \mathbf{v} = 0$ are those points $[\mathbf{v}]$ where $X\mathbf{v} = \mathbf{0}$.*

So in case (ii) of Example 47, where $X = \mathrm{diag}(1, 1, 0)$, the unique singular point is $[0, 0, 1]$, the intersection point of the pair of lines. In case (iii) we have $X = \mathrm{diag}(1, 0, 0)$, then the singular points are the points on the line $z_0 = 0$: in other words every point on the conic is singular.

Remark 55 *The conic is nonsingular if and only if X is invertible, which is equivalent to the only solution to $Xv = 0$ being $v = 0$. So the conic is nonsingular if and only it has no singular points in projective space. This justifies the terminology in the definition above.*

If we work over $\mathbb{C}$ or $\mathbb{R}$, then we may further understand the notion of a singular point using ideas of multivariable differentiation. The conic is defined by the equation $f = 0$ where $f\colon v \mapsto v^T X v$. The derivative of f at v, in the sense of multivariable calculus, is $\mathrm{d}f_v\colon h \mapsto 2h^T X v$, which has maximal rank one unless $Xv = 0$. So the singular points are the points where $\mathrm{d}f_v$ has less than maximal rank, and hence where the manifold structure on the conic breaks down. In Example 47, this happens in case (ii) exactly where the lines intersect.

Nonsingular conics actually have a very nice description. If we fix a point x on the conic, and take a projective line not containing x, then projection from x onto the line actually sets up a bijection between the conic and the line. (If $\mathbb{F} = \mathbb{C}$, this in fact defines a homeomorphism between the conic and the projective line, and hence the Riemann sphere, though note this is *not* a projective equivalence).

Theorem 56 *Let C be a nonsingular conic in the projective plane, and let x be a point of C. Let l be a projective line in the plane not containing x. Then there is a bijection $\alpha\colon l \to C$ such that $x, y, \alpha(y)$ are collinear, for $y \in l$.*

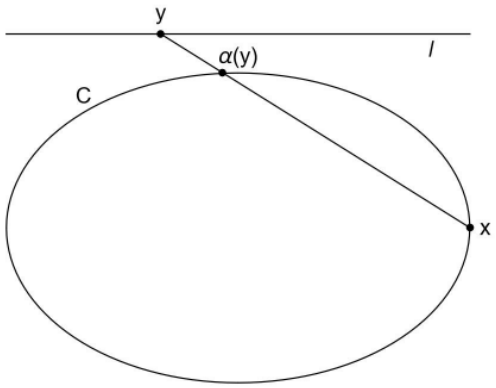

Fig. 8 – rational parameterization

Remark 57 *Note that the dual of the set of lines through x is a line in the dual plane. It would be more natural to set up a bijection between C and the lines through x. Under this bijection x corresponds to the tangent line through x.*

Proof Let B denote the nondegenerate, symmetric, bilinear form whose quadratic form Q defines the conic C. Let $x = [v]$ be a point on C, so that $B(v, v) = 0$.

For each $y \in l = \mathbb{P}(U)$, we want to see when (other than at x) the projective line containing x and y meets the conic. We will find that there is a unique such point $\alpha(y)$.

Let $y \in \mathbb{P}(U)$ have representative vector $u \in U$. As $x = [v]$ does not lie on $\mathbb{P}(U)$ then $x \neq y$ and v, u are linearly independent. Consider the 2-dimensional space W_u spanned by v and u, so the projective line we are constructing is $\mathbb{P}(W_u)$. Observe that the bilinear form B cannot be identically zero on the space W_u as C is non-singular.

With respect to the basis v, u, the form Q restricted to W_u is

$$Q(\lambda v + \mu u) = 2\lambda\mu B(v, u) + \mu^2 B(u, u)$$

and $B(v, u), B(u, u)$ are not both zero. So the projective line $\mathbb{P}(W_u)$ meets the conic at two points. One is the basepoint $x = [v]$, corresponding to $(\lambda, \mu) = (1, 0)$. The other, corresponding to $(\lambda, \mu) = (B(u, u), -2B(v, u))$, is defined to be $\alpha(y)$. Note that α is injective as given any point $z \neq x$ on the conic, the projective line through x, z meets the line $\mathbb{P}(U)$ in a unique point y. Moreover, $\alpha(y) = x$ exactly when $B(v, u) = 0$, which defines a unique point in $\mathbb{P}(U)$. ■

We have set up a bijection between a nonsingular conic and the projective line. This kind of bijection is called a **rational parameterization.**

The existence of a rational parameterization for the conic has some nice applications in the theory of Diophantine equations. These are polynomial equations where we are primarily interested in rational or integral solutions.

Example 58 *Consider the equation*

$$X^2 - Y^2 - Z^2 = 0,$$

whose solutions are Pythagorean triples. As our basepoint on the conic defined by the above equation we may take $[1\colon 1\colon 0]$. *We can take* $X = 0$ *as the projective line, which does not contain the basepoint. So if* y *is a point on the projective line with representative vector* $u = (0, \lambda_1, \lambda_2)$ *then*

$$\begin{aligned} \alpha(y) &= B(u,u)v - 2B(u,v)u \\ &= -(\lambda_1^2 + \lambda_2^2)(1,1,0) + 2\lambda_1(0, \lambda_1, \lambda_2) \\ &= (-(\lambda_1^2 + \lambda_2^2), \lambda_1^2 - \lambda_2^2, 2\lambda_1\lambda_2). \end{aligned}$$

It is clear that this does indeed give solutions to the equations. Replacing X *by its negative, we obtain the familiar formula for Pythagorean triples:*

$$X = s^2 + t^2 \quad : \quad Y = s^2 - t^2 \quad : \quad Z = 2st,$$

and by taking s, t *to be rational (respectively, integral) we get the solution in rational numbers (respectively, integers). For example,* $(s,t) = (2,1)$ *gives* $(X,Y,Z) = (5,3,4)$, *while* $(s,t) = (3,2)$ *and* $(4,3)$ *give the triples* $(13,5,12)$ *and* $(25,7,24)$ *respectively.*

Example 59 *Find a rational parameterization for the conic* $x^2 + xy + y^2 = 1$.

Solution A point on the conic is $(1,0)$. This time we will set up a bijection with lines passing through $(1,0)$, which have the form $y = q(x-1)$ where q is rational. We then find

$$x^2 + xq(x-1) + q^2(x-1)^2 = 1$$

which factorizes to

$$(x-1)\left(x + 1 + qx + q^2(x-1)\right) = 0.$$

The second root is

$$x = \frac{q^2 - 1}{1 + q + q^2},$$

so that

$$y = q(x-1) = \frac{-q(2+q)}{1+q+q^2}$$

so that

$$x = \frac{q^2-1}{1+q+q^2}, \qquad y = \frac{-q(2+q)}{1+q+q^2}.$$

Note that the point $(1,-1)$ is achieved only by setting the parameter $q = \infty$. Alternatively we can present all the solutions projectively as

$$[x_0\colon x_1\colon x_2] = \left[q^2 + q + 1\colon q^2 - 1\colon -q(2+q)\right].$$

■

Example 60 *Find all the rational solutions to Pell's equation*

$$x^2 - 2y^2 = 1.$$

Solution We will work with the inhomogeneous co-ordinates x and y. Note that the point $(1, 0)$ satisfies Pell's equation and consider the line $y = q(x-1)$ where q is rational. Substituting this into Pell's equation we find that

$$x^2 - 2q^2(x-1)^2 = 1.$$

This factorizes easily (and in any case we know $x = 1$ to be a root of the equation) and so we have

$$(x-1)(x+1-2q^2(x-1)) = 0.$$

The second root for x is then

$$x = \frac{2q^2+1}{2q^2-1},$$

and

$$y = q(x-1) = \frac{2q}{2q^2-1}.$$

■

Example 61 *Determine all the rational solutions* $(x, y) \in \mathbb{Q}^2$ *of the equation*

$$x^2 + 3xy + 2y^2 + y = 1.$$

Solution The projectivized curve has equation

$$x^2 + 3xy + 2y^2 + yz - z^2 = 0$$

which has associated matrix

$$X = \frac{1}{2}\begin{pmatrix} 2 & 3 & 0 \\ 3 & 4 & 1 \\ 0 & 1 & -2 \end{pmatrix}.$$

As the third column added to twice the second column equals three times the first column, X is singular and so in the conic. In fact, one can quickly spot that the defining equation factorizes as

$$(x + y + 1)\,(x + 2y - 1) = 0.$$

Thus the conic consists of two lines and the rational points on the conic either have the form $(q, -q-1)$ or $(1-2q, q)$ where q is rational. (If one fails to spot the factorization then it can be found by applying the quadratic formula, treating x as a constant and solving for y.)

Note that the two lines meet at $(-3, 2)$, which agrees with $[-3\colon 2\colon 1]$ being the singular point of the conic. We see

$$X\begin{pmatrix} -3 \\ 2 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 3 & 0 \\ 3 & 4 & 1 \\ 0 & 1 & -2 \end{pmatrix}\begin{pmatrix} -3 \\ 2 \\ 1 \end{pmatrix} = \mathbf{0}.$$

As X has rank 2, then this is the only singular point of the conic. ■

Given a non-singular conic C in a projective plane $\mathbb{P}^2$, then at each point there is a uniquely defined tangent line. This leads to a well-defined map from the conic to the dual projective space $\mathbb{P}^{2*}$. It turns out the image of C is a non-singular conic, called the **dual conic** in $\mathbb{P}^{2*}$.

Example 62 *Find a rational parameterization for the dual conic in* $\mathbb{P}^{2*}$ *of* $x_1^2+x_1x_2+x_2^2=x_0^2$.

Solution In the earlier example we found a rational parameterization for the conic to be

$$[x_0\colon x_1\colon x_2] = \left[q^2+q+1\colon q^2-1\colon -q(2+q)\right].$$

From our earlier proof of the existence of tangent lines, we know that any point $\mathbf{x}$ in the conic has tangent line with equation $\mathbf{y}^T X\mathbf{x}=0$ where the symmetric matrix X represents the bilinear form.

Recall that we identify the line $\alpha_0x_0+\alpha_1x_1+\alpha_2x_2=0$ with the point $[\alpha_0\colon \alpha_1\colon \alpha_2]$ in the dual space. As a symmetric matrix representing the conic is

$$X = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & \frac{1}{2} \\ 0 & \frac{1}{2} & 1 \end{pmatrix},$$

then the dual conic has a rational parameterization

$$\begin{aligned} [\alpha_0\colon \alpha_1\colon \alpha_2] &= \left[-q^2-q-1\colon q^2-1-\frac{1}{2}q(2+q)\colon \frac{1}{2}(q^2-1)-q(2+q)\right] \\ &= \left[-2q^2-2q-2\colon q^2-2q-2\colon -q^2-4q-1\right]. \end{aligned}$$

■

With this notion of a dual conic, we can describe the dual of Pascal's Theorem which is in fact another classical theorem of geometry, *Brianchon's Theorem.*

Theorem 63 ***(Brianchon, 1810)*** *If a hexagon is circumscribed about a conic, the three diagonals are concurrent.*

In the Part B course B3.3 *Algebraic Curves,* you will see that nonsingular curves of higher degree in the projective plane do not admit rational parameterizations. Indeed, over $\mathbb{C}$ such curves are not homeomorphic to the Riemann sphere. The genus of a degree d nonsingular curve in the complex projective plane is $\frac{1}{2}(d-1)(d-2)$ which is only zero for $d=1,2$ i.e. the case of lines and conics, whilst a nonsingular cubic is topologically a torus.

For further reading, introducing more ideas of algebraic geometry, see:

- F. Kirwan, *Complex algebraic curves*, LMS Student Texts, CUP, 1992.
- K. Smith, L. Kahanpää, P. Kekäläinen and W. Traves, *An invitation to algebraic geometry*, Springer Universitext, 2000.