2 Affine Geometry

2.1 Proportions and Affine Planes

While the notion of a proportion is geometrically intuitive, using the proportions in the denominator makes them sometimes inconvenient to use algebraically. If a line is parametrized in point-vector form, we can read off the proportions as follows:

Lemma 2.1 *The point $T = (1-t)P + tQ$ divides the segment PQ in the proportion $\tau = \frac{t}{1-t}$.*

Proof: Traveling from P to Q, the point T is reached in the above parametrization at time t, and there remains time $1-t$ to go. $\square$

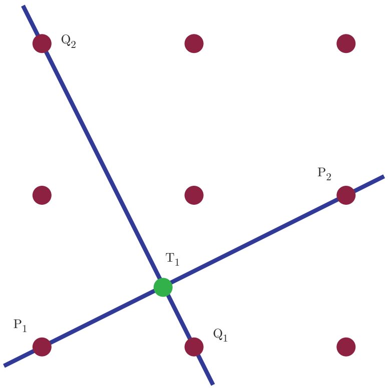


Figure 14 Basic proportion computation

Example 2.1 Let $P_1 = (0, 0)$, $P_2 = (2, 1)$, $Q_1 = (1, 0)$, $Q_2 = (0, 2)$. Find the proportions σ and τ in which the intersection point T of the segments P_1P_2 and Q_1Q_2 divides these segments. We write

$$T = (1 - s)P_1 + sP_2 = (1 - t)Q_1 + tQ_2$$

which becomes

$$T = \begin{pmatrix} 2s \\ s \end{pmatrix} = \begin{pmatrix} 1-t \\ 2t \end{pmatrix}$$

which has the solutions $s = \frac{2}{5}$ and $t = \frac{1}{5}$. This implies $\sigma = 2 : 3$ and $\tau = 1 : 4$.

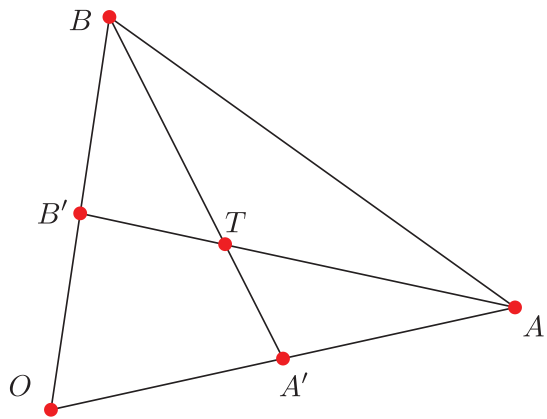


Figure 15 Intersection of Bisectors

Example 2.2 We can also argue with proportions when no explicit coordinates are given. As an example, we determine in which proportions the intersection of two midpoint bisectors of a triangle divide the bisectors. Let ΔOAB be a triangle as in **Figure 15**, and A' and B' be the midpoints of OA and OB, respectively. To determine the intersection T of AB' and BA', we interpret A, A' and B, B' as vectors with O as origin of our coordinate system. Then

$$T = (1 - s)A + sB' = (1 - t)B + tA' \ .$$

As $A' = \frac{1}{2}A$ and $B' = \frac{1}{2}B$, this implies

$$(1 - s)A + s\frac{1}{2}B = (1 - t)B + t\frac{1}{2}A \ .$$

Regrouping gives

$$(1 - s - \frac{1}{2}t)A = (1 - t - \frac{1}{2}s)B \ .$$

As the vectors A and B are linearly independent, this implies that

$$1 - s - \frac{1}{2}t = 0 = 1 - t - \frac{1}{2}s,$$

which has $s = t = \frac{2}{3}$. Hence T divides BA' and AB' in the proportion $2 : 1$.

This example still works if we replace the real numbers by any field in which we can divide by 2 and 3. Let's see what goes wrong if we use as field the set $\mathbb{F}_3 = \{0, 1, 2\}$ of integers modulo 3. Important new rules are $2 + 2 = 1 = 2 \cdot 2$ and $\frac{1}{2} = 2$.
The (affine) plane $\mathbb{F}_3^2$ consists of 9 points that we can represent in a 3×3 array. There are four lines through each point, with a total of 12 lines, each with three points on it. Thus the sets of points and lines in $\mathbb{F}_3^2$ is a configuration of type $9_4 12_3$, which is called the *Hesse configuration*.

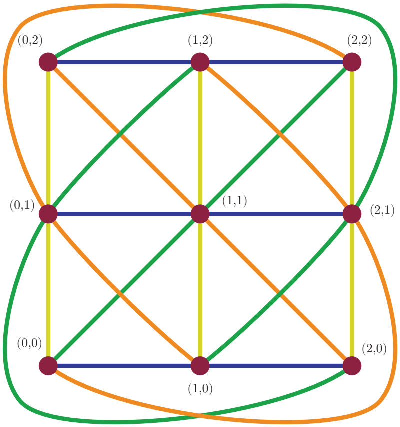


Figure 16 The Hesse configuration

It is easy to check that a midpoint of a segment is always the third point on the line extending that segment. Now for a triangle ΔABC in $\mathbb{F}_3^2$, the vector from the midpoint $\frac{1}{2}(B+C) = -B-C$ to A is equal to $A+B+C$, and this remains true if we use the midpoint bisectors ending at B or C. In other words, all three midpoint bisectors of a triangle are parallel in this geometry!

Exercise 2.1 Find an incidence homomorphism from the Desargues configuration to the Hesse configuration that is bijective for the set of points, and injective for the set of lines. In other words, find a realization of the Pappus configuration in the plane $\mathbb{F}_3^2$.

Exercise 2.2 In a parallelogram $abcd$ the edge bc is divided by e in the proportion $2:1$, and the edge ad is divided by f in the proportion $2:3$. Determine in what proportions the segments ae and bf intersect each other.

Exercise 2.3 Consider the triangle $\Delta(p_1p_2p_3)$ with

$$p_1 = (1,-1) \qquad p_2 = (4,1) \qquad p_3 = (2,3)$$

and the line through $(4,-9)$ and $(1,19)$. Compute the proportions r_i with which this line intersects the three lines p_1p_2, p_2p_3 and p_3p_1. Then compute $r_1r_2r_3$.

2.2 Background: Groups and Fields

We have two reasons to introduce *groups*: They serve as the main underlying mathematical structure to define *fields*, which in turn we need to define affine and projective spaces — two rich and important classes of incidence geometries. Secondly, we will use geometrically defined groups like the automorphism group of an incidence structure to study geometries.

Definition 2.1 A *group* is a set G with a distinguished *neutral element* e and an operation $*$ such that the following axioms hold

1. For all $a \in G$ we have $a * e = a = e * a$.
2. For all $a \in G$ there is an element $a^{-1} \in G$ such that $a*a^{-1} = e = a^{-1}*a$.
3. For all $a, b, c \in G$ we have the *associativity law* $a * (b * c) = (a * b) * c$.

If the group also satisfies the *commutativity law* $a*b = b*a$ then the group is called *abelian*.

The first set of examples is the one we have in mind for defining fields further on:

Example 2.3

1. The real numbers $(\mathbb{R}, +, 0)$ with addition as the operation form a group.
2. The non-zero real numbers $(\mathbb{R}^*, \cdot, 1)$ with multiplication as the operation form a group.
3. Similarly there are groups $(\mathbb{Q}, +, 0)$ and $(\mathbb{Q}^*, \cdot, 1)$ using the rational numbers.
4. Denote by $\mathbb{Z}_n = \{0, ..., n-1\}$ and define $a \oplus b$ as the remainder of $a+b$ after division by n. This is the *cyclic group* with n elements. Another common notation for this group is $\mathbb{Z}/n\mathbb{Z}$.

The next two examples show that there are very different kinds of groups. They will become important later:

Example 2.4 A *permutation* σ of $\{1, ..., n\}$ is an ordered list $(\sigma_1, ..., \sigma_n)$ with $\sigma_i \in \{1, ..., n\}$ and without repetition. In other words, the map $i \mapsto \sigma_i$ is a bijection of the set $\{1, ..., n\}$. Denote by S_n the set of all permutations of $\{1, ..., n\}$. We use as group multiplication the composition:

$$(\sigma \circ \tau)(i) = \sigma(\tau(i))$$

Then $(S_n, \circ)$ is called the *symmetric group* of order n. It has $n!$ elements.

Example 2.5 The set $GL_2(\mathbb{R})$ of invertible 2×2 matrices with real entries is a group. The neutral element is the identity matrix, and the operation is matrix multiplication. The inverse of an element is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

This shows that the set $\mathrm{SL}(2,\mathbb{Z})$ of 2×2 matrices with integer entries and determinant 1 is also a group, a *subgroup* of $GL_2(\mathbb{R})$.

Exercise 2.4 Why is the matrix product of two invertible matrices again invertible?

Exercise 2.5 Why is the set of real numbers with the subtraction as operation not a group?

In what follows, we will denote by $\mathbb{F}^* = \mathbb{F} - \{0\}$ the set $\mathbb{F}$ with the 0 element removed.

Definition 2.2 A *field* is a set $\mathbb{F}$ with two distinguished elements denoted by 0 and 1 and two operations denoted by $+$ (addition) and $\cdot$ (multiplication), that satisfy the following properties:

1. $(\mathbb{F}, +, 0)$ is a abelian group.
2. $(\mathbb{F}^*, \cdot, 1)$ is a abelian group.
3. The distributivity law $a \cdot (b + c) = a \cdot b + a \cdot c$ holds for all $a, b, c \in \mathbb{F}$.

By convention, we extend the multiplication so that $0 \cdot a = 0 = a \cdot 0$ for all $a \in \mathbb{F}$. Basic examples of fields are the real numbers $(\mathbb{R}, \cdot, +)$, the rational numbers $(\mathbb{Q}, \cdot, +)$, and the complex numbers $(\mathbb{C}, \cdot, +)$.

Exercise 2.6 Recall that a function is called *rational* if it can be written as the quotient of two polynomials. Using the addition and multiplication of functions as an operation, show that the set of all rational functions is a field.

For the purpose of geometry, we will mostly need the real and sometimes the complex numbers as fields. There are, however, also finite geometries that play an important role in coding theory, and they desire finite fields.

Definition 2.3 Let n be a positive integer, and denote by $\mathbb{F}_n$ the set $\{0, 1, ..., n-1\}$. We have defined an addition on $\mathbb{F}_n$ by adding the numbers as usual and then taking the remainder after division by n, this was the cyclic group of n elements. We can define a multiplication in the same way. For instance, modulo 7 we have $5 \cdot 6 = 30 = 2 \pmod 7$.

Theorem 2.1 *For a prime number p, the set $\mathbb{F}_p$ with modular addition and multiplication becomes a field.*

Proof: The crucial step is to show that $\mathbb{F}_p^* = \{1, ..., p-1\}$ with modular multiplication is a group. To see this, we first show that the modular product of non-zero elements $a, b \in \mathbb{F}_p$ is never 0. If $a \cdot b = 0 \pmod p$, then $p|a \cdot b$. As p is a prime number, this implies $p|a$ or $p|b$, so that $a = 0$ or $b = 0$.
Now consider for a fixed element $a \in F_p^*$ the map

$$\begin{aligned} A : \mathbb{F}_p^* &\to \mathbb{F}_p^* \\ b &\mapsto a \cdot b \end{aligned}$$

This map indeed maps into F_p^*. Furthermore it is injective: Suppose that $A(b) = A(c)$. Then $0 = A(b-c) = a(b-c)$. As $a \neq 0$, we have $b = c$. But an injective map from a finite set to itself is also surjective. In particular there is an element $b \in \mathbb{F}_p$ with $a \cdot b = 1$, and we have found the multiplicative inverse of a. $\square$

Exercise 2.7 Show that $\mathbb{F}_6$ is not a field with the modular addition and multiplication as operations.

Exercise 2.8 Find a number a so that $a^2 = 2$ in $\mathbb{F}_{17}$. Is there such a number in $\mathbb{F}_{19}$?

For any prime number p, we have constructed a field with p elements, and this is essentially the only field with p elements. There are also fields with p^n elements, where p is a prime number and n a positive integer. They are, however, for $n \geq 2$ not given just by the modular arithmetic of $\mathbb{Z}/p^n\mathbb{Z}$. The next exercise shows how to turn $\mathbb{F}_{3^2}$ into a field.

Exercise 2.9 Show that the set of pairs $\{(a, b) : a, b \in \mathbb{F}_3\}$ becomes a field by defining $(a, b) + (a'b') = (a + a', b + b')$ and $(a, b) \cdot (a'b') = (aa' - bb', ab' + a'b)$. If we write $1 = (1, 0)$ and $i = (0, 1)$, we can also write $a + bi = (a, b)$, and have the familiar identity $i^2 = -1$. Hint for the multiplicative inverse:

$$\frac{1}{(a, b)} = \frac{(a, -b)}{a^2 + b^2}$$

Why do we do not divide by 0? Does this also work if we replace $\mathbb{F}_3$ with $\mathbb{F}_5$?

2.3 Affine Spaces

In this section, we will introduce affine spaces which generalize Euclidean spaces. We begin by reviewing vector spaces.

Definition 2.4 A vector space V over a field $\mathbb{F}$ is a set with a distinguished element 0 and operations $+ : V \times V \to V$ and $\cdot : \mathbb{F} \times V \to V$ such that

1. $(V, +, 0)$ is an abelian group,
2. For all $r, s \in \mathbb{F}$ and $v \in V$, we have the mixed associativity law $r \cdot (s \cdot v) = (rs) \cdot v$,
3. For all $r, s \in \mathbb{F}$ and $v \in V$, we have the mixed distributivity law $(r+s) \cdot v = r \cdot v + s \cdot v$,
4. For all $r \in \mathbb{F}$ and $v, w \in V$, we have the mixed distributivity law $r \cdot (v + w) = r \cdot v + r \cdot w$,
5. For all $c \in V$ we have the compatibility law $1 \cdot v = v$.

Example 2.6 For any field $\mathbb{F}$, the standard example is the vector space $V = \mathbb{F}^n$ of ordered n-tuples of elements of $\mathbb{F}$. We write elements of these vector spaces as columns. The number n is called the *dimension* of the vector space. We define addition and scalar multiplication of vectors component wise. For instance, for $n = 2$ we write

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \end{pmatrix} \qquad \text{and} \qquad r\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} rv_1 \\ rv_2 \end{pmatrix}$$

These are all the vector spaces we will need. However, there are more, and they deserve to be mentioned at least:

Example 2.7 Let $\mathbb{F}^\infty$ be the set of all infinite sequences $f = (f_1, f_2, ...)$ with $f_i \in \mathbb{F}$. We define addition and multiplication with scalars component by component as above.

Exercise 2.10 How many elements do the vector spaces $\mathbb{F}_2^7$ and $\mathbb{F}_7^2$ have?

Many familiar properties of vectors follow from the axioms. For instance:

Proposition 2.1 *In a vector space V, $0 \cdot v = 0$.*

Note that the 0 on the left is $0 \in \mathbb{F}$, while on the right $0 \in V$.

Proof: We have

$$
\begin{aligned}
0 \cdot v &= (0 + 0) \cdot v \\
&= 0 \cdot v + 0 \cdot v
\end{aligned}
$$

Adding the additive inverse of $0 \cdot v$ to both sides proves the claim. $\square$

Proposition 2.2 *In a vector space V, $(-1) \cdot v = -v$.*

Before we begin with the proof, let's make sure we understand why there is something to show. The -1 is an element of the field $\mathbb{F}$, namely the additive inverse of the multiplicative neutral element 1. On the other hand, $-v$ is the additive inverse of v in the group $(V, +)$.

Proof: By **Proposition 2.1**

$$
\begin{aligned}
0 &= 0 \cdot v \\
&= (1 - 1) \cdot v \\
&= 1 \cdot v + (-1) \cdot v \\
&= v + (-1) \cdot v
\end{aligned}
$$

This shows that $(-1) \cdot v$ is the additive inverse of v. $\square$

Definition 2.5 A set of vectors $v_1, ..., v_n$ is *linearly independent* if and only if $\sum_{i=1}^{n} a_i v_i = 0$ implies that $a_i = 0$ for all i.

Example 2.8 The two vectors $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} -2 \\ -4 \\ -6 \end{pmatrix}$ are dependent as $2\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} -2 \\ -4 \\ -6 \end{pmatrix} = 0$. On the other hand, $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ and $\begin{pmatrix} 2 \\ 4 \\ -6 \end{pmatrix}$ are independent. The vector equation $\lambda\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \mu\begin{pmatrix} 2 \\ 4 \\ -6 \end{pmatrix} = 0$ is equivalent to the linear system of equations

$$\begin{aligned} \lambda + 2\mu &= 0 \\ 2\lambda + 4\mu &= 0 \\ 3\lambda - 6\mu &= 0 \end{aligned}$$

The last two equations determine $\lambda = \mu = 0$.

We are now ready to introduce affine spaces.

Definition 2.6 The *affine space* of dimension n over the field $\mathbb{F}$ is the set $\mathbb{F}^n$. An *affine plane* is a 2-dimensional affine space.

Why do we distinguish between the affine space $\mathbb{F}^n$ and the vector space $\mathbb{F}^n$ if they are the same sets anyway? The language of vector spaces includes the choice of the origin, vector subspaces, linear automorphisms, and more. On the other hand, the language of affine spaces will not have a distinguished point, but slightly different notions of affine subspaces and affine automorphisms. In essence, an affine space becomes a vector space after choosing the origin. This seems like a pedantic distinction to make, but avoids confusion.
However, we can and will use the tools from linear algebra to describe shapes and prove theorems. For instance:

Definition 2.7 Let $\mathbb{F}^n$ be an affine space. The line through the point $p \in \mathbb{F}^n$ in the direction of $v \in \mathbb{F}^n - \{0\}$ is the set $\{p + tv : t \in \mathbb{F}\}$. Two lines are called *parallel* if they have proportional direction vectors.

Every affine space defines an incidence geometry where the points are the elements of the space, and the lines are the subsets just defined. As expected, a point is incident with a line if the point is an element of the line.

Theorem 2.2 *In an affine plane $\mathbb{F}^2$, any two lines either intersect in a single point or are parallel. In this case, they are either equal, or disjoint.*

Proof: Let the two lines be given as lines through points p_1, p_2 and directions vectors v_1, v_2. We distinguish two cases: First suppose that the two direction vectors are linearly independent. Then they are a basis of $\mathbb{F}^2$, and the equation $p_1 - p_2 = t_1 v_1 - t_2 v_2$ has a unique solution t_1, t_2, determining the intersection as $p_1 + t_1 v_1 = p_2 + t_2 v_2$. If on the other hand v_1 and v_2 are linearly dependent, then v_1 and v_2 span a 1-dimensional subspace of $\mathbb{F}^2$. If $p_2 - p_1$ lies not in this subspace, the two lines are disjoint, because the equation $p_1 + t_1 v_1 = p_2 + t_2 v_2$ has no solution. Finally, if $p_2 - p_1$ lies in the subspace, we can show that the two lines are equal: To show that the first line is contained in the second, we have for every value of t_1 find a value t_2 such that $p_1 + t_1 v_1 = p_2 + t_2 v_2$. This is equivalent to $p_1 - p_2 + t_1 v_1 = t_2 v_2$. As both $p_1 - p_2$ and v_1 are multiples of v_2, this must be possible. Similarly we show that the second line is contained in the first. $\square$

So we expect many familiar properties of Euclidean geometry to still be valid in general affine geometries.
In an affine geometry over a finite field $\mathbb{F}_p$, any line consists of p points. To see this, we just need to show that no two elements in $\{p + tv : t \in \mathbb{F}\}$ are equal for different values of t. Suppose that $p + t_1 v = p + t_2 v$. Then $(t_2 - t_1)v = 0$, and as $v \neq 0$, this implies $t_1 = t_2$.

Exercise 2.11 In this exercise, we will study the affine plane $\mathbb{F}_3^2$.

1. How many point are in $\mathbb{F}_3^2$?
2. How many lines are in $\mathbb{F}_3^2$?
3. How many lines are in $\mathbb{F}_3^2$ that pass through the origin $(0, 0)$?
4. How many points lie on each line?

Solution: $\mathbb{F}_3^2$ is a Cartesian product, so there are $9 = 3 \cdot 3$ points. A line is given as a set $p + \lambda v$ where $\lambda \in \mathbb{F}_3$, so there are as many points on each lines as there are elements in $\mathbb{F}_3$, i.e. 3 points. To count the lines through the origin, we pick a point different from the origin. Then we know that there is precisely one line through the origin and the closen point, so we get $8 = 9 - 1$ lines. But we have counted each line twice, because besides the origin there are two more points on each line. Thus there are 4 lines through the origin. To count the total number of lines, we pick two different points in $\mathbb{F}_3$. There are $9 \cdot 8 = 72$ such choices.

Each determines a unique line through these points, but we have counted each line $6 = 3!$ times, as there are 3 points on each line. This there are $12 = 72/6$ lines all together.

2.4 Dilations, Translations, and Menelaus' Theorem

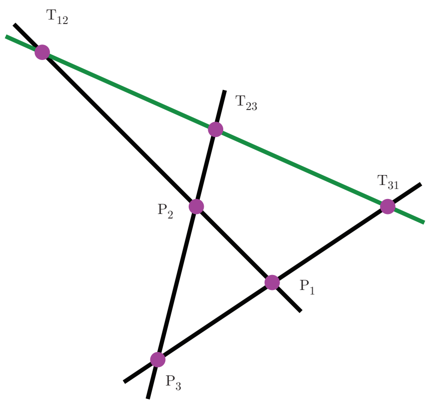


Figure 17 Menelaus' Theorem

In preparation of a proof of **Pappus's Theorem 1.3**, we will prove the following theorem:

Theorem 2.3 (Menelaus) *Let P_1, P_2, P_3 be three points in an affine plane $\mathbb{F}^2$ that are not collinear. Let T_{ij} divide the segment P_iP_j in the proportion $\tau_{ij} \neq -1$. Then the three points T_{12}, T_{23}, T_{31} are collinear if and only if $\tau_{12}\tau_{23}\tau_{31} = -1$.*

It is immediately clear that if we know in what proportions a line intersects two edges of a triangle, the proportion with which it divides the third edge is in principle determined. The importance of the theorem lies in the fact that the relation between the three proportions is in fact quite simple, so that this theorem might actually be useful.

Our first proof is computational. We chose P_1 as the origin of the affine plane $\mathbb{F}^2$ and thus can treat $\mathbb{F}^2$ as a vector space. Choose $\overrightarrow{P_1P_2}$ and $\overrightarrow{P_1P_3}$ as the basis vectors of $\mathbb{F}^2$. Thus we can abbreviate $a\,\overrightarrow{P_1P_2} + b\,\overrightarrow{P_1P_3}$ as $\begin{pmatrix} a \\ b \end{pmatrix}$.

By assumption,

$$T_{12} = \frac{1}{1+\tau_{12}}(P_1 + \tau_{12}P_2) = \frac{1}{1+\tau_{12}}\begin{pmatrix} \tau_{12} \\ 0 \end{pmatrix}$$

$$T_{23} = \frac{1}{1+\tau_{23}}(P_2 + \tau_{23}P_3) = \frac{1}{1+\tau_{23}}\begin{pmatrix} 1 \\ \tau_{23} \end{pmatrix}$$

$$T_{31} = \frac{1}{1+\tau_{31}}(P_3 + \tau_{31}P_1) = \frac{1}{1+\tau_{31}}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

By **Theorem 1.4**, the points T_{12}, T_{23}, T_{31} are collinear if and only if

$$0 = \det\begin{pmatrix} \frac{\tau_{12}}{1+\tau_{12}} & \frac{1}{1+\tau_{23}} & 0 \\ 0 & \frac{\tau_{23}}{1+\tau_{23}} & \frac{1}{1+\tau_{31}} \\ 1 & 1 & 1 \end{pmatrix}$$

As $\tau_{ij} \neq -1$, we can multiply each column by the appropriate τ_{ij} to clear the denominators without losing the test for being zero, and obtain

$$0 = \det\begin{pmatrix} \tau_{12} & 1 & 0 \\ 0 & \tau_{23} & 1 \\ 1+\tau_{12} & 1+\tau_{23} & 1+\tau_{31} \end{pmatrix} = \det\begin{pmatrix} \tau_{12} & 1 & 0 \\ 0 & \tau_{23} & 1 \\ 1 & 0 & \tau_{31} \end{pmatrix} = \tau_{12}\tau_{23}\tau_{31} + 1 \ ,$$

where we have subtracted the first two rows from the last in the second step.
To prepare a second proof, we will make use of affine transformations:

Definition 2.8 Let $\mathbb{F}^n$ be an affine space of dimension n over the field $\mathbb{F}$. An *affine transformation* is a mapping of the form

$$\begin{aligned} A : \mathbb{F}^n &\to \mathbb{F}^n \\ v &\mapsto Av + b \end{aligned}$$

where A is an $n \times n$ matrix with entries in $\mathbb{F}$ and b is an element of $\mathbb{F}^n$.

Injective affine transformations map lines to lines and points to points and are therefore examples of incidence homomorphisms.

Definition 2.9 A *translation* in the direction of $b \in \mathbb{F}^n$ is an affine transformation of the form $Av = v + b$.

The set of translations form a group under composition.

Definition 2.10 A *dilation* or *homothety* or *homothecy* or *uniform scaling* with center p and factor $\lambda \in \mathbb{F}^*$ is an affine transformation of the form $Av = \lambda(v - p) + p$.

Note that the set of dilations does not form a group, because the composition of dilations is a translation if the product of their scale factors is equal to 1.

Definition 2.11 A dilation-translation is an affine transformation of the form $Av = \lambda v + b$ with $\lambda \in \mathbb{F}^*$. They form a group under composition.

Exercise 2.12 In this exercise, we will study the special linear group $\mathrm{SL}_2(\mathbb{F}_3)$ of 2×2 matrices with elements in $\mathbb{F}_3$ and of determinant 1.

1. How many 2×2 matrices with entries in $\mathbb{F}_3$ have rank 0?
2. How many 2×2 matrices with entries in $\mathbb{F}_3$ have rank 1?
3. How many 2×2 matrices with entries in $\mathbb{F}_3$ have rank 2?
4. How many elements are in $\mathrm{SL}_2(\mathbb{F}_3)$?

Solution: There is only one matrix of rank 0, the 0-matrix. A matrix of rank 1 has a 1-dimensional column space, i.e. there is a line through the origin in $\mathbb{F}_3^2$ such that the columns of the matrix lie on this line. By the previous exercise, there are four such lines. For each of them, we pick a non-zero vector on that line, and write the two columns as multiples of the vector. The factors cannot be both 0, as otherwise the rank of the matrix would be 0. Hence there are $8 = 3 \cdot 3 - 1$ choices of factors, and thus a total of $32 = 4 \cdot 8$ matrices of rank 1.

As any 2×2 matrix has either rank 0, 1, or 2, and there are a total of $81 = 3^4$ 2×2 matrices, we can conclude that there are $48 = 81 - 1 - 32$ matrices of rank 2. Alternatively, we could also argue as follows: For the first column vector of a matrix of rank 2, we can pick any non-zero vector. There are 8 such choices. For the second column vector, we can take any vector that is not on the line through the origin and the first column vector. There are 6 such choices. Thus there are 48 matrices of rank 2. Arguing this way, we could eliminate the argument above that counts matrices of rank 1.

Finally, a rank 2 matrix has either determinant 1 or 2. There must be the same number of either kind, as we can change its determinant by multiplying the first column by 2. Thus there are 24 elements of $\mathrm{SL}_2(\mathbb{F}_3)$.

Exercise 2.13 Let $D_1 v = 2\left(v - \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) + \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ be a dilation in $\mathbb{R}^2$. Find another dilation $D_2 v = \lambda(v - p) + p$ such that $(D_2 \circ D_1)v = v + \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Exercise 2.14 The following puzzle is played on the set of points $\mathbb{Z}^2$ with integer coordinates in $\mathbb{R}^2$. The points $p_1 = (0,0)$, $p_2 = (1,-1)$, and $p_3 = (-2,1)$ are 'mirrors', and the player has a peg placed on some point. A move consists of jumping with the peg across any of the three mirrors. For instance, if the peg is at the point $(1,0)$, we can jump to $(-1,0)$, $(1,-2)$, or $(-5,2)$, depending on the mirror we use. Find a sequence of jumps that takes a peg at position $(1,0)$ to position $(1,2)$ that is different from the solution below.
Another formulation of the problem asks to find a word R in R_1, R_2, R_3, that, when interpreted as a composition of the affine transformations $R_i(v) = -(v - p_i) + p_i$, becomes the translation $R(v) = v + \begin{pmatrix} 0 \\ 2 \end{pmatrix}$.

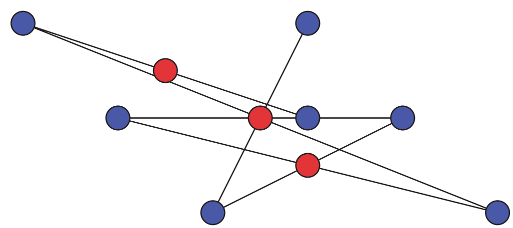


Figure 18 A solution to the jumping puzzle

Exercise 2.15 In $\mathbb{R}^2$, the circle with center $p = (x_0, y_0)$ and radius $r > 0$ is the set

$$S_r^2(p) = \{(x, y) \in \mathbb{R}^2 : (x - x_0)^2 + (y - y_0)^2 = r^2\}$$

Show that for any two circles there is a unique dilation-translation $D(v) = \lambda v + b$ with $\lambda > 0$ that maps the first circle to the second.

2.5 Menelaus' Theorem again, and Pappus's Theorem

Menelaus' Theorem 2.3 gives us a condition when points are collinear — a tool we need to prove **Pappus's Theorem 1.3**. As a warm-up, we will prove Menelaus' theorem a second time with fewer computations.

Theorem 2.4 *A dilation-translation A of an affine plane that maps a line l to itself is either the identity, a translation in the direction of the line, or a dilation with center on the line.*

Proof: We begin with a case distinction:

1. If A is the identity, we are done.

2. Let $Av = v + b$ be a translation, but not the identity. Then for a point $q \in l$, $b = Aq - q \neq 0$ is proportional to the direction vector of the line, so A is a translation in that direction.

3. Let A be a dilation with fixed point p, but not the identity. Suppose that p does *not* lie on l. Let $q \in l$ be an arbitrary point, and consider the unique line l' through p and q. Both l and l' are mapped to itself by A: This is true for

l by assumption, and for l' because the center of the dilation lies on l'. Thus their unique intersection q is also mapped to itself. As A is not the identity, it can only have one fixed point. Hence $p = q$, contradicting the assumption that p does not lie on l.

□

Lemma 2.2 *Assume that t divides pq in the proportion τ. Then the dilation factor λ of the dilation A with center at t that maps q to p is $\lambda = -\tau$.*

Proof: Check that $Av = -\tau(v - t) + t$ with $t = \frac{1}{1+\tau}(p + \tau q)$ maps q to p! □

Proof: We now give a second proof of **Menelaus' Theorem 2.3**. Let's first assume that $\tau_{12}\tau_{23}\tau_{31} = -1$. We have to show that T_{12}, T_{23} and T_{31} are collinear. Denote by A_{ij} the dilation of $\mathbb{F}^2$ with center at T_{ij} that maps P_j to P_i. By the Lemma above, A_{ij} has dilation factor $-\tau_{ij}$. None of these dilations can be the identity, as the triangle vertices are distinct points. The composition $A = A_{12} \circ A_{23} \circ A_{31}$ fixes P_1 and has dilation factor $\lambda = -\tau_{12}\tau_{23}\tau_{31} = 1$. Thus A is the identity, and in particular maps the line l through T_{23} and T_{31} to itself. Because the composition $A_{23} \circ A_{31}$ maps l to itself in any case, also A_{12} must map l to itself.

By **Theorem 2.4**, the fixed point T_{12} of A_{12} must lie on l, so that T_{12}, T_{23} and T_{31} are collinear as claimed.
Now assume that T_{12}, T_{23} and T_{31} lie on the same line l. We have to show that $\tau_{12}\tau_{23}\tau_{31} = -1$. The affine transformations A_{ij} map l to itself. Because the vertices of a triangle are not collinear by definition, not all three points P_i can lie on l. Let's assume that P_1 does not lie on l. Because A fixes P_1 and l, it must be the identity, by **Theorem 2.4**. Hence its dilation factor is equal to $1 = -\tau_{12}\tau_{23}\tau_{31}$. □

Now we come to a proof of **Pappus's Theorem 1.3**:

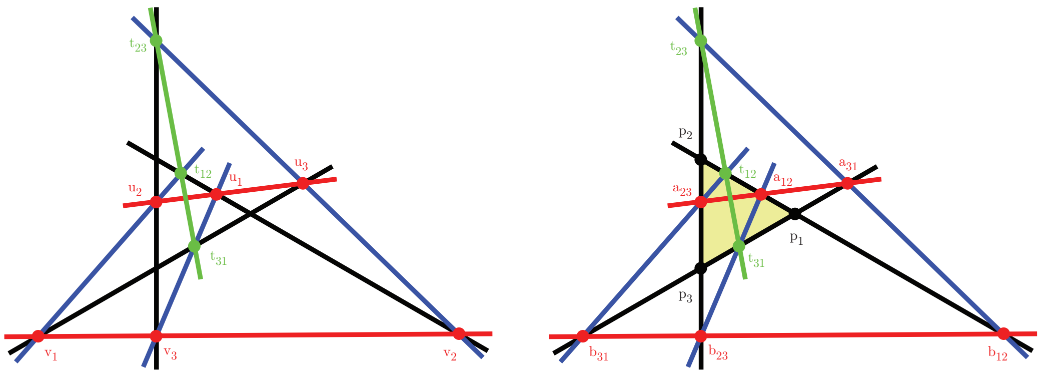


Figure 19 A proof of Pappus theorem

We first recall the setup: We have two triplets u_1, u_2, u_3 and v_1, v_2, v_3 of collinear points, placed on the red lines. Then we claim the the three points t_{12}, t_{23}, t_{31} are collinear (on the green line), where t_{ij} is the intersection of the two lines $u_i v_j$ and $u_j v_i$.

As **Menelaus' Theorem 2.3** gives us a criterion for collinearity, we need to find a triangle that is intersected by the lines through u_1, u_2, u_3 and v_1, v_2, v_3, and that has t_{12}, t_{23}, t_{31} on its edges. The natural candidates for the edges are the six lines $u_i v_j$. As we do not want any of the points of the configuration to become a vertex of the triangle, we have just two choices for picking three of the six lines: We choose the black lines $u_1 v_2$, $u_2 v_3$, $u_3 v_1$ and label their intersection points as p_1, p_2, p_3 so that the points t_{ij} lie on the line $p_i p_j$. The triangle defined by the black lines is our Menelaus triangle, marked yellow. Next we relabel the points u_i and v_i as a_{ij} and b_{ij}, again so that they lie on the line $p_i p_j$.

Denote by α_{ij} (resp. β_{ij} and τ_{ij}) the proportion with which a_{ij} (resp. b_{ij} and t_{ij}) divide the segment $p_i p_j$.

As by assumption the a_{ij} are collinear, we have by **Menelaus' Theorem 2.3** that $\alpha = \alpha_{12}\alpha_{23}\alpha_{31} = -1$, and likewise $\beta = \beta_{12}\beta_{23}\beta_{31} = -1$.

Our claim is that the t_{ij} are collinear, which is equivalent to $\tau = \tau_{12}\tau_{23}\tau_{31} = -1$, again by **Menelaus' Theorem 2.3**. We have not used the collinearity of the points on the remaining three blue lines. These give us

$$
\begin{aligned}
\alpha_{12}\beta_{23}\tau_{31} &= -1 \\
\alpha_{23}\beta_{31}\tau_{12} &= -1 \\
\alpha_{31}\beta_{12}\tau_{23} &= -1
\end{aligned}
$$

Multiplying both side of these three equations gives $\alpha\beta\tau = -1$, and hence $\tau = -1$ as claimed. Notice that it was essential to argue with just one Menelaus triangle, because every division point was used twice, and we need to be sure that the proportion is the same in each application.

2.6 Ceva's Theorem

Ceva's Theorem 2.7 is another simple situation where two proportions determine a third. Before we prove it, we will develop a tool that will allow us to prove theorems by just doing it in special cases: We first show that proportions are preserved by affine transformations.

Theorem 2.5 *Let A be an affine transformation, and let $p \neq q$ be two points. Assume that also $p' = Ap$ and $q' = Aq$ are distinct. Let t divide pq in the proportion τ. Then At divides $p'q'$ also in the proportion τ.*

Proof: Apply $Av = Lv + b$ to $t = \frac{1}{1+\tau}(p + \tau q)$ to get

$$\begin{aligned} At &= \frac{1}{1+\tau}(Lp + \tau Lq) + b \\ &= \frac{1}{1+\tau}(Ap + \tau Aq)\ . \end{aligned}$$

□

Next we show that we can use affine transformations to move points around quite flexibly.

Theorem 2.6 *Let $p_0, ..., p_n$ be points in affine space $\mathbb{F}^n$. Then there is an affine map that sends 0 to p_0 and the standard basis vectors $e_1 = (1, 0, ..., 0)$ etc. to p_i.*

Proof: To define $Av = Lv + b$, we set $b = p_0$ and use as L the $n \times n$ matrix whose column vectors are the vectors $p_i - p_0$. $\square$

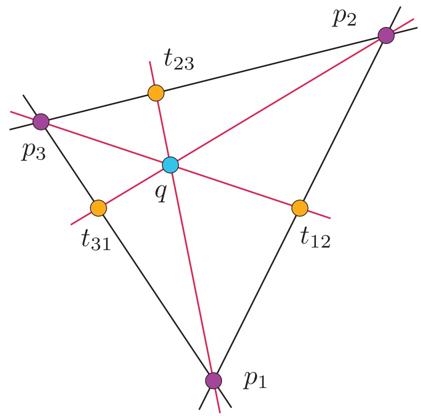


Figure 20 Ceva's Theorem

Theorem 2.7 (Ceva) *Let $\Delta p_1 p_2 p_3$ be a triangle in an affine plane $\mathbb{F}^2$. Denote by t_{ij} the points that divide $p_i p_j$ in the proportion $\tau_{ij} \neq -1$.*
Then the lines $p_k t_{ij}$ for $\{i, j, k\} = \{1, 2, 3\}$ are concurrent (or parallel) if and only if

$$\tau_{12}\tau_{23}\tau_{31} = 1 \ .$$

Proof: Let's first assume that the vertices of the triangle have the coordinates $p_1 = (1,0,0)$, $p_2 = (0,1,0)$, $p_3 = (0,0,1)$ in affine *space* $\mathbb{F}^3$. Then the points t_{ij} have coordinates

$$\tau_{12} = \frac{1}{1+\tau_{12}}(1, \tau_{12}, 0)$$

$$\tau_{23} = \frac{1}{1+\tau_{23}}(0, 1, \tau_{23})$$

$$\tau_{31} = \frac{1}{1+\tau_{31}}(\tau_{31}, 0, 1).$$

The lines through t_{ij} and p_k are given as the intersection of the triangle plane $x_1 + x_2 + x_3 = 1$ with the planes

$$\tau_{12}x_1 = x_2$$

$$\tau_{23}x_2 = x_3$$

$$\tau_{31}x_3 = x_1,$$

because each pair of points t_{ij} and p_k satisfies both equations.

Now let's first assume that the three lines are concurrent. Then there is a common intersection point (x_1, x_2, x_3) of the four planes, and its coordinates must satisfy all four equations. In particular, none of the x_i can be 0, because otherwise all $x_i = 0$ by the last three equations, contradicting that $x_1 + x_2 + x_3 = 1$. But then multiplying both sides of the last three equations and dividing by $x_1x_2x_3$ gives $\tau_{12}\tau_{23}\tau_{31} = 1$ as desired.

If on the other hand $\tau_{12}\tau_{23}\tau_{31} = 1$ and the three lines are not all parallel, at least two of them intersect in a point q. For the sake of concreteness, let's assume these are the lines p_1t_{23} and p_2t_{31}. Then the point q will satisfy the last two equations $\tau_{23}x_2 = x_3$ and $\tau_{31}x_3 = x_1$. Because of $\tau_{12}\tau_{23}\tau_{31} = 1$, it must also satisfy the first equation $\tau_{12}x_1 = x_2$, which means that q also lies on p_3t_{12} as claimed.

To prove the theorem for an arbitrary triangle in $\mathbb{F}^2$ with vertices p_1, p_2, p_3, take an affine map $A : \mathbb{F}^3 \to \mathbb{F}^2$ that sends the standard coordinate vectors to p_i. This is a bijective affine map from the affine plane $x_1 + x_2 + x_3 = 1$ to $\mathbb{F}^2$. As bijective affine maps preserve proportions, we are done. $\square$

The main reason why this proof works so easily is that we have replaced the somewhat complicated description of a line in the plane by the easier description of a plane in space that passes through the line and the origin. Similarly, points in the plane can be represented by a line through the origin and the point. This is the general motivation to introduce projective spaces.

Exercise 2.16 Consider the triangle with vertices $p_1 = (1,2)$, $p_2 = (2,3)$, and $p_3 = (4,1)$ in the affine plane $\mathbb{F}_5^2$ over the field $\mathbb{F}_5$ with 5 elements. The side p_ip_j is being divided by the points t_{ij} in the proportions $\tau_{12} = 1$, $\tau_{23} = 2$, and $\tau_{31} = 3$. Are the three lines p_1t_{23}, p_2t_{31}, and p_3t_{12} concurrent? If yes, determine their common intersection.

Exercise 2.17 Let $\Delta = (p_1, p_2, p_3)$ be a triangle in $\mathbb{R}^2$, with the three vertices not collinear. Let q be another point that does not lie on any of the sides of the triangle. The lines p_iq intersect the edge p_jp_k in a point t_{jk}. Here the indices are all distinct, i.e. $\{i,j,k\} = \{1,2,3\}$. The point q divides the line p_it_{jk} in the proportion σ_{jk}, We are told that $\sigma_{23} = \frac{5}{6}$ and $\sigma_{31} = \frac{8}{3}$. Determine σ_{12}.

Solution: As proportions are invariant under affine transformations, we can assume that $q = (0,0)$, $p_1 = (1,0)$, and $p_2 = (0,1)$. By the definition of proportions,

$$q = \frac{1}{1+\sigma_{jk}}(p_i + \sigma_{jk}t_{jk}) \ .$$

Using this for $(i,j,k) = (1,2,3)$ with the given values implies

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = \frac{6}{11}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{5}{6}t_{23}\right) \ .$$

so that $t_{23} = (-\frac{6}{5}, 0)$. Using this for $(i, j, k) = (2, 3, 1)$ gives similarly $t_{31} = (0, -\frac{3}{8})$. Now we determine p_3 as the intersection of $p_1 t_{31}$ with $p_2 t_{23}$. This is accomplished by solving

$$p_3 = s p_1 + (1 - s) t_{31} = t p_2 + (1 - t) t_{23}$$

for s and t. This gives $p_3 = (-3, -\frac{3}{2})$.

Now we determine t_{12} as the intersection of $p_3 q$ with $p_1 p_2$ as $t_{12} = (\frac{2}{3}, \frac{1}{3})$. Finally, the proportion σ_{12} is determined by solving

$$q = \frac{1}{1 + \sigma_{12}} (p_3 + \sigma_{12} t_{12}) \ ,$$

which gives $\sigma_{12} = \frac{9}{2}$.

Exercise 2.18 Let $\Delta = (p_1, p_2, p_3)$ be a triangle in $\mathbb{R}^2$, with the three vertices not collinear. Let q be another point that does not lie on any of the sides of the triangle. Assume that the lines $p_i q$ intersect the edge $p_j p_k$ in a point q_i. Here the indices are all distinct, i.e. $\{i, j, k\} = \{1, 2, 3\}$. The point q divides the line $p_i q_i$ in the proportion σ_i. Show that

$$\sigma_1 \sigma_2 \sigma_3 = 2 + \sigma_1 + \sigma_2 + \sigma_3 \ .$$

Solution: Because proportions are preserved under affine transformations, we can assume that $p_1 = (1,0)$, $p_2 = (0,1)$, $p_3 = (0,0)$. Let $q = (x,y)$. Then the line p_1q intersects p_2p_3 in the point $q_1 = \left(0, \frac{y}{1-x}\right)$, and likewise the line p_2q intersects p_1p_3 in the point $q_2 = \left(\frac{x}{1-y}, 0\right)$. We are given that q divides p_1q_1 in the proportion σ_1, this implies that $x = \frac{1}{1+\sigma_1}$. Likewise, q divides p_2q_2 in the proportion σ_2 implying that $y = \frac{1}{1+\sigma_2}$. Now we can determine σ_3 in terms of σ_1 and σ_2: The line p_3q intersects p_1p_2 in the point

$$q_3 = \frac{1}{x+y}(x,y) = \frac{1}{2+\sigma_1+\sigma_2}(1+\sigma_2, 1+\sigma_1)\ ,$$

which divides p_3q_3 thus in the proportion

$$\sigma_3 = \frac{\sigma_1+\sigma_2+2}{\sigma_1\sigma_2-1}\ .$$

This implies the claimed identity.

3 Projective Spaces

3.1 Background: Dot and Cross Products

In this section, we will use a few properties of the dot and cross products. Let's recall their definition.

Definition 3.1 Let $\mathbb{F}$ be a field, and let $v, w \in \mathbb{F}^n$ be two vectors. Then

$$v \cdot w = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \bullet \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = v_1 w_1 + \ldots + v_n w_n$$

is called the *dot product* of v and w. We call v and w *orthogonal* or *perpendicular* if their dot product is equal to 0.

The dot product is an example of an *inner product*, which we will consider later in detail. Note that the dot product is a map that takes two vectors and has as a result

a scalar, i.e. an element of $\mathbb{F}$. In general, there is no multiplication of vectors that results again in a vector that has been found useful. However, in dimension 3, we have the cross product:
Let $\mathbb{F}$ be a field, and let $v, w \in \mathbb{F}^3$ be two vectors. Then

$$v \times w = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} \times \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ -v_1 w_3 + v_3 w_1 \\ v_2 w_3 - v_3 w_2 \end{pmatrix}$$

is called the *cross product* of v and w.
One feature of the cross product is that its result is a vector orthogonal to its arguments. In other words, we have

$$v \bullet (v \times w) = 0 = w \bullet (v \times w) \ .$$

This follows by a computation, or from the more general important formula

$$u \bullet (v \times w) = \det(u, v, w) \ .$$

3.2 The Real Projective Plane

Motivated by the proof of **Ceva's Theorem 2.7**, we will introduce the *real projective plane* $\mathbb{RP}^2$ as an incidence geometry. This is in preparation to introduce projective spaces over arbitrary fields.

Definition 3.2 Points in the real projective plane $\mathbb{RP}^2$ are lines in $\mathbb{R}^3$ through the origin, and lines in $\mathbb{RP}^2$ are planes in $\mathbb{R}^3$ through the origin. A point and line in $\mathbb{RP}^2$ are incident when the line in $\mathbb{R}^3$ representing the point in $\mathbb{RP}^2$ is contained in the plane in $\mathbb{R}^3$ representing the line in $\mathbb{RP}^2$.

The historical origin of the projective plane lies in the necessity to understand the foundations of *perspective drawing*.
The *central perspective* represents a 3-dimensional object in a planar drawing by connecting each point in space that is to be drawn with the center of perspectivity (the eye of the artist, which we make the origin of our affine space) by a line. Note that this line represents a point in the projective plane of all lines through the origin. The intersection of this line with a canvas plane is then drawn. Similarly, to represent in line in space, this line is extended to the plane containing the line and the origin, and its intersection in the canvas plane is the drawn representation of the line. This has the well-known effect that parallel lines in space that are not parallel to the

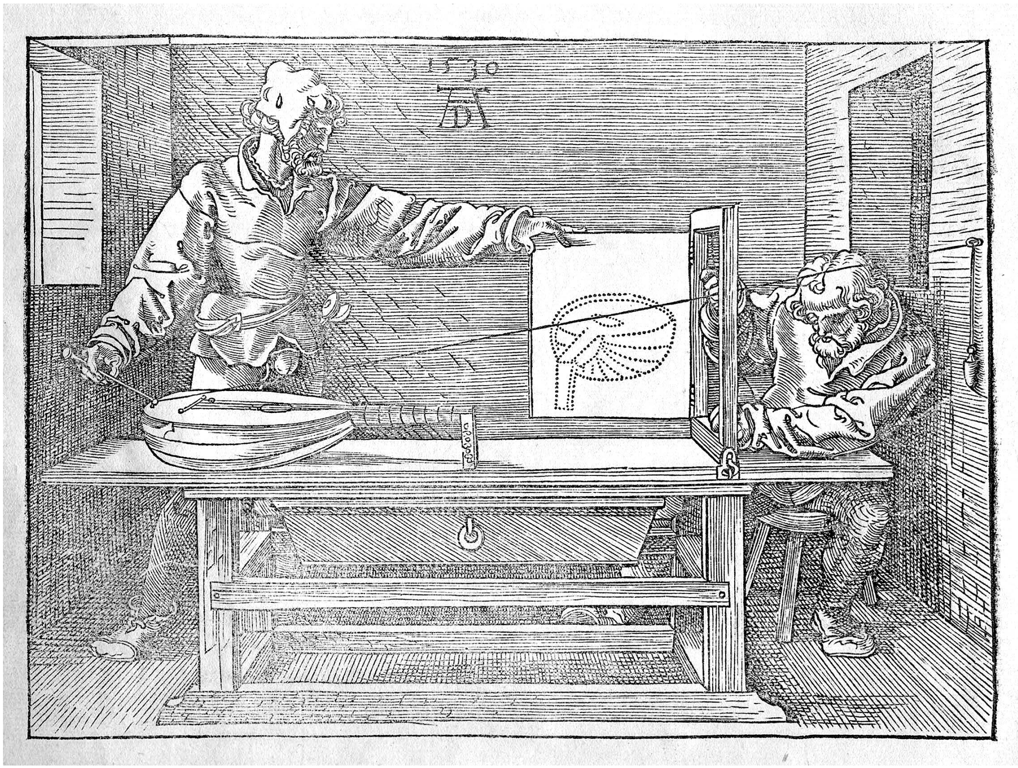


Figure 21 Instructions in perspective drawing (Albrecht Dürer 1530)

canvas are represented by lines on the canvas that intersect in a common point, the *vanishing point*. This is because the lines in space are extended to planes in space that all intersect in a line through the origin, which intersects the canvas in the vanishing point.

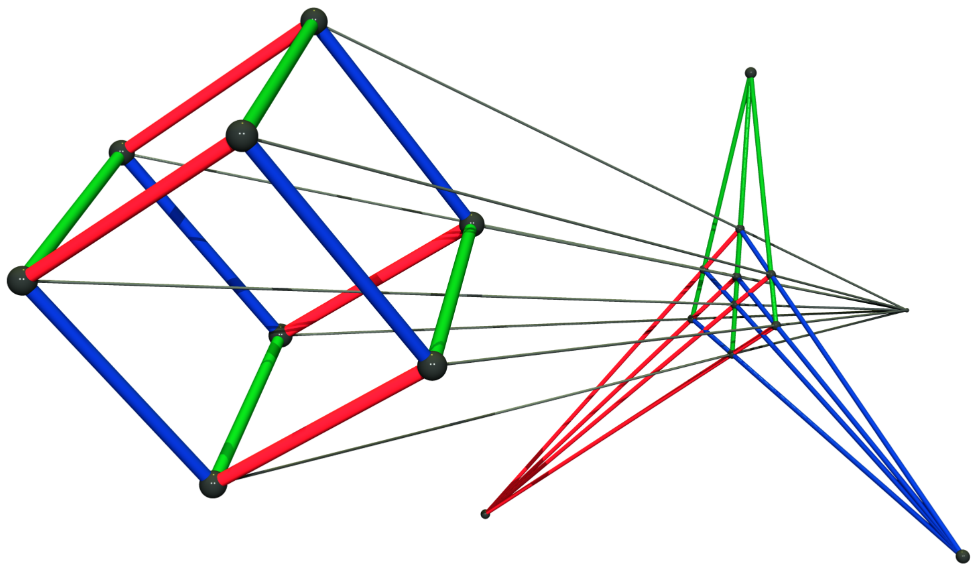


Figure 22 Central projection of a cube

Exercise 3.1 For a central projection, the center of perspectivity is at $(0, 0, 0)$, and the canvas plane is the plane $y = 1$. A cube is being projected onto the canvas. We are given that four parallel edges of the cube have their vanishing point at $(1, 1, 1)$, and four other parallel edges at $(-1, 1, 1)$. Determine the vanishing point of the third set of parallel edges of the cube. Hint: What can you say about the vectors from the center of perspectivity to the three vanishing points?

Solution: The central projection of a line in space is obtained by intersecting the plane that contains that line and the origin (i.e. the center of perspectivity) with the canvas. Parallel lines lie in planes through the origin that have the direction vector of the lines in common and thus intersect in a line through the origin in that direction. This line will intersect the canvas in the vanishing point of the parallel lines.

In our case this means that that three vectors to the vanishing points must be proportional to the three direction vectors of the edges of the cube. In particular, they are pairwise orthogonal. Thus the vector to the third vanishing point is a multiple of $(1, 1, 1) \times (-1, 1, 1) = (0, -2, 2)$. As the vanishing point lies in the plane $y = 1$, we have the solution $(0, 1, -1)$.

Next we would like to get some intuition about this new geometry. Each line in $\mathbb{R}^3$ through the origin intersects the 2-sphere in a pair of antipodal points. Hence, the real projective plane is also the set of antipodal points of the 2-dimensional sphere S^2. This description can be simplified further by throwing away from each pair of antipodal points the point in the lower hemisphere. This aloows us to think of the projective plane as the set of points in the upper hemisphere — with one problem: along the equator, antipodal points still occur in pairs and thus represent only one point in the projective plane. Flattening the upper hemisphere to a disk by projecting it vertically onto the xy-plane, we get a 2-dimensional description of the projective plane as a disk where antipodal points on the boundary circle are identified.

As a line in the projective plane is a plane in $\mathbb{R}^3$ through the origin, its intersection with the sphere becomes a great circle on the unit sphere, which projects to an ellipse (or a diameter) in the disk touching the boundary circle in opposite points. This is why projective geometry is sometimes also called *elliptic geometry*.

It is also instructive to look at a region in the sphere near its equator. This cylindrical region has again its antipodal points identified, and we can thus throw away the western part of it. What remains is an equatorial strip with two vertical arcs on the $0°$ and $180°$ meridians that are still identified, but with a half twist: This is known as a *Möbius strip*.

The Möbius strip has many remarkable properties. If you cut it along the closed inner core curve, you get a doubly twisted cylinder:

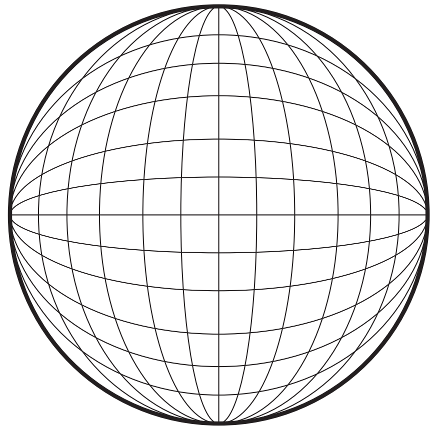
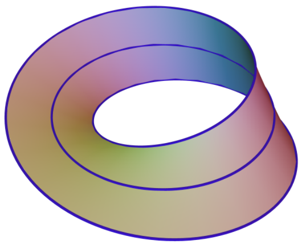
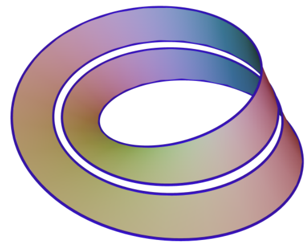


Figure 23 Projective lines in the disk model



with core circle



cut apart

Figure 24 The Möbius strip

Exercise 3.2 What do you get when you cut the Möbius strip along a curve that is $1/3$ away from its boundary (and winds around twice)?

Another feature of the Möbius strip is that its boundary is just one closed curve, in contrast to the cylinder, which has two closed boundary curves.
Surprisingly, one can arrange the Möbius strip in space without self-intersections so that its boundary curve is a true circle. Even more remarkable, all the blue curves in **Figure 25** are circular arcs.

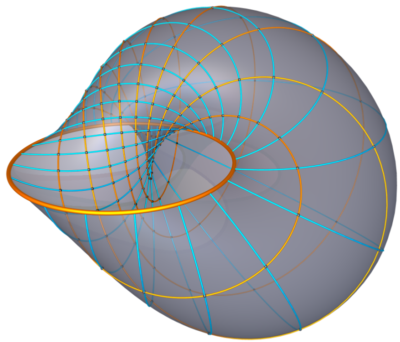


Figure 25 The Möbius strip with a circular boundary

Next we will develop some tools to be able to do computations in the projective plane. To describe a point in $\mathbb{RP}^2$, we take a point $(x_1, x_2, x_3) \in \mathbb{R}^3$ on the line representing the point, and denote the point in $\mathbb{RP}^2$ as $(x_1 \colon x_2 \colon x_3)$. Two such representations $(x_1 \colon x_2 \colon x_3)$ and $(y_1 \colon y_2 \colon y_3)$ define the same point in $\mathbb{RP}^2$ if there is $\lambda \in \mathbb{R}^*$ such that $(x_1, x_2, x_3) = \lambda(y_1, y_2, y_3)$. We say that the point is given by *homogeneous coordinates*.

To describe a line in $\mathbb{RP}^2$, recall that such a line is given by a plane in $\mathbb{R}^3$ through the origin. First suppose that the line is given by two points (x_1, x_2, x_3) and (y_1, y_2, y_3) that are not on a single line through the origin. Then the plane in $\mathbb{R}^3$ through these two points and the origin is the set

$$\Pi = \{\lambda(x_1, x_2, x_3) + \mu(y_1, y_2, y_3) : \lambda, \mu \in \mathbb{R}\}$$

and we can write the corresponding line l of points in $\mathbb{RP}^2$ as

$$l = \{(\lambda x_1 + \mu y_1 : \lambda x_2 + \mu y_2 : \lambda x_3 + \mu y_3) : \lambda, \mu \in \mathbb{R}\, (\lambda, \mu) \neq (0,0)\}$$

There is, however, a simpler way. A plane in $\mathbb{R}^3$ can also be given by a homogeneous linear equation

$$\Pi = \{(z_1, z_2, z_3) : a_1 z_1 + a_2 z_2 + a_3 z_3 = 0\}$$

for suitable $a_1, a_2, a_3 \in \mathbb{R}$, and the corresponding line in $\mathbb{RP}^2$ becomes

$$l = \{(z_1 : z_2 : z_3) : a_1 z_1 + a_2 z_2 + a_3 z_3 = 0\} \ .$$

Note that this makes sense as a homogeneous equation in the variables x_i, as it remains valid if we multiply them by the same real number.
In our case where the plane was given by two points we can find the homogeneous equation as follows: Let

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

$$\begin{pmatrix} x_2y_3 - x_3y_2 \\ -x_1y_3 + x_3y_1 \\ x_1y_2 - x_2y_1 \end{pmatrix}$$

be the *cross product* $a = x \times y$ of the vectors $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ and $y = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$. As the cross product is perpendicular to its two factors, we have $a \bullet x = 0 = a \bullet y$, so that both x and y satisfy the homogeneous equation $a \bullet z = a_1z_1 + a_2z_2 + a_3z_3 = 0$. Therefore all linear combinations $\lambda x + \mu y$ do so as well, and thus all points of the plane through x, y and the origin do.

3.3 Projective Spaces

Definition 3.3 A relation $\sim$ on a set S is called an *equivalence relation* if it satisfies the following axioms:

- (**r**eflexivity) For all $a \in S$ holds $a \sim a$.
- (**s**ymmetry) For all $a, b \in S$ holds that if $a \sim b$, then also $b \sim a$.
- (**t**ransitivity) For all $a, b, c \in S$ holds that if $a \sim b$ and $b \sim c$, then also $a \sim c$.

For $a \in S$, we denote by $[a]\{b \in S : a \sim b\}$ the *equivalence class* of a.

Exercise 3.3 Let G be a group and H a subgroup of G. Define a relation $a \sim b$ on G by $a \sim b \Leftrightarrow ab^{-1} \in H$. Show that this is an equivalence relation.

Proposition 3.1 *The set of equivalence classes $\{[a] : a \in S\}$ are a* partition *of S, i.e. they are either equal or disjoint, and their union is all of S.*

Proof: If $a \in S$, then $a \in [a] \subset S$, so the union of all equivalence classes is equal to S. Now let $a, b \in S$ and assume that $c \in [a] \cap [b]$. This means that $c \sim a$ and $c \sim b$. We have to show that $[a] = [b]$.

Let $a' \in [a]$. Then $a' \sim a$, which implies $a' \sim c$ and thus in turn $a' \sim b$, using transitivity. Thus $a' \in [b]$, and we have shown that $[a] \subset [b]$. By symmetry, we also have $[b] \subset [a]$, and are done. □

We denote the set of equivalence classes by $S/\sim$ and call it the quotient of S by the equivalence relation $\sim$. Note that we have a projection $S \to S/\sim$ which sends $s \to [s]$.

Exercise 3.4 Let $(G, \circ, 1)$ be a group. Define a relation $\sim$ on G by $a \sim b$ if and only if there is an element $g \in G$ such that $b = g \circ a \circ g^{-1}$. Show that this relation is an equivalence relation. For $G = S_4$ the symmetric group of four elements, determine the partition of S_4 into equivalence classes. Hint: Use the cycle representation of permutations.

Lemma 3.1 *Let $\mathbb{F}$ be a field and let $V = \mathbb{F}^{n+1}$. We call two elements $v, w \in V - \{0\}$* equivalent *and write $v \sim w$ if they lie on the same line through the origin, i.e. if there is $\lambda \in \mathbb{F}^*$ such that $w = \lambda v$. This is an equivalence relation. We call the set of equivalence classes $\mathbb{FP}^n = V/\sim$ the* projective space *of dimension n. For a $k+1$-dimensional subspace U of $\mathbb{F}^{n+1}$, we denote the set of equivalence classes by $\mathbb{P}(U) \subset \mathbb{FP}^n$ and call it a k-dimensional subspace of $\mathbb{FP}^n$. More conveniently, for a point $(x_1, ..., x_{n+_1}) \in \mathbb{F}^{n+1} - \{0\}$, we denote its equivalence class by $(x_1 \colon \cdots \colon x_{n+1})$.*

The affine plane $\mathbb{F}^n$ becomes a subset of $\mathbb{FP}^n$ as follows:
A point $x = (x_1, ..., x_n) \in \mathbb{F}^n$ can be augmented by adding additional coordinate 1, and taking the equivalence class, i.e. by sending

$$\begin{aligned} \mathbb{F}^n &\to \mathbb{FP}^n \\ (x_1, ..., x_n) &\mapsto (x_1 \colon ... \colon x_n \colon 1) \ . \end{aligned}$$

Geometrically, we are representing a point x in $\mathbb{F}^n$ by the line through the origin and the point $(x, 1)$ in the plane $x_{n+1} = 1$ just above $(x, 0)$.
Thus we see that a projective space of dimension n contains the affine space of the same dimension. What other points do we have in $\mathbb{FP}^n$? The remaining points

$(x_1 : \dots : x_{n+1})$ are precisely those that have $x_{n+1} = 0$, i.e. that are elements of the projective subspace $\mathbb{P}(\{x : x_{n+1} = 0\}$. Therefore we can write inductively

$$\begin{aligned}\mathbb{FP}^n &= \mathbb{F}^n \cup \mathbb{FP}^{n-1} \\ &= \mathbb{F}^n \cup \mathbb{F}^{n-1} \ldots \cup \mathbb{F}^1 \cup \mathbb{F}^0 \,.\end{aligned}$$

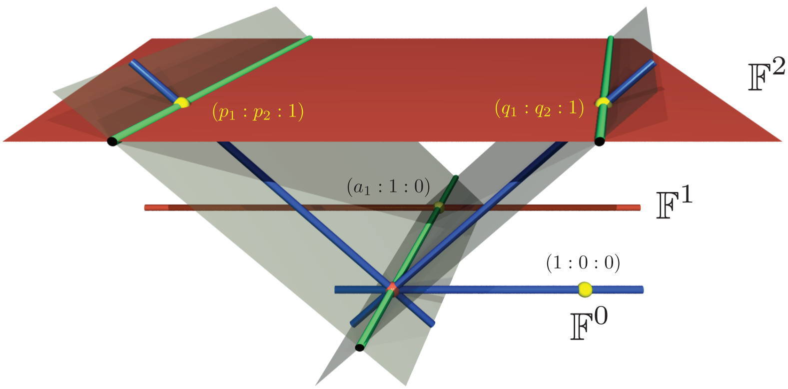


Figure 26 Even parallel lines intersect in a projective plane

Let's make this concrete by considering the complex projective line as $\mathbb{CP}^1 = \mathbb{C}^1 \cup \mathbb{C}^0 = \mathbb{C} \cup \infty$. Similarly, the real projective plane can be decomposed as $\mathbb{RP}^2 =$

$\mathbb{R}^2 \cup \mathbb{RP}^1 = \mathbb{R}^2 \cup \mathbb{R}^1 \cup \mathbb{R}^0$. Thus both $\mathbb{CP}^1$ and $\mathbb{RP}^2$ contain $\mathbb{C} = \mathbb{R}^2$ as subsets, but differ in how they *compactify* the set.
In a general projective plane, we have the following simple *collinearity test* for three points:

Lemma 3.2 *Three points $x = (x_1 : x_2 : x_3)$, $y = (y_1 : y_2 : y_3)$, $z = (z_1 : z_2 : z_3)$ in a projective plane $\mathbb{FP}^2$ are collinear if and only if*

$$\det(x, y, z) = \det \begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{pmatrix} = 0$$

Proof: Three points in $\mathbb{FP}^2$ are collinear if they are incident with the same line, i.e. if the corresponding lines in $\mathbb{F}^3$ lie in the same 2-dimensional subspace. This is the case if and only if the three vectors x, y, z are linearly dependent. □

Exercise 3.5 For which value of a is the line through the points $(1 : 2 : 1)$ and $(3 : 1 : 0)$ incident with the point $(a : -1 : -1)$?

Solution: We use the collinearity test from **Lemma 3.2**, and compute

$$\det \begin{pmatrix} 1 & 3 & a \\ 2 & 1 & -1 \\ 1 & 0 & -1 \end{pmatrix} = 2 - a \ .$$

Thus for $a = 2$ the points are collinear.

Exercise 3.6 Consider the projective plane $\mathbb{F}_3\mathbb{P}^2$ over the field with 3 elements. Show that the two triangles with vertices at $p_1 = (1\colon 1\colon 0)$, $p_2 = (1\colon 2\colon 1)$, $p_3 = (0\colon 2\colon 1)$ and $q_1 = (1\colon 0\colon 0)$, $q_2 = (1\colon 1\colon 1)$, $q_3 = (0\colon 0\colon 1)$ are in perspective centrally. Then verify Desargues' theorem by computing the three intersections of corresponding lines (like p_1q_1 with p_2q_2), and showing that they are collinear.

Exercise 3.7 Show that in the projective plane $\mathbb{F}_3\mathbb{P}^2$ over the field with 3 elements, the set of points and lines form a configuration of type 13_4.

Exercise 3.8 Show that the Hesse configuration in **Figure 16** can be realized in the complex projective plane $\mathbb{CP}^2$ by writing

$$\begin{aligned} p_{00} &= (0\colon -1\colon 1) & p_{01} &= (-1\colon 0\colon 1) & p_{02} &= (-1\colon 1\colon 0) \\ p_{10} &= (0\colon y\colon 1) & p_{11} &= (x\colon 0\colon 1) & p_{12} &= (y\colon 1\colon 0) \\ p_{20} &= (0\colon x\colon 1) & p_{21} &= (y\colon 0\colon 1) & p_{22} &= (x\colon 1\colon 0) \end{aligned}$$

for suitable complex numbers $x \neq y$.

3.4 Projective Lines, Planes and Transformations

A point in a projective plane $\mathbb{FP}^2$ is given by its homogeneous coordinates $x = (x_1 : x_2 : x_3)$ which represents the line $\lambda(x_1, x_2, x_3)$ in $\mathbb{F}^3$. Likewise, a line this projective plane can also be given by homogeneous coordinates $a = (a_1 : a_2 : a_3)$, which now represent the plane in $\mathbb{F}^3$ given by the homogeneous linear equation $\{x \in \mathbb{F}^3 : a \bullet x = a_1x_1 + a_2x_2 + a_3x_3) = 0\}$, where $a \bullet x$ is the *dot product* between a and x.

Thus we note that the lines in a projective plane can also be interpreted as points in another projective plane, the *dual projective plane*. We will explain this duality in a few examples.

First, notice that the test whether a line $x = (x_1 : x_2 : x_3)$ is incident with a plane $a = (a_1 : a_2 : a_3)$ is given by $a \bullet x = 0$.

The line through two different points x and y is given by $a = x \times y$.	The point of intersections of the two different lines a and b is given by $x = a \times b$.

This works because the cross product of two independent vectors in $\mathbb{F}^3$ is a non-zero vector whose dot product with the two given vectors is zero.

Three points x, y, z in $\mathbb{FP}^2$ are collinear if and only if $\det(x, y, z) = 0$.	Three lines a, b, c in $\mathbb{FP}^2$ are concurrent if and only if $\det(a, b, c) = 0$.

Here are two ways to see this: Three points in $\mathbb{FP}^2$ are collinear if the corresponding

lines in $\mathbb{F}^3$ lie in the same plane through the origin, which means that they are linearly dependent, which is being tested by the determinant condition. We can also argue as follows: The line through x an y is given by $x \times y$. The point z is incident with this line if $(x \times y) \bullet z = 0$. But we either know or are able to verify that $(x \times y) \bullet z = \det(x, y, z)$.
We can argue similarly for the concurrency, or as follows: Three lines a, b, c in $\mathbb{FP}^2$ are concurrent in x if and only if $a \bullet x = b \bullet x = c \bullet x = 0$. But this means that the matrix with rows a, b, c has $x \neq 0$ in its null space, so its determinant is 0.

Exercise 3.9 Find the equation of a line through the point $p = (1 : -1 : 2)$ that is concurrent with the two lines $2x + 3y - z = 0$ and $-x + y + 3z = 0$.

Solution: We first determine the intersection q of the two lines by using the cross product

$$p = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} \times \begin{pmatrix} -1 \\ 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 10 \\ -5 \\ 5 \end{pmatrix} \sim \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}.$$

The line through p and q is then given by a further cross product

$$p \times q = \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \times \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} = \begin{pmatrix} -1 \\ -3 \\ -1 \end{pmatrix}$$

so that the line has the equation $x + 3y + z = 0$.

Affine spaces had many incidence automorphisms that were given by matrices. We will now see that the same is true for projective spaces. Recall that for $x = (x_0, ..., x_n) \in \mathbb{F}^{n+1}$, we denote by $[x] = (x_0 : ... : x_n) \in \mathbb{P}\mathbb{F}^n$ the point in projective space.

Definition 3.4 Let $\mathbb{F}\mathbb{P}^n$ be a projective space, and $A \in \mathbb{F}^{(n+1)\times(n+1)}$ be an invertible matrix. Then we define for $x = (x_0, ..., x_n) \in \mathbb{F}^{n+1}$

$$A[x] = [Ax] \ ,$$

and call this the *projective linear transformation* given by A. This is well defined because matrix multiplication by A is linear.

Next we determine how projective transformations affect lines.

Exercise 3.10 Find the equation of the line that is the image of the line $x+2y+z = 0$ under the projective linear transformation given by

$$A = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Solution: As a first solution, we pick two points on the given line, say $p = (1 : 0 : -1)$ and $q = (2 : -1 : 0)$. Their images under A are $Ap = (1 : 1 : -1)$ and $Aq = (3 : 0 : -1)$. The line through these two points is given by $Ap \times Aq = (1 : 2 : 3)$ so that the equation of the line becomes $x + 2y + 3z = 0$.

This solution does not work well in theoretical arguments or when several image lines have to be computed. Here is a different approach:

Proposition 3.2 *The image of a line given by a vector a under the projective linear transformation given by a matrix A is given by the vector $(A^\top)^{-1}a$.*

Proof: We think of a as a column vector. Then a point p lies on the line given by a if $a^\top \cdot p = 0$. Here the row vector $a^\top$ is the *transpose* of the column vector a, and the product $a^\top \cdot p$ is matrix multiplication. Thus the image point Ap satisfies

$$\begin{aligned} ((A^\top)^{-1}a)^\top \cdot Ap &= a^\top A^{-1} Ap \\ &= 0 \end{aligned}$$

$\square$

In our example, we have

$$(A^\top)^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

and thus $(A^\top)^{-1}a = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ as before.

We have many more projective linear transformations of $\mathbb{FP}^n$ than affine linear transformation of $\mathbb{F}^n$. Let's look at this in a simple example:

Consider the projective line $\mathbb{FP}^1$, and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with entries in $\mathbb{F}$. First of all, we can think of the projective line as $\mathbb{FP}^1 = \mathbb{F}^1 \cup \mathbb{F}^0$: If for $(x_0 : x_1) \in \mathbb{FP}^1$ the coordinate $x_1 \neq 0$, we can write is as $\left(\frac{x_0}{x_1} : 1\right)$, or shorter as $\frac{x_0}{x_1}$. If on the other hand $x_1 = 0$, then necessarily $x_0 \neq 0$, and this means that there is only one point $(1 : 0)$ to consider, which we will denote succinctly as ∞. Because

$$A\left[\begin{pmatrix} x \\ 1 \end{pmatrix}\right] = \left[A\begin{pmatrix} x \\ 1 \end{pmatrix}\right] = \left[\begin{pmatrix} ax+b \\ cx+d \end{pmatrix}\right] \ ,$$

we can also just write Ax as the *Möbius transformation* $\frac{ax+b}{cx+d}$, which will be at the center of everything we do.
We know from **Theorem 2.6** that on an affine line we can find an affine linear transformation $y = ax + b$ that maps any two distinct points to any two other distinct points. We can do better with projective linear transformations:

Theorem 3.1 *For any three distinct points in the projective line $\mathbb{FP}^1$, there is a unique projective linear map $A : \mathbb{FP}^1 \to \mathbb{FP}^1$ that sends the three points to any three other distinct points.*

Proof: We will first show that we can map $(1 : 0)$, $(0 : 1)$ and $(1 : 1)$ to any three distinct points $a = (a_1 : a_2)$, $b = (b_1 : b_2)$, $c = (c_1 : c_2)$. As a and b are distinct, the vectors $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ and $\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ are linearly independent and form thus a basis of $\mathbb{F}^2$. Hence we can write

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \lambda \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} + \mu \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

with coefficients $\lambda, \mu \in \mathbb{F}$. Then

$$A = \begin{pmatrix} \lambda a_1 & \mu b_1 \\ \lambda a_2 & \mu b_2 \end{pmatrix}$$

satisfies $a = \left[A\begin{pmatrix}1\\0\end{pmatrix}\right]$, $b = \left[A\begin{pmatrix}0\\1\end{pmatrix}\right]$ and $c = \left[A\begin{pmatrix}1\\1\end{pmatrix}\right]$ as desired.

Now let a, b, c and a', b', c' be two triples of pairwise distinct points each. Let A and A' be the projective transformations that send $(1:0)$, $(0:1)$ and $(1:1)$ to a, b, c and a', b', c', respectively. Then $T = A' \cdot A^{-1}$ sends a, b, c to a', b', c' as desired. □

Exercise 3.11 Let T be the projective linear transformation that maps $(0:1:-1)$ to $(1:-1:0)$ to $(-1:0:0)$ to $(0:0:1)$ to $(0:1:-1)$. Find a point that is fixed by T.

Solution: The projective transformation that sends $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:1)$ to $(0:1:-1)$, $(1:-1:0)$, $(-1:0:0)$, $(0:0:1)$ is given by

$$T_1 = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and the projective transformation that sends $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, $(1:1:1)$ to $(0:1:-1)$, $(1:-1:0)$, $(-1:0:0)$, $(0:0:1)$, $(0:1:-1)$ is given by

$$T_2 = \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Then

$$T = T_2 T_1^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}$$

maps the four given points as desired. A point in $\mathbb{RP}^2$ is fixed by T if it is an eigenvector of T. T has as real eigenvalue only -1, and an eigenvector is given by $(1 : -1 : 1)$.

Exercise 3.12 In the projective plane $\mathbb{F}_3\mathbb{P}^2$, find a projective linear transformation in form of a 3×3 matrix that maps

$$(0 : 1 : 2) \mapsto (1 : 2 : 0) \mapsto (2 : 0 : 1) \mapsto (0 : 1 : 2)$$

Exercise 3.13 Let T be the projective linear transformation that maps $(1 : 1 : 1)$ to $(0 : 1 : 1)$ to $(1 : 0 : 1)$ to $(1 : 1 : 0)$ to $(1 : 1 : 1)$. Where does T map the point $(1 : 0 : 0)$?

Exercise 3.14 Let $\mathbb{FP}^2$ be a projective plane. A set of four points p_1, p_2, p_3, p_4 is a *projective frame* if no three of them are collinear. Suppose we have two projective frames p_1, p_2, p_3, p_4 and q_1, q_2, q_3, q_4. Show that there is a projective linear transformations that maps p_i to q_i for $i = 1, ..., 4$.

Exercise 3.15 Show that the Möbius transformations

$$f(z) = \frac{1}{1-z}$$

$$g(z) = \frac{z}{z-1}$$

generate a group of order 6 which is isomorphic to the symmetric group S_3 of three elements. Hint: What do these Möbius transformations do to 0, 1, and ∞?

Exercise 3.16 To which line does the projective linear transformation given by

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

map the line $x + y + z = 0$?

4 Conics

4.1 Historical Motivation

THEON OF SMYRNA wrote a little book about 100 AD, *Expositio rerum mathematicorum ad legendum Platonem utilium,* containing little mathematics but many historical anecdotes. Among them is a famous story: to get rid of a plague, the inhabitants of Delos consulted an oracle about what to do. The oracle demanded that they should double the volume of their existing, cube-shaped altar.

This perplexed the Greeks. In modern language, it required them to construct, with ruler and compass, the number $\sqrt[3]{2}$. This is the factor by which the edge length of the cube must be multiplied in order to double its volume. Now, while the Greeks were good at geometric constructions, they didn't know that one can only construct those numbers that can be obtained by standard arithmetic operations (addition, subtraction, multiplication, division) from the integers or by extracting square roots. In particular, extracting the cube root of 2 is impossible.

After a while the Greeks gave up and used other construction methods. HIPPOCRATES OF CHIOS knew that finding solutions of

$$\frac{1}{x} = \frac{x}{y}$$

is equivalent to extracting square roots $x^2 = y$, and he realized that by solving the two equations

$$\frac{1}{x} = \frac{x}{y} = \frac{y}{z}$$

simultaneously he would be able to solve $z = x^3$.
As was discovered by Menaechmus, this can be done by finding the intersection of the two parabolas (for $z = 2$)

$$y = x^2 \qquad \text{and} \qquad y^2 = xz$$

While this isn't a way to find $\sqrt[3]{2}$ with ruler and compass, it gives a mechanical way of constructing this point, as a parabola can be constructed mechanically.
The parabola belongs to a class of curves, the so-called *conic sections*, which are the simplest planar curves after the line and the circle. Besides the parabola, this class contains also the *ellipse* and the *hyperbola*.
All conic sections can be obtained, as the name suggests, by cutting a Euclidean cone with a plane. We will begin with a different description and come back to the cones later.

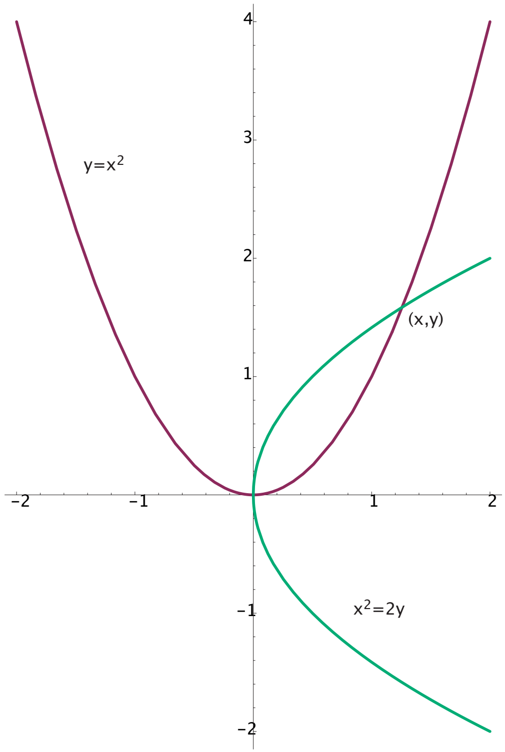


Figure 27 Doubling the cube by intersecting two parabolas

Definition 4.1 An *ellipse* is the set of points in the plane which has fixed distance sum d to two given *focal points* F_1 and F_2:

$$E = E_d(F_1, F_2) = \{P : |P - F_1| + |P - F_2| = d\}$$

In the special case of $F_1 = F_2$, we obtain a circle with center F_1 and radius $r = d/2$. Our first goal will be to find a parameterization of an ellipse. We will assume for simplicity that the focal points have coordinates $F_1 = (-f, 0)$ and $F_2 = (f, 0)$ and that the focal distance has the form $d = 2r$. Then a point with coordinates $P = (x, y)$ on the ellipse $E_d(F_1, F_2)$ satisfies the equation

$$|(x, y) - (-f, 0)| + |(x, y) - (f, 0)| = 2r$$

This is equivalent to

$$\sqrt{(x+f)^2 + y^2} = 2r - \sqrt{(x-f)^2 + y^2}$$

Squaring gives

$$(x+f)^2 + y^2 = 4r^2 - 4r\sqrt{(x-f)^2 + y^2} + (x-f)^2 + y^2$$

Rearranging, simplifying, and squaring again yields

$$(xf - r^2)^2 = r^2((x - f)^2 + y^2)$$

which finally can be rewritten as

$$\frac{x^2}{r^2} + \frac{y^2}{r^2 - f^2} = 1$$

This is the so-called *intercept form* of an ellipse. If we put $a = r$ and $b^2 = r^2 - f^2$, the new equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

describes an ellipse that intersects the coordinate axis in $(\pm a, 0)$ and $(0, \pm b)$. This ellipse can be parameterized using trigonometric functions as

$$c(t) = (a \cos t, b \sin t)$$

Theorem 4.1 *The radii from the two focal points F_1 and F_2 to the same point P on an ellipse cut the ellipse under the same angle.*

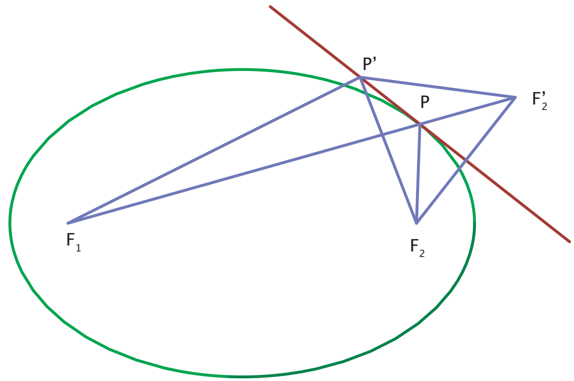


Figure 28 Reflective property of the ellipse

Proof: Reflect F_2 at the tangent line l to the ellipse at P, and denote its image by F_2'. The segment F_1F_2' intersects l in a point P'. Our first goal is to show that in fact $P = P'$.

$$
\begin{aligned}
F_1F_2{}' &= F_1P' + P'F_2{}' \\
&= F_1P' + P'F_2 \qquad \text{by symmetry across } l \\
&\geq F_1P + PF_2 \qquad \text{as } P' \text{ lies outside the ellipse} \\
&= F_1P + PF_2{}' \\
&= F_1F_2' \qquad \text{by symmetry across } l
\end{aligned}
$$

By the triangle inequality, the point P must lie on F_1F_2'. As it also lies on l, it must be the intersection point of these two lines and therefore coincide with P'. As

$$
\angle(PF_1, -l) = \angle(PF_2', +l) = \angle(PF_2, +l)
$$

the claim follows. □

This theorem has found its applications in architecture: In rooms with elliptical shape two people placed at the focal points can understand each other by whispering. A close relative to the ellipse is the hyperbola:

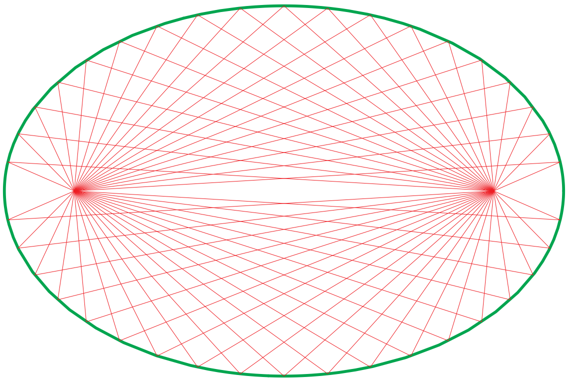


Figure 29 Sound waves meet in the focal points

Definition 4.2 A *hyperbola* is the set of points in the plane which have fixed distance difference $d = 2r$ to two given *focal points* F_1 and F_2:

$$H = H_d(F_1, F_2) = \{P : |PF_1 - PF_2| = d\}$$

Note that the region between the hyperbolas is given by the inequality

$$-d < |P - F_1| - |P - F_2| < d$$

A similar computations as the one above lets us find the intercept form of a hyperbola.

Proposition 4.1 *Let $H_d(F_1, F_2)$ be a hyperbola with focal points $F_1 = (-f, 0)$ and $F_2 = (f, 0)$ and focal distance $d = 2r$. Let $a = r$ and $b = \sqrt{r^2 - f^2}$. Then $H_d(F_1, F_2)$ is given by the equation*

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$$

Exercise 4.1 Prove this proposition.

The hyperbola also has a reflection law:

Theorem 4.2 *Let P be a point on a hyperbola with the two foci F_1 and F_2. Then the tangent to the hyperbola at P divides the angle F_1PF_2 in half.*

Proof: Reflect F_2 at the tangent through P and denote the image by F_2'. Connect F_1 with F_2' by a straight line and denote its intersection with the tangent by P'.

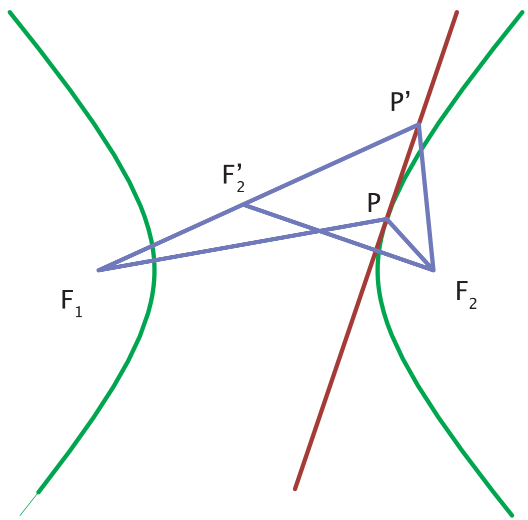


Figure 30 Reflection law for the hyperbola

We would like to show that F_2' actually lies on the line F_1P. As F_2' lies to the left of the right branch of the hyperbola, we know that

$$F_1P' - P'F_2 \leq F_1P - PF_2$$

using that $F_1P' = F_1F_2' + F_2'P' = F_1F_2' + F_2P'$ and $PF_2 = PF_2'$ gives

$$F_1F_2' + F_2'P \leq F_1P$$

so that by the triangle inequality, F_2' must lie on F_1P. □

A consequence of this is

Theorem 4.3 *Confocal hyperbolas and ellipses intersect each other orthogonally.*

Proof: Let P be a point of intersection of a hyperbola and an ellipse with same foci F_1 and F_2. The tangent to the hyperbola and the normal to the ellipse both halve the angle F_1PF_2 and hence must coincide. □

This planar theorem has higher dimensional generalizations. The following figure shows the pairwise orthogonal intersection of three quadric surfaces in space. This area was once of great interest; GASTON DARBOUX has written a whole book about such surfaces.

Exercise 4.2 The set of points in the plane that has a fixed distance product to two given points is called a *lemniscate*. Draw the lemniscate that consists all of points P such that $PF_1 \cdot Pf_2 = 2$ with $F_1 = (-1, 0)$ and $F_2 = (1, 0)$.

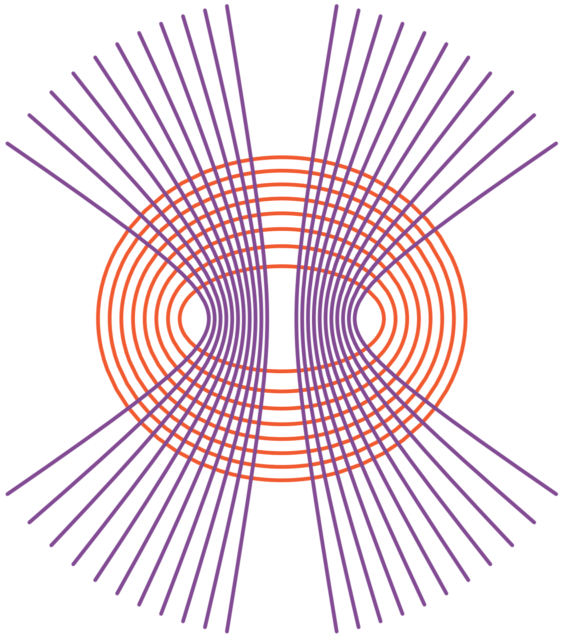


Figure 31 Confocal hyperbolas and ellipses intersect each other orthogonally

4.2 Dandelin's Spheres

The name *conic section* indicates that the ellipse and hyperbola have something to do with *cones*. In fact, one can obtain these curves by intersecting a suitable cone with a suitable plane.

That these intersections are truly ellipses, hyperbolas and parabolas follows from an amazingly simple geometric construction of GERMINAL PIERRE DANDELIN (1794–1847) which locates the focal points of the conic section in a very clever way.

We begin by intersecting the cone with a plane as shown in **figure 32**. We want to see why the green intersection E is an ellipse. Our first goal is two locate two points as candidates for the focal points.

We place a blue and a yellow sphere inside the cone so that they just touch the cone and the plane from both sides. Note that these spheres touch the cone in two circles in parallel planes. Let's call the points where the blue and yellow sphere touch the plane F_{blue} and F_{yellow}.

We now claim that these two points have the focal point property for the intersection E of the cone with the plane.

To see this, we draw an arbitrary line though the tip of the cone. It meets the top (blue) sphere in a point P_{blue}, the ellipse in a point P, and the bottom (yellow) sphere in a point P_{yellow}.

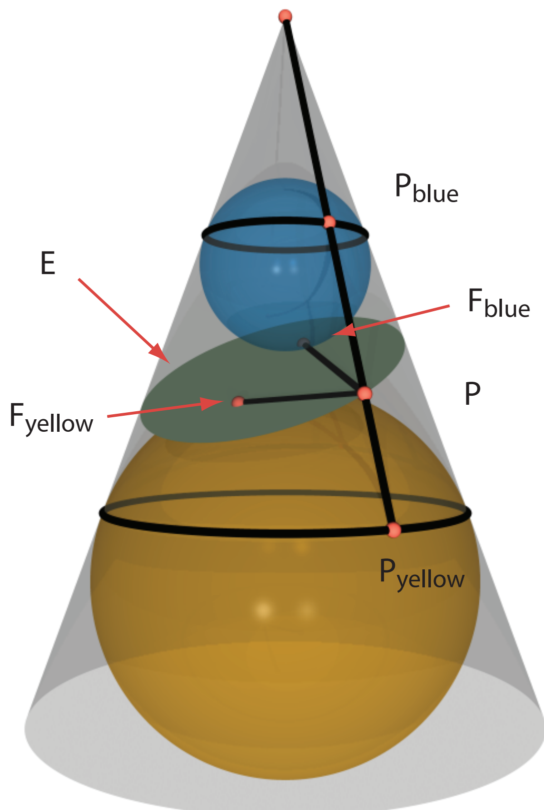


Figure 32 Dandelin's Spheres

Now we are going to use a very simple but useful fact: Whenever we have a sphere and a point outside the sphere all line segments through the point that touch the sphere will have the same length.
In particular, this means that the following distances in our figure are equal:

$$PF_{\text{blue}} = PP_{\text{blue}} \qquad \text{and} \qquad PF_{\text{yellow}} = PP_{\text{yellow}}$$

Adding these equations shows that

$$\begin{aligned} PF_{\text{blue}} + PF_{\text{yellow}} &= PP_{\text{blue}} + PP_{\text{yellow}} \\ &= P_{\text{yellow}}PP_{\text{blue}} \end{aligned}$$

because all points P, P_{blue}, and P_{yellow} lie on a line.
But this last distance is just the distance between the two circles in which the spheres touch the cone, and this is a constant independent of the choice of the line. Therefore the focal point property holds for F.

Exercise 4.3 Repeat the argument to show that the intersection of a double cone with a plane as in **figure 33** is a hyperbola.

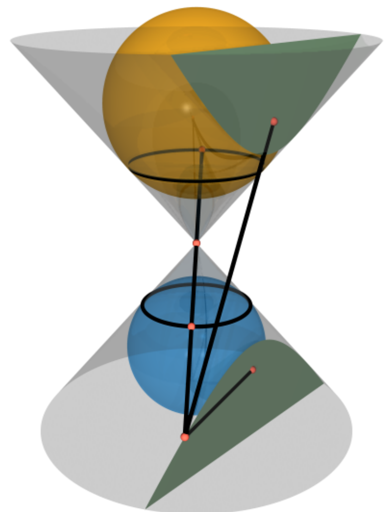


Figure 33 Dandelin's Spheres

4.3 Projective Conics

We will now introduce shapes other than just points and lines. While lines are given by a linear equation, we will now consider sets that can be described by a single quadratic equation.

Definition 4.3 Let $c(x_1, x_2, x_3)$ be a homogeneous quadratic polynomial with coefficients in the field $\mathbb{F}$. Then the set of points

$$C = \{(x_1 : x_2 : x_3) \in \mathbb{FP}^2 : c(x_1, x_2, x_3) = 0\}$$

is called a *conic*.

To get an intuition how these conics look like, we will first look at examples in $\mathbb{RP}^2$, the real projective plane, which we think of as the real affine plane $\mathbb{R}^2 = \{(x_1 : x_2 : 1) \in \mathbb{RP}^2\}$, together with a *line at infinity* $\mathbb{RP}^1 = \{(x_1 : x_2 : 0) \in \mathbb{RP}^2\}$.

Example 4.1

1. Let $c(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$. Then the zero set of this polynomial in the affine plane $x_3 = 1$ is the circle $x_1^2 + x_2^2 = 1$, and there are no points at infinity.

2. Let $c(x_1, x_2, x_3) = x_1 x_2 - x_3^2$. Then the zero set of this polynomial in the affine plane $x_3 = 1$ is the hyperbola $x_1 x_2 = 1$. At infinity ($x_3 = 0$), we get the equation $x_1 x_2 = 0$, which has the two solutions $(1 : 0 : 0)$ and $(0 : 1 : 0)$. Note that these are the intersections of the asymptotes $x_2 = 0$ and $x_1 = 0$ with the line at infinity.

3. Let $c(x_1, x_2, x_3) = (x_1 - x_2) \cdot (x_1 - x_3)$. Then the zero set of this polynomial in the affine plane $x_3 = 1$ are the two lines $x_1 = x_2$ and $x_1 = 1$. At infinity ($x_3 = 0$), we get the equation $(x_1 - x_2)x_1 = 0$, which has the two solutions $(1 : 1 : 0)$ and $(0 : 1 : 0)$. These two points are the points at infinity of the two lines.

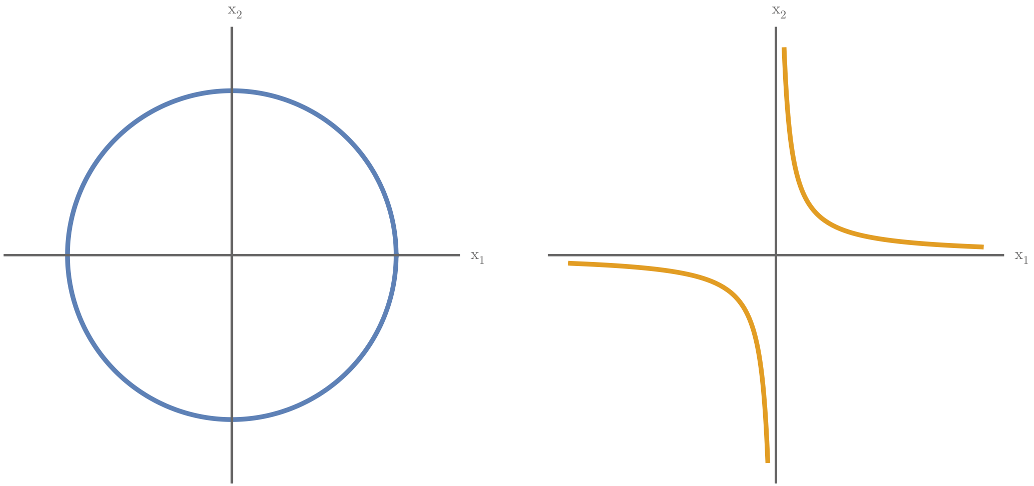


Figure 34 Two simple conics

Example 4.2 Let's now look at the conic given by $c(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$ in projective plane over the field $\mathbb{F}_5$. In the affine plane $x_3 = 1$, the equation becomes $x_1^2 + x_2^2 = 1$, which has the solutions $(1:0:1)$, $(4:0:1)$, $(0:1:1)$ and $(0:4:1)$. At the line $x_3 = 0$ at infinity, we get the equation $x_1^2 + x_2^2 = 0$, which has the solutions $(1:2:0)$ and $(1:3:0)$.

We have been successful so far to represent points and lines in the projective plane using coordinates, and computing with them using tools from linear algebra. Can we do the same with conics?

Lemma 4.1 *For a vector $x \in \mathbb{F}^3$ and matrix $C \in \mathbb{F}^{3\times 3}$, we have*

$$\begin{aligned} x^\top C x &= \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \cdot \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \\ &= c_{11}x_1^2 + c_{22}x_2^2 + c_{33}x_3^2 + (c_{12}+c_{21})x_1x_2 \\ &\quad + (c_{13}+c_{31})x_1x_3 + (c_{23}+c_{32})x_2x_3 \ . \end{aligned}$$

Thus we can describe any conic by a 3×3 matrix C as the set $\{x \in \mathbb{FP}^2 : x^\top C x = 0\}$. Note that when the characteristic of $\mathbb{F}$ is not 2 (so that we can divide by 2), we can replace c_{ij} with $\frac{1}{2}(c_{ij}+c_{ji})$, which defines the same conic by a *symmetric matrix*.
What does a projective transformation P do to a conic? If the conic is given by a matrix C and x lies on that conic, than x will satisfy the equation $x^\top C x = 0$. Thus Px will satisfy $(Px)^\top ({P^{-1}}^\top C P^{-1}) Px = 0$, so that Px will lie on the conic given by the matrix ${P^{-1}}^\top C P^{-1}$. In particular:

Proposition 4.2 *Projective transformations map conics to conics.*

4.4 Pascal's Theorem

As we have seen in **Exercise 1.3**, **Pappus's Theorem 1.3** appears also to be true when the six points don't lie on two lines but on a circle.
Even more generally, we have

Theorem 4.4 (Pascal's Theorem) *Given a conic in a projective plane* $\mathbb{FP}^2$ *and six points* a, b, c *and* a', b', c' *on the conic. Denote the intersection of the lines* ab' *and* $a'b$ *by* p, *of* ac' *and* $a'c$ *by* q, *and of* bc' *and* $b'c$ *by* r. *Then the three points* p, q *and* r *are collinear.*

Proof: To prove Pascal's theorem, we will use our computational skills in the projective plane. In principle, the argument is straightforward, as we can compute lines through points and intersections of lines as cross products, and determine whether three points are collinear using the determinant condition. However, using the coordinates of six points on a conic will be rather involved, and thus our first step will be to use a projective transformation to move three of the points into special locations.

Let's assume that either a, b, c or a', b', c' are *not* collinear — otherwise, we are in the case of **Pappus's Theorem 1.3**. Then, by **Exercise 3.14**, there is a projective transformation that sends a', b', and c' to $(1 : 0 : 0)$, $(0 : 1 : 0)$,

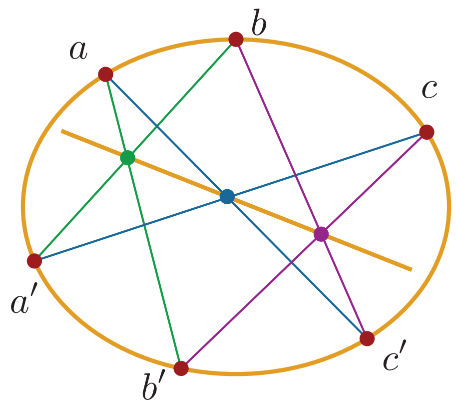


Figure 35 Pascal's Theorem

and $(0:0:1)$. This projective transformation will also map our conic to a new conic, which we now assume to be given by the equation

$$c_{11}x_1^2 + c_{22}x_2^2 + c_{33}x_3^2 + c_{12}x_1x_2 + c_{13}x_1x_3 + c_{23}x_2x_3 = 0\ .$$

The special location of a', b', and c' allows us to simplify this equation. For instance, as $a' = (1:0:0)$ lies on this conic, we have $c_{11} = 0$, and similarly $c_{22} = 0$ and $c_{33} = 0$. Thus our conic is simply given by $c_{12}x_1x_2 + c_{13}x_1x_3 + c_{23}x_2x_3 = 0$. We now begin the bulk work to determine the points p, q, and r. The lines ab' and $a'b$ are given by

$$a \times b' = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -a_3 \\ 0 \\ a_1 \end{pmatrix}$$

$$a' \times b = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0 \\ -b_3 \\ b_2 \end{pmatrix}$$

so that their intersection is

$$p = \begin{pmatrix} -a_3 \\ 0 \\ a_1 \end{pmatrix} \times \begin{pmatrix} 0 \\ -b_3 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_3 \\ a_3 b_2 \\ a_3 b_3 \end{pmatrix} .$$

Likewise, the lines ac' and $a'c$ are given by

$$a \times c' = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_2 \\ -a_1 \\ 0 \end{pmatrix}$$

$$a' \times c = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \times \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ -c_3 \\ c_2 \end{pmatrix}$$

so that their intersection is

$$q = \begin{pmatrix} a_2 \\ -a_1 \\ 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ -c_3 \\ c_2 \end{pmatrix} = -\begin{pmatrix} a_1 c_2 \\ a_2 c_2 \\ a_2 c_3 \end{pmatrix} .$$

Finally, the lines bc' and $b'c$ are given by

$$b \times c' = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \times \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b_2 \\ -b_1 \\ 0 \end{pmatrix}$$

$$b' \times c = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \times \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} c_3 \\ 0 \\ -c_1 \end{pmatrix}$$

so that their intersection is

$$r = \begin{pmatrix} b_2 \\ -b_1 \\ 0 \end{pmatrix} \times \begin{pmatrix} c_3 \\ 0 \\ -c_1 \end{pmatrix} = \begin{pmatrix} b_1 c_1 \\ b_2 c_1 \\ b_1 c_3 \end{pmatrix} .$$

To show now that p, q, and r are collinear, we have to show that $\det(p, q, r) = 0$, or

$$\det \begin{pmatrix} a_1b_3 & a_1c_2 & b_1c_1 \\ a_3b_2 & a_2c_2 & b_2c_1 \\ a_3b_3 & a_2c_3 & b_1c_3 \end{pmatrix} = 0 \ .$$

Let's divide the first column by a_3b_3, the second by a_2c_2, and the third by b_1c_1. This gives

$$\det \begin{pmatrix} a_1/a_3 & a_1/a_2 & 1 \\ b_2/b_3 & 1 & b_2/b_1 \\ 1 & c_3/c_2 & c_3/c_1 \end{pmatrix} = 0 \ .$$

Next we multiply the first row by a_2a_3, the second row by b_1b_3, and the third row by c_1c_2, which gives

$$\det \begin{pmatrix} a_1a_2 & a_1a_3 & a_2a_3 \\ b_1b_2 & b_1b_3 & b_2b_3 \\ c_1c_2 & c_1c_3 & c_2c_3 \end{pmatrix} = 0 \ .$$

Because we multiply and divide by the same numbers in the last two steps, the first and last matrices have in fact the same (symbolic) determinants. This is true even if one of the variables is 0.

We haven't used that a, b, c lie also on the conic. This means that

$$c_{12}\begin{pmatrix} a_1a_2 \\ a_1a_3 \\ a_2a_3 \end{pmatrix} + c_{13}\begin{pmatrix} b_1b_2 \\ b_1b_3 \\ b_2b_3 \end{pmatrix} + c_{23}\begin{pmatrix} c_1c_2 \\ c_1c_3 \\ c_2c_3 \end{pmatrix} = 0 ,$$

so that the matrix has linearly dependent rows and thus indeed determinant 0.

□

Our proof can also be used to show the following converse of **Pascal's Theorem 4.4**:

Corollary 4.1 *Let six points a, b, c and a', b', c' be given. Denote the intersection of the lines ab' and $a'b$ by p, of ac' and $a'c$ by q, and of bc' and $b'c$ by r. If the three points p, q and r are collinear, that the given six points lie on a conic.*

Proof: As in the proof above, we can assume that $a' = (1 : 0 : 0)$, $b' = (0 : 1 : 0)$, and $c' = (0 : 0 : 1)$. These points will lie on *any* conic of the form $c_{12}x_1x_2 + c_{13}x_1x_3 + c_{23}x_2x_3 = 0$. We can compute the three intersections p, q and r as before.Their collinearity implies that we can find c_{12}, c_{13} and c_{23} such that

$$c_{12}\begin{pmatrix} a_1a_2 \\ a_1a_3 \\ a_2a_3 \end{pmatrix} + c_{13}\begin{pmatrix} b_1b_2 \\ b_1b_3 \\ b_2b_3 \end{pmatrix} + c_{23}\begin{pmatrix} c_1c_2 \\ c_1c_3 \\ c_2c_3 \end{pmatrix} = 0 \ ,$$

which means that also a, b and c lie on that conic. □

Thus Pascal's theorem gives us a necessary and sufficient condition so that six points lie on a conic. We will see in **Theorem 4.7** that there is always a conic through five points if no three of them are collinear.
There are further generalizations of **Pappus's Theorem 1.3** and **Pascal's Theorem 4.4**. A nice book with some of them is (Evelyn et al., 1974).

4.5 Normal Forms of Real Conics

We have seen that the projective transformation T^{-1} maps the conic given by the symmetric matrix A to the conic given by the symmetric matrix $T^\top AT$.

Definition 4.4 Two $n \times n$-matrices A and B are called *similar* if there is an invertible $n \times n$-matrix T such that $B = T^\top AT$.

We leave it as an exercise to show that this is an equivalence relation. Equivalence classes of similar matrices are discussed in Linear Algebra as normal forms of matrices. We restrict our attention to real matrices.
Note that this notion of equivalence is different from the notion of equivalent matrices in the sense that $B = T^{-1}AT$. Matrices can be used to represent linear maps or quadratic forms on a vector space with respect to a basis. A change of basis given by T transforms the matrix into an equivalent matrix (in the case of maps) or into a similar matrix (in the case of forms).

Definition 4.5 An $n \times n$-matrix T is called *orthogonal* if $T^\top \cdot T = I$.

A standard fact is that a symmetric matrix has an orthonormal basis of eigenvectors. This is equivalent to

Theorem 4.5 *For any symmetric matrix $A \in \mathbb{R}^{n\times n}$ there is an orthogonal matrix T such that $A = T^\top DT$ for a diagonal matrix D.*

Definition 4.6 Two matrices A and B are called *equivalent* if there is an orthogonal matrix T such that $A = T^\top BT$.

We can use this theorem to determine equivalence classes of real symmetric matrices:

Definition 4.7 The *signature* of a symmetric matrix is the number of positive eigenvalues minus the number of negative eigenvalues.

Theorem 4.6 *A real symmetric matrix is equivalent to a diagonal matrix with diagonal entries ± 1 or 0.*

Proof: By the previous theorem, the matrix is equivalent to a diagonal matrix D. Denote by T the diagonal matrix whose entries are the reciprocals of the absolute values of the non-zero entries of D. Then $T^\top DT$ has the claimed form. $\square$

We can now classify all real conics up to projective transformations: They must be of the form $x^2 + y^2 = z^2$ in the case $\det A \neq 0$, because $x^2 + y^2 + z^2 = 0$ represents the empty set. If one eigenvalue is 0, we get $x^2 = y^2$, so the conic is the union of two lines. Finally, if two eigenvalues are 0, we have $x^2 = 0$, so the conic is one line, with multiplicity two.

In particular, we see that in the real projective plane ellipses and hyperbolas are affine images of the same conic.

Exercise 4.4 Find a projective linear transformation of $\mathbb{RP}^2$ that maps the conic $x^2 + y^2 = z^2$ to the conic $xz = y^2$. Verify your claim.

4.6 Lines and Conics

In this section we will assume that the base field has characteristic different from 2, i.e. that $1+1 \neq 0$. This allows us to represent a conic by a *symmetric* 3×3 matrix, and will avoid case distinctions.
We will also have to exclude sometimes that the conic is degenerate.

Definition 4.8 A conic is *non-degenerate* if it is given by an invertible matrix. Otherwise, the conic is called *degenerate*.

Examples of degenerate conics are unions of two lines. If two lines are given by $\alpha = \{x : a^\top \cdot x = 0\}$ and $\beta = \{x : b^\top \cdot x = 0\}$, then the conic given by the matrix

$$A = a \cdot b^\top = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 & b_3 \end{pmatrix} = \begin{pmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{pmatrix}$$

consists of just these two lines. To see this, note that $x^\top A x = (x^\top a)(x^\top b)^\top$ which is zero if and only if x lies on either line.

Proposition 4.3 *If three distinct points on a conic are collinear, then the conic is the union of two lines and thus degenerate.*

Proof: Assume that $p \neq q$ lie on the conic given by a symmetric matrix C. Then a point $sp+tq$ on the line through p and q lies on the conic if $(sp+tq)^\top C(sp+tq) = 0$. Expanding and using that p and q are on C gives $stp^\top Cq = 0$. Assuming that there is a third solution besides $s = 0$ or $t = 0$ implies that $p^\top Cq = 0$, so that in fact the entire line $sp+tq$ lies on the conic. Suppose the line is given by $a \bullet v = 0$. Then the quadratic polynomial $v^\top Av$ factors as $(a \bullet v)(b \bullet v)$ for some vector b.

□

Exercise 4.5 For which value of t is the conic $2x^2 - 2y^2 - tz^2 + 3xy - xz + 3yz = 0$ in in $\mathbb{RP}^2$ degenerate, and in which two lines does it decompose in this case?

Solution: The conic is represented by the matrix

$$A = \begin{pmatrix} 2 & \frac{3}{2} & -\frac{1}{2} \\ \frac{3}{2} & -2 & \frac{3}{2} \\ -\frac{1}{2} & \frac{3}{2} & -t \end{pmatrix}.$$

We compute

$$\det A = \frac{25}{4}(t-1)$$

which is zero if $t = 1$. In this case, we expect the polynomial $2x^2 - 2y^2 - z^2 + 3xy - xz + 3yz$ to become a product of two linear expressions. We show two ways to determine the factors. A general product of two linear expressions has the form $(a_1x + a_2y + a_3z)(b_1x + b_2y + b_3z)$. Expanding this and comparing coefficients gives the system of equations

$$a_1b_1 = 2 \qquad a_2b_2 = -2 \qquad a_3b_3 = -1$$
$$a_1b_2 + a_2b_1 = 3 \qquad a_1b_3 + a_3b_1 = -1 \qquad a_2b_3 + a_3b_2 = 2 \ .$$

Using the first three to eliminate b_1, b_2, b_3 from the last three equations gives

$$-2\frac{a_1}{a_2} + 2\frac{a_2}{a_1} = 3 \qquad -\frac{a_1}{a_3} + 2\frac{a_3}{a_1} = -1 \qquad -\frac{a_2}{a_3} - 2\frac{a_3}{a_2} = 3 \ .$$

Common denominators and factoring gives

$$(2a_1 - a_2)(a_1 + 2a_2) = 0 \qquad (a_1 - 2a_3)(a_1 + a_3) = 0 \qquad (a_2 + a_3)(a_2 + 2a_3) \ .$$

This gives eight choices of systems of three linear equations, depending on which factor we choose to be 0 in each product. Only two of them produce non-trivial solutions, for instance $a_1 = 1$, $a_2 = 2$ and $a_3 = -1$. This results in $b_1 = 2$, $b_2 = -1$, $b_3 = 1$. We can now check that indeed

$$2x^2 - 2y^2 - z^2 + 3xy - xz + 3yz = (x + 2y - z)(2x - y + z) \ .$$

The other solution just exchanges the two factors. Alternatively, we can diagonalize the matrix A for $t = 1$. We find the eigenvalues $\lambda_1 = -\frac{7}{2}$, $\lambda_2 = \frac{5}{2}$, and $\lambda_3 0$ with corresponding eigenvectors

$$e_1 = \begin{pmatrix} 1 \\ -3 \\ 2 \end{pmatrix} \qquad e_2 = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \qquad e_3 = \begin{pmatrix} -1 \\ 3 \\ 5 \end{pmatrix} .$$

To find a line on the conic, we write a point as $p = a_1 e_1 + a_2 e_2 + a_3 e_3$ and compute

$$\begin{aligned} p^\top A p &= a_1^2 \lambda_1 (e_1 \bullet e_1) + a_2^2 \lambda_2 (e_2 \bullet e_2) \\ &= a_1^2 (-\frac{7}{2})(14) + a_2^2 (\frac{5}{2})(10) \\ &= -(7a_1)^2 + (5a_2)^2 \ . \end{aligned}$$

This is equal to 0 for $7a_1 \pm 5a_2 = 0$. Thus we obtain two lines on the conic as the sets

$$
\begin{aligned}
l_1 &= \{5re_1 + 7re_2 + se_3 : r, s \in \mathbb{R}^2 - \{0\}\} \\
l_2 &= \{5re_1 - 7re_2 + se_3 : r, s \in \mathbb{R}^2 - \{0\}\} \ .
\end{aligned}
$$

We can find vectors representing the lines by taking the cross product of any two vectors on these lines. Namely,

$$
(5e_1 + 7e_2) \times e_3 = -70 \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix} \quad \text{and} \quad (5e_1 - 7e_2) \times e_3 = -70 \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix}
$$

so that we obtain the same factorization as before.

Through any two different points in a projective plane, there is a unique line. How many points determine a conic? Let's count parameters: A conic is given by a homogeneous quadratic equation in three variables, which has six coefficients. As scaling the parameters doesn't affect the conic, we count five effective parameters. On the other hand, each point on a conic will determine a linear equation for the coefficients. We thus expect to find a conic through five given points. More precisely, we have:

Theorem 4.7 *Given five points such that no three are collinear, there is a unique conic containing the five points.*

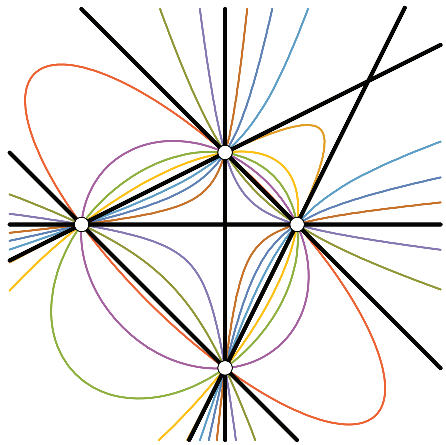


Figure 36 Conics through four points

Proof: Suppose we are given five points $p_1, ..., p_5$, no three of them collinear. Pick the first four, and form two *degenerate conics*. The first consists of the two lines $p_1 p_2$ and $p_3 p_4$, and is given by the matrix $A = (p_1 \times p_2) \cdot (p_3 \times p_4)^\top$. Similarly, the second degenerate conic consists of the two lines $p_1 p_3$ and $p_2 p_4$, and is given by the matrix $B = (p_1 \times p_3) \cdot (p_2 \times p_4)^\top$. All four points $p_1, ..., p_4$ lie on *both* degenerate conics, and therefore they will also lie on the conics given by $A + tB$ for any $t \in \mathbb{F}$.

Now the fifth point enters the game: As no three points of the points are collinear, p_5 does not lie on the conic defined by B, so that $p_5^\top B p_5 \neq 0$. Thus the equation $p_5^\top (A + tB) p_5 = 0$ has a unique solution t_0, and the conic given by $A + t_0 B$ will contain all five points $p_1, ..., p_5$.
For the uniqueness statement, assume that there are two conics C_1 and C_2 both containing five points $p_1, ..., p_5$. Let p_6 be a point on the line $p_1 p_2$ but different from p_1 and p_2, and by assumption also different from $p_3, ..., p_5$. By the same trick as before, we can find parameters $s, t \in \mathbb{F}$ so that $sC_1 + \mu C_2$ also contains p_6. But if a conic contains three collinear points it is degenerate, in which case it is a union of two lines. Thus all six points lie on two lines, and therefore three of the five given points must lie on one of the two lines, contradicting the assumption. $\square$

Example 4.3 Let's find the conic in $\mathbb{RP}^2$ through the five points $p_1 = (0 : -1 : 1)$, $p_2 = (0 : 2 : 1)$, $p_3 = (2 : 1 : 1)$, $p_4 = (2 : 2 : 1)$, $p_5 = (-4 : -1 : 1)$. As these points all lie in the affine plane $z = 1$ of $\mathbb{RP}^2$, we can visualize the points and compute the conic in $\mathbb{R}^2$:
The line l_{12} (resp. l_{34}) through p_1 and p_2 (resp. p_3 and p_4) has the equation $x = 0$ (resp. $x = 2$), so that the degenerate conic containing these two lines has the equation $x(x-2) = 0$. Similarly, the line l_{13} (resp. l_{24}) through p_1 and p_3 (resp. p_2 and p_4) has the equation $y = x - 1$ (resp. $y = 2$), so that the degenerate conic containing these two lines has the equation $(x-y-1)(y-2) = 0$.

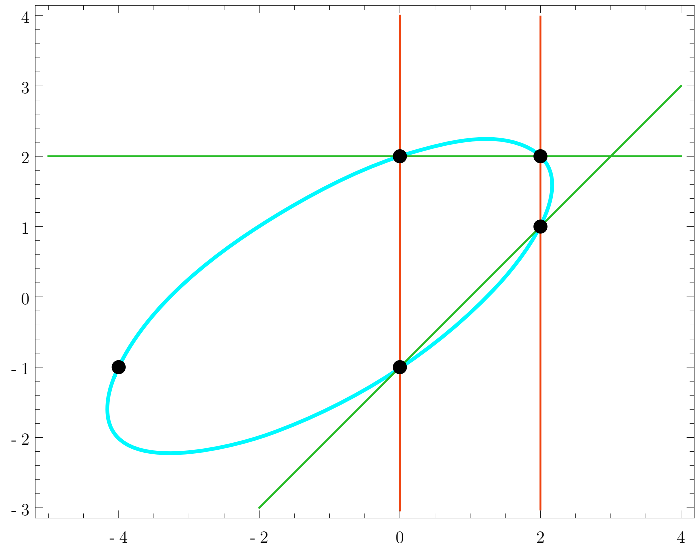


Figure 37 A conic through 5 points

Then the combined conics C_t with the equation $tx(x-2)+(x-y-1)(y-2)$ contain all four points $p_1, ...p_4$. In order that also p_5 lies on C_t, we need $0 = t(-4)(-4-2)+(-4+1-1)(-1-2) = 24t+12$ so that $t = -\frac{1}{2}$ and the equation for $C_{-1/2}$ simplifies to

$$x^2 + 2y^2 - 2xy + 2x - 2y - 4 = 0\ .$$

We could have done the computation also in homogeneous coordinates. The lines through p_1p_2 and p_3p_4 are given by the cross products

$$l_{12} = p_1 \times p_2 \sim \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad l_{34} = p_3 \times p_4 \sim \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$$

which gives the degenerate conic

$$A = l_{12} \cdot l_{34}^\top = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\ .$$

Likewise, the lines through p_1p_3 and p_2p_4 are given by the cross products

$$l_{13} = p_1 \times p_3 \sim \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \quad \text{and} \quad l_{24} = p_2 \times p_4 \sim \begin{pmatrix} 0 \\ 1 \\ -2 \end{pmatrix}$$

which gives the degenerate conic

$$B = l_{13} \cdot l_{24}^\top = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & -2 \\ 0 & -1 & 2 \\ 0 & -1 & 2 \end{pmatrix} .$$

Finally, testing whether the point p_5 lies on the combined conic given by $tA + B$ gives the equation

$$0 = p_5^\top (tA + B) p_5 = 24t + 12 \ ,$$

again solved by $t = -\frac{1}{2}$.

Exercise 4.6 Find a a conic in the projective plane $\mathbb{F}_5\mathbb{P}^2$ that contains the points $(1:1:2)$, $(1:1:3)$, $(1:3:0)$, $(1:4:2)$ and $(1:4:3)$. Find one more point on this conic.

Exercise 4.7 Find the two conics that pass through the four points $p_1 = (2:1:1)$, $p_2 = (2:-1:1)$, $p_3 = (-2:1:1)$, $p_4 = (-2:-1:1)$ and are tangent to the line $x + 2y + 5z = 0$. Then determine the point of tangency both cases.

Solution: We first determine lines $l_{i,j}$ through p_i and p_j as follows:

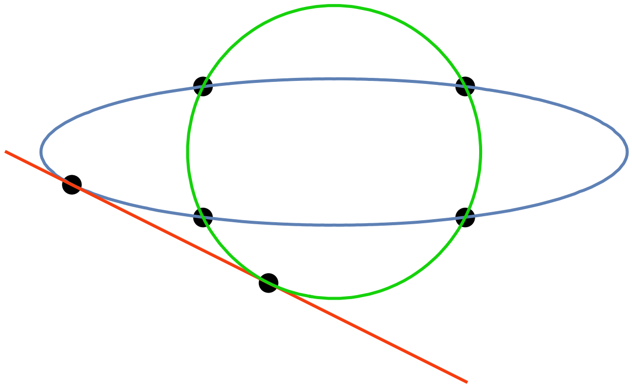


Figure 38 Conics through four points and tangent to line

$$p_1 \times p_2 = \begin{pmatrix} 2 \\ 0 \\ -4 \end{pmatrix} \Rightarrow l_{12} : x - 2z = 0$$

$$p_3 \times p_4 = \begin{pmatrix} 2 \\ 0 \\ 4 \end{pmatrix} \Rightarrow l_{34} : x + 2z = 0 \ .$$

$$p_1 \times p_3 = \begin{pmatrix} 0 \\ -4 \\ 4 \end{pmatrix} \Rightarrow l_{13} : y - z = 0$$

$$p_2 \times p_4 = \begin{pmatrix} 0 \\ -4 \\ -4 \end{pmatrix} \Rightarrow l_{24} : y + z = 0$$

The degenerate conic that consists of the two lines l_{12} and l_{34} is thus given by

$$C_0 = x^2 - 4z^2 = 0 \ ,$$

and the degenerate conic that consists of the two lines l_{13} and l_{24} by

$$C_1 = 4y^2 - 4z^2 = 0 \ .$$

Both degenerate conics contain p_1 through p_4, and hence so does $C_\lambda = (1 - \lambda)C_0 + \lambda C_1$ for any λ. We left the factor 4 in the conic C_1 so that C_λ becomes particularly simple. This combined conic is represented by the symmetric matrix

$$C_\lambda = \begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & 4\lambda & 0 \\ 0 & 0 & -4 \end{pmatrix}.$$

We are clearly lucky here that the matrix is diagonal and therefore easy to invert. Suppose that the line represented by $l = (1 : 2 : 5)$ is tangent to the conic at some point p. Then p must satisfy $p^\top C_\lambda p = 0$ (so that it lies on the conic) and $C_\lambda p = l$ (so that l is the tangent line to C_λ at p). We use the second equation to determine p as

$$p = C_\lambda^{-1} l = \begin{pmatrix} 1/(1-\lambda) \\ 1/(2\lambda) \\ -5/4 \end{pmatrix}.$$

Now we test whether this p lies on the conic C_λ:

$$
\begin{aligned}
p^\top C_\lambda p &= p^\top l \\
&= \frac{1}{1-\lambda} + \frac{1}{\lambda} - \frac{25}{4} \\
&= \frac{(5\lambda-1)(5\lambda-4)}{4\lambda(1-\lambda)} \ .
\end{aligned}
$$

Thus we find two solutions $\lambda_1 = \frac{1}{5}$ and $\lambda_2 = \frac{4}{5}$. The corresponding conics are

$$
C_{1/5} = x^2 + y^2 - 5z^2 = 0 \quad \text{and} \quad C_{4/5} = x^2 + 16y^2 - 20z^2 = 0 \ ,
$$

and p is given by

$$
p_{1/5} = (-1 : -2 : 1) \quad \text{and} \quad p_{4/5} = (-4 : -\frac{1}{2} : 1) \ .
$$