

MAS3210 Geometries and Designs

Semester 1, 2009/2010

Lecturer: Dr A Duncan

We are all familiar with shapes, patterns and pictures from our earliest consciousness. So, too, geometry, concerning particular spatial configurations which have pictorial elegance and beauty or practical significance, has its origins at the beginning of mathematical explorations. The serious study of geometry involves the systematic development of its basic concepts and subsequent formation of appropriate algebraic and analytic methods. This can occur in settings other than the ordinary Euclidean world; for example, in the projective plane which has a line at infinity or in planes where the co-ordinates belong to a finite field. Figures in the latter involve a finite number of points, lines and conics etc., which have combinatorial properties. These generalise to the ideas of designs, which figure in applications like the design of experiments. There is a wealth of possible material. The module will seek to convey an appreciation of some of this.

Books

1. Combinatorial Mathematics, H.J. Ryser (Math. Assoc. of America).
2. A Course in Combinatorics, J.H. Van Lint and R.M. Wilson (C.U.P).
3. **Library §512.5, §511.6**

Notes

The printed notes consist of lecture notes, intended to supplement the notes you make during the lectures, exercises and a mock exam with solutions. Material given on slides in the lectures is covered in the printed notes, what is written on the blackboard during lectures may not be. There should be enough space in the printed notes for you to write down the notes you take in lectures. The notes, exercises and other course information can be found on the web at

www.mas.ncl.ac.uk/~najd2/teaching/mas3210/
from where they can be viewed or printed out.

AJ Duncan August 2009

Contents

1	Combinatorial Designs	1
1.1	A Simpler Problem	2
1.2	2-Designs	3
1.3	Trivial Designs	8
1.4	Arithmetic of 2-designs	10
1.5	Applications	12
1.6	Steiner Systems	17
1.7	Projective Planes	26
1.8	Fisher's Inequality	26
1.9	Complementary designs	28
1.10	Symmetric Designs	32
1.11	Matrix Multiplication, J-Matrices and Determinants	36
1.12	Incidence Matrices	41
1.13	Symmetric Designs	54
2	Geometry Of The Projective Plane	64
2.1	The Euclidean Plane \mathbb{E}	64
2.2	The Line At Infinity	69
2.3	Lines in $\mathbb{P}_2(\mathbb{K})$	72
2.4	Duality	78
2.5	The Projective Planes $\mathbb{P}_2(\mathbb{K})$	81
2.6	The Triangle of Reference and the Unit Point	94
2.7	Desargues' Theorem	102
2.8	Pappus' Theorem	108
3	Conics	113
3.1	Introduction	113
3.2	Conics in $\mathbb{P}_2(\mathbb{K})$	114
3.3	Singular and Nonsingular Conics	115
3.4	A Canonical Form	128
3.5	Pascal's Theorem	134
3.6	5 points determine a conic	140
3.7	Non-singular Conics in $\mathbb{P}_2(p)$	142

1 Combinatorial Designs

Broadly speaking, a (combinatorial) design is a set together with a number of special subsets satisfying two conditions. The subject has its roots in Statistics, in the design and analysis of experiments.

- (1) **The Prussian Officers Problem (Euler, 1779)** In the Prussian army there are 6 different officer ranks. One officer of each rank is selected from each of 6 regiments, making 36 officers in all. Can you arrange the officers in a 6×6 square so that each row and each column contains just one officer of each rank and just one officer from each regiment?

Answer Euler conjectured that it could not be done, G. Tarry confirmed this in 1900.

- (2) **Kirkman's Schoolgirls Problem (Kirkman, 1850)**

A class of 15 schoolgirls are taken for a walk each day.

They walk in 5 rows, 3 abreast. Can it be arranged so

that, in the course of a 7 day week, each pair of girls

are in the same row on precisely one day?

Answer

Yes. See later.

These are **combinatorial problems**, concerned with a finite set of n objects which can be 'arranged' in a number (N say) of ways. Two sorts of questions arise.

- (A) Among the N arrangements, is there one which satisfies certain prescribed conditions?
- (B) If the answer to (A) is YES, how many of the N arrangements satisfy the conditions?

Of course it is in principle possible to resolve such questions by **exhaustion**, i.e., by examining each of the N arrangements in turn. In practice, however, such an approach is ruled out because N is impossibly large, even when n is quite small. This phenomenon is called the **combinatorial explosion**. For example, the number of ways of arranging a class of 30 students in order of merit is $30!$, roughly 2.65×10^{32} .

This is where mathematics comes in. It can be used to work out the implications of the 'prescribed conditions', and hence reduce the number of arrangements that we need to consider (in effect, to replace N by a smaller number). Having cut down the number of possibilities we may then use exhaustion to administer the coup de grace (as Tarry did with Euler's problem). But exhaustion is usually regarded as a last resort.

1.1 A Simpler Problem

Problem A swimming club wants to send a squad of 10 to a swimming gala consisting of $b \leq 20$ races. From this squad it has to enter a team of size k in each race, with different teams for different races. Also any two squad members are to swim together exactly twice. Is it possible to do this, and if so what are the possible values for b and k ?

We are dealing with a set X of size $v = 10$. We would have b special subsets of X of size k , chosen in such a way that each pair of elements of X belongs to precisely

2 of these subsets, where $2 \leq k \leq 10$. Thus we would have a number of special subsets (the teams) satisfying two conditions: the subsets have the same size; any pair of elements of X lie in the same number of special subsets.

Answer

Yes: $k = 4$, $b = 15$. (See later.)

1.2 2-Designs

Let us first fix some notation.

Notation 1.1. Suppose that $v, k \in \mathbb{N}$ with $v \geq k$. By a v -set we mean a set with v elements. Given a v -set X , a k -subset is a subset of X with k elements.

Remark 1.2. *Suppose that X is a v -set and that $k \leq v$. Then*

the number of k -subsets of X is

$$\binom{v}{k} = \frac{v!}{k!(v-k)!}$$

Definition 1.3. A $2 - (v, k, \lambda)$ design consists of

- a v -set X (of **points**)
- together with a non-empty set \mathcal{B} of k -subsets (**blocks**)
- such that each 2-subset of X lies in exactly λ of the blocks.

Remarks 1.4. (a) We refer to the design (X, \mathcal{B}) . The numbers v, k, λ are *parameters* of the design.

(b) In the original Statistics setting, an experiment would

be designed to give information about various ‘treatments’ applied to some situation: these might be medical treatments for a disease or fertilizers for a crop.

The number v refers to the number of varieties of treatment used (i.e., the number of treatments) in the experiment.

(c) By saying that \mathcal{B} is a *set* of k -subsets of X , we are

asserting that blocks are distinct. [In fact, in Statistical

experiments, it is sometimes the case that blocks are repeated, but we shall always take them as distinct.]

- (d) Each block has the same size k .
- (e) Usually \mathcal{B} does not contain all of the k -subsets.
- (f) We shall always assume that $2 \leq k \leq v$. If a $2 - (v, k, \lambda)$ design exists, then $\lambda \geq 1$ (for if we take a block B and take two distinct points $P, Q \in B$, then the 2-subset $\{P, Q\}$ lies in at least one block). [If we allowed $k = 1$, then we should always have a $2 - (v, k, \lambda)$ design with $\lambda = 0$.]
- (g) The fundamental question is: For given, v, k and λ , does a $2 - (v, k, \lambda)$ design exist? The answer is: sometimes but not always.
- (h) In the swimming club problem above, we are asking:

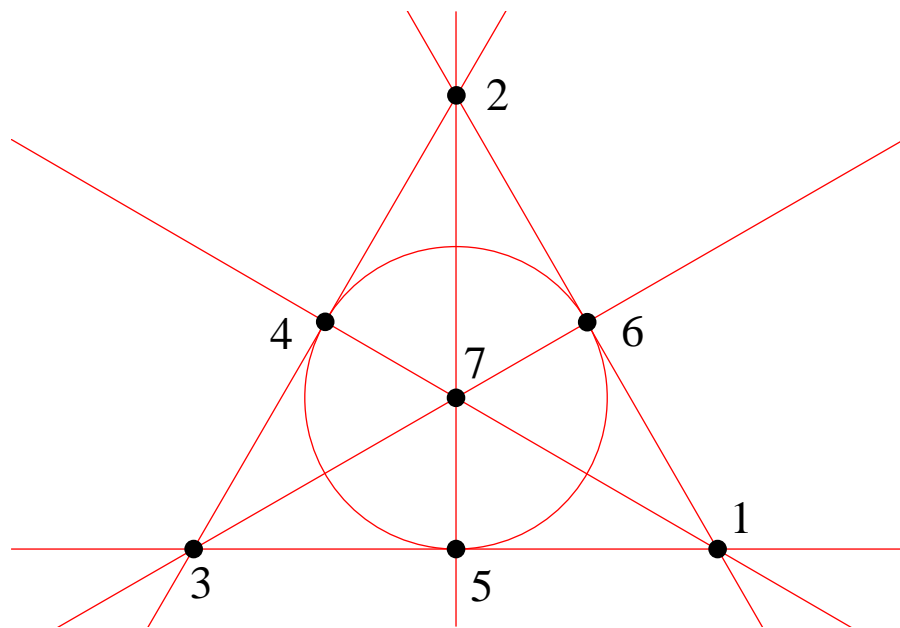
does there exist a $2 - (10, k, 2)$ design with $b \leq 20$?
- (i) In the Kirkman Schoolgirl problem, we are asking (in part): does a $2 - (15, 3, 1)$ design exist? However we are asking for additional conditions to be satisfied as

well.

Notation 1.5. We use b to denote the number of blocks: $b = |\mathcal{B}|$. (We do not build b into the definition: it turns out that it is determined by v , k and λ .)

Example 1.6. Here is an example of a $2 - (7, 3, 1)$ design (the **Fano Plane**).

The following diagram has seven points and seven 'lines'.



Here $X = \{1, 2, 3, 4, 5, 6, 7\}$ so $|X| = 7$. Each block is a set of three points on a line, where we count the circle 4, 5, 6 as a 'line'. Thus

$$\mathcal{B} = \{\{1, 6, 2\}, \{2, 4, 3\}, \{3, 5, 1\}, \{1, 7, 4\}, \{2, 7, 5\}, \{3, 7, 6\}, \{4, 5, 6\}\}.$$

We can use symmetry to help us check efficiently that any two points lie in exactly one block. The rotational symmetry of the triangle means that an argument applied to the point 1 applies equally well to the points 2 and 3, and an argument applied to the point 4 applies equally well to the points 5 and 6.

Suppose that P, Q are distinct points. One possibility is

that one of P, Q is one of 1, 2, 3. If we consider the pos-

sibility that one of P, Q is 1, then we have just six possibilities for P, Q and we can check the blocks containing them:

1, 2	1, 3	1, 4	1, 5	1, 6	1, 7
$\{1, 6, 2\}$	$\{3, 5, 1\}$	$\{1, 7, 4\}$	$\{3, 5, 1\}$	$\{1, 6, 2\}$	$\{1, 7, 4\}$

Here we see that $\{P, Q\}$ is contained in exactly one block.

By symmetry, the same argument applies if one of P, Q is 2 or 3. Now suppose that neither of P, Q is 1, 2 or 3.

Then one of them is a 4, 5 or 6. If we consider the possibility that one of P, Q is 4 but neither is 1, 2 or 3, then we have just three possibilities for P, Q and we can check the blocks containing them:

4, 5	4, 6	4, 7
$\{4, 5, 6\}$	$\{4, 5, 6\}$	$\{1, 7, 4\}$

Again we see that $\{P, Q\}$ is contained in exactly one

block. By symmetry, the same argument applies if one of P, Q is 5 or 6.

Observe that

- Precisely 3 lines pass through each point.
- 2 distinct lines have just one point in common.

1.3 Trivial Designs

Theorem 1.7. *Let X be any v -set with $v \geq 2$, let $2 \leq k \leq v$ and let \mathcal{B} be the set of all k -subsets of X . Then (X, \mathcal{B}) is a $2 - (v, k, \lambda)$ design with $\lambda = \binom{v-2}{k-2}$.*

Proof. Let $\{P, Q\}$ be any 2-subset of X . The number of k -subsets of X which include $\{P, Q\}$ is equal to the number of ways of choosing $k - 2$ elements from the remaining $v - 2$, i.e., $\binom{v-2}{k-2}$. Since \mathcal{B} consists of all k -subsets of X , each 2-subset lies in $\binom{v-2}{k-2}$ blocks. Hence (X, \mathcal{B}) is a $2 - (v, k, \lambda)$ design with $\lambda = \binom{v-2}{k-2}$.

□

Definition 1.8. A $2 - (v, k, \lambda)$ design is **trivial** if \mathcal{B} is the set of all k -subsets of X .

Theorem 1.9. If $k = 2$ then the only $2 - (v, k, \lambda)$ design is the trivial one and $\lambda = 1$.

Proof. If $k = 2$ then the blocks are 2-subsets of X . Each 2-subset of X must be included in λ blocks, where $\lambda \geq 1$, i.e., so each 2-subset must be a block. Thus the design is trivial and each 2-subset is contained in one block so $\lambda = 1$ (alternatively $\lambda = \binom{v-2}{0} = 1$).

□

Theorem 1.10. If $k = v$ then the only $2 - (v, k, \lambda)$ design is the trivial one and $\lambda = 1$.

Proof. If $k = v$ then the blocks have size v , so there is just one block, namely X itself. Thus every k -subset is a blocks and so the design is trivial. There is only one block so we must have $\lambda = 1$ (alternatively $\lambda = \binom{v-2}{v-2} = 1$).

□

Corollary 1.11. *In a non-trivial $2 - (v, k, \lambda)$ design $2 < k < v$.*

Proof. Follows immediately from the preceding theorems. □

1.4 Arithmetic of 2-designs

Theorem 1.12. *In a $2 - (v, k, \lambda)$ design, the number of blocks is given by $b = \frac{\lambda v(v-1)}{k(k-1)}$.*

Proof. We count the number of ordered triples (P, Q, B) ,

where P, Q are distinct members of X , $B \in \mathcal{B}$ and $P, Q \in B$.

We do this in two different ways and then compare.

(1) Choose B first: there are b choices for B . For each

choice of B there are k choices for P and then $k - 1$

choices for Q , making $bk(k - 1)$ triples (P, Q, B) .

(2) Choose P and Q first: there are v choices for P and

then $v - 1$ choices for Q . For each choice of P and

Q there are λ choices for B containing P, Q , making

$\lambda v(v - 1)$ triples (P, Q, B) .

The number of triples does not depend on the way we count. Therefore $bk(k - 1) = \lambda v(v - 1)$, i.e., $b = \lambda \frac{v(v - 1)}{k(k - 1)}$. □

Remark 1.13. This explains why b was not specified in the definition of a $2 - (v, k, \lambda)$ design: it is completely determined by v, k and λ .

Theorem 1.14. In a $2 - (v, k, \lambda)$ design, each point lies in the same number of blocks, namely,

$$r = \lambda \frac{(v - 1)}{(k - 1)}.$$

Proof. Let P be any point of X and regard P as fixed. Let r be the number of blocks containing P . We count the number of pairs (Q, B) , where $Q \in X \setminus \{P\}$, $B \in \mathcal{B}$ and $P, Q \in B$. We do this in two different ways and then compare.

- (1) Choose B first: there are r blocks containing P so we can do this in r ways. For each choice of B there are $k - 1$ choices for Q , making $r(k - 1)$ pairs (Q, B) .
- (2) Choose Q first: there are $v - 1$ points of X different from P so we can do this in $v - 1$ ways. For each choice of Q there are λ choices for B containing P, Q , making $\lambda(v - 1)$ pairs (Q, B) .

The number of pairs does not depend on the way we count. Therefore $r(k - 1) = \lambda(v - 1)$, i.e., $r = \lambda \frac{(v - 1)}{(k - 1)}$. This expression does not depend on the choice of P , so r is the same for every point of X . □

Corollary 1.15. In a $2 - (v, k, \lambda)$ design with $v > k$, it must be the case that $r > \lambda$.

Proof. This follows immediately from Theorem 1.14, given that $\frac{(v - 1)}{(k - 1)} > 1$. □

Theorem 1.16. In a $2 - (v, k, \lambda)$ design, $bk = vr$.

Proof. This follows immediately from Theorems 1.12 and 1.14. □

1.5 Applications

Example 1.17. Show that there is no $2 - (13, 5, 2)$ design.

Solution

Suppose that such a design exists. Then $v = 13, k = 5, \lambda = 2$, so

$$r = \lambda \cdot \frac{(v-1)}{(k-1)} = \frac{2 \times 12}{4} = 6.$$

Also

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{2 \times 13 \times 12}{5 \times 4} = \frac{78}{5} \notin \mathbb{Z}.$$

Contradiction, since b must be a whole number. Therefore supposition wrong: no such design exists.

Example 1.18. Show that there is no $2 - (12, 4, 2)$ design.

Solution

Suppose that such a design exists. Then $v = 12, k =$

4, $\lambda = 2$, so

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{2 \times 12 \times 11}{4 \times 3} = 22$$

but

$$r = \lambda \cdot \frac{(v-1)}{(k-1)} = \frac{2 \times 11}{3} \notin \mathbb{Z}.$$

Contradiction, since r must be a whole number. Therefore supposition wrong: no such design exists.

Example 1.19. Show that there are at most two values of k for which a non-trivial $2 - (31, k, 1)$ design exists.

Solution

Suppose that non-trivial a $2 - (31, k, 1)$ design exists.

Then $v = 31$, $\lambda = 1$ and $2 < k < 31$, so

$$r = \lambda \cdot \frac{(v-1)}{(k-1)} = \frac{1 \times 30}{k-1} = \frac{30}{k-1}.$$

Therefore $k - 1$ divides 30 and $k \geq 3$. Also

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{31 \times 30}{k(k-1)}.$$

But $k < 31$ so k and $k - 1$ are relatively prime to 31 and therefore $k(k - 1)$ divides 30. Since $(k - 1)^2 < k(k - 1) \leq 30$, we need only consider values of k with $3 \leq k \leq 6$: only $k = 3$ and $k = 6$ are possible. If $k = 3$, then $b = 155$ and $r = 1 \times \frac{31 - 1}{3 - 1} = 15$. If $k = 6$, then $b = 31$ and $r = 1 \times \frac{31 - 1}{6 - 1} = 6$. [We have not shown that $2 - (31, 3, 1)$ and $2 - (31, 6, 1)$ designs actually exist. In fact we shall see examples of both in due course.]

Example 1.20. Show that if a $2 - (v, 3, 1)$ design exists then v must be of the form $6n + 1$ or $6n + 3$.

Solution

Here $k = 3$, $\lambda = 1$, so

$$r = \lambda \cdot \frac{(v - 1)}{(k - 1)} = \frac{v - 1}{2},$$

so v is odd and hence of the form $6n + 1$, $6n + 3$ or $6n + 5$.

Also

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{v(v-1)}{6}.$$

If v were of the form $6n + 5$ then b would be of the form

$$\frac{(6n+5)(6n+4)}{6} = \frac{36n^2 + 54n + 20}{6} = 6n^2 + 9n + \frac{20}{6},$$

which is not a whole number. Therefore v must be of the form $6n + 1$ or $6n + 3$.

Example 1.21. Suppose that a schoolteacher is able to give each child in her class 3 differently coloured crayons, drawn from a box containing crayons of 6 different colours. No 2 children receives the same 3 colours. In fact, each pair of colours are given two exactly 2 children. How many children are in the class? How many crayons of each colour are used?

Solution

Let X be the set of colours, so $|X| = 6$. Each child receives a 3-subset of X and different children have different selections of colours. Let \mathcal{B} be the set of 3-subsets used (the blocks). Each 2-subset occurs in precisely 2

blocks. Thus we have a $2 - (6, 3, 2)$ design, i.e., $v = 6, k = 3, \lambda = 2$.

We are asked for b (= the number of blocks = the number of children) and r (= the number of times each colour is used). By Theorems 1.12 and 1.14,

$$b = \lambda \frac{v(v-1)}{k(k-1)} = \frac{2 \times 6 \times 5}{3 \times 2} = 10$$

$$r = \lambda \cdot \frac{(v-1)}{(k-1)} = 2 \cdot \frac{5}{2} = 5.$$

Thus there are 10 children and each colour is used 5 times, so 5 crayons of each colour are used. [Once again, we have not actually shown that such a design exists, merely explored its properties on the assumption that it does exist. But see later.]

Exercise 1.22. Show that if $k = v - 1$, then the only $2 - (v, k, \lambda)$ design is the trivial one. [Hint: use the expression for r to get a lower bound for λ and use this to show that $b \geq v$; explain why in the case of a $2 - (v, v - 1, \lambda)$ design it must happen that $b \leq v$.]

1.6 Steiner Systems

Definition 1.23. A $2 - (v, k, 1)$ design is known as a **Steiner System of order v** . In particular if $k = 3$, then it is called a Steiner Triple System (STS).

Remarks 1.24. (a) **By Example 1.20, the only possibilities for**

**Steiner Triple Systems of order v are when $v \equiv 1$ or 3
(mod 6).**

(b) **The trivial $2 - (3, 3, 1)$ design is an STS of order 3**

(c.f., Theorems 1.7 and 1.10).

(c) **The Fano Plane (Example 1.6) is a $2 - (7, 3, 1)$ design,**

i.e., an STS of order 7.

(d) **A solution to the Kirkman Schoolgirl Problem would**

be a $2 - (15, 3, 1)$ design, i.e., an STS of order 15.

Definition 1.25 (Binary Projective Spaces). Given any $n \geq 2$, let V_{n+1} be the set of all vectors of length $n + 1$ with each entry either 0 or 1. Then we can add

vectors in V_{n+1} by performing operations $(\text{mod } 2)$. The zero vector is just the vector $(0, 0, \dots, 0)$. If u, v are distinct non-zero vectors, consider the set of vectors $\{u, v, u+v\}$: we observe that $u+(u+v) = 2u+v = v, v+(u+v) = 2v+u = u$, so the sum of any two elements is the third; moreover $u, v, u+v$ are distinct with $u+v$ non-zero (for if $u+v = 0$, then $u = v$; if $u = u+v$, then $v = 0$; if $v = u+v$, then $u = 0$).

Let X be the set of all non-zero vectors in V_{n+1} and let \mathcal{B} be the set of all 3-subsets of X of the form $u, v, u+v$ where $u \neq v$. We call (X, \mathcal{B}) the **binary projective space of dimension n** .

Theorem 1.26. *The binary projective space of dimension n is an STS of order $2^{n+1} - 1$.*

Proof. To begin with, V_{n+1} has 2^{n+1} vectors so X is a $(2^{n+1} -$

$1)$ -set. We are given a non-empty set \mathcal{B} of 3-sets (blocks).

Let x, y be distinct elements of X . Then x, y lie in the

block $\{x, y, x+y\}$. Furthermore in any block in \mathcal{B} the

sum of any two elements is the third, so a block contain-

ing x, y must contain $x+y$ and hence this block must

be $\{x, y, x+y\}$. Hence (X, \mathcal{B}) is a $2 - (2^{n+1} - 1, 3, 1)$

design, i.e., an STS of order $2^{n+1} - 1$.

□

Remark 1.27. As a consequence of Theorem 1.26, we know that there are infinitely many STSs (at least one of order $2^{n+1} - 1$ for each $n \geq 2$) and therefore infinitely many designs.

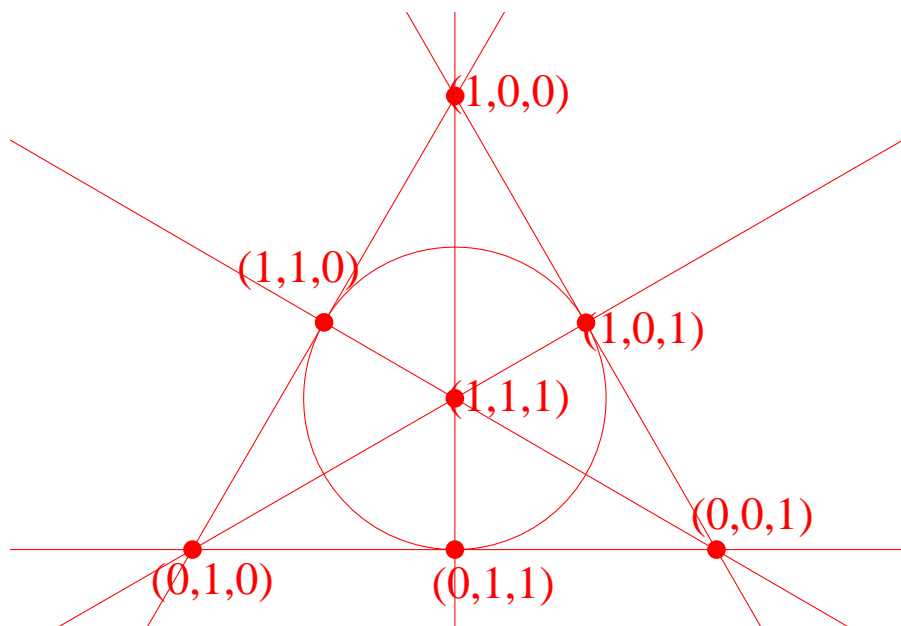
Examples 1.28. (a) When $n = 2$, we have an STS of order 7, i.e., a $2 - (7, 3, 1)$ design. X consists of the vectors:

$$(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 0), (0, 1, 1), (1, 0, 1), (1, 1, 1).$$

The blocks then are:

$$\begin{aligned} &\{(1, 0, 0), (0, 1, 0), (1, 1, 0)\}, \{(1, 0, 0), (0, 0, 1), (1, 0, 1)\}, \\ &\{(0, 1, 0), (0, 0, 1), (0, 1, 1)\}, \{(1, 0, 0), (0, 1, 1), (1, 1, 1)\}, \\ &\{(0, 1, 0), (1, 0, 1), (1, 1, 1)\}, \{(0, 0, 1), (1, 1, 0), (1, 1, 1)\}, \\ &\{(1, 1, 0), (0, 1, 1), (1, 0, 1)\}. \end{aligned}$$

We can label the Fano Plane as follows:



Thus the Fano Plane is simply the smallest binary projective space (and it is a plane because it has dimension 2).

(b) When $n = 3$ we get an STS of order 15. This is a candidate for a solution to the Kirkman Schoolgirl Problem.

(c) When $n = 4$ we get an STS of order 31, i.e., a $2 - (31, 3, 1)$ design (see Example 1.19).

Theorem 1.29. *If there exist Steiner Triple Systems of orders v_1 and v_2 , then there exists a Steiner Triple System of order v_1v_2 .*

Proof. Suppose that (X, \mathcal{B}) and (Y, \mathcal{C}) be STSs of orders v_1 and v_2 respectively. We list the elements of X as $1, 2, \dots, v_1$ and the elements of Y as $1, 2, \dots, v_2$. Then Z is defined to be $\{(i, j) : 1 \leq i \leq v_1, 1 \leq j \leq v_2\}$, so Z has v_1v_2 elements.

We define a number of blocks of Z as follows:

(a) For each block $\{p, q, r\}$ in \mathcal{B} and for each $1 \leq j \leq v_2$,

there is a 3-subset $\{(p, j), (q, j), (r, j)\}$ of Z .

(b) For each block $\{s, t, u\}$ in \mathcal{C} and for each $1 \leq i \leq v_1$,

there is a 3-subset $\{(i, s), (i, t), (i, u)\}$ of Z .

(c) For each block $\{p, q, r\}$ in \mathcal{B} and for each block $\{s, t, u\}$

in \mathcal{C} , there are six 3-subsets of Z (one for each ordering of s, t, u): $\{(p, s), (q, t), (r, u)\}$, $\{(p, s), (q, u), (r, t)\}$, $\{(p, t), (q, s), (r, u)\}$, $\{(p, u), (q, t), (r, s)\}$, $\{(p, t), (q, u), (r, s)\}$, $\{(p, u), (q, s), (r, t)\}$.

Look at the example that follows and return to the proof.

Observe that the blocks we have defined are distinct, so they form a set \mathcal{D} of 3-subsets. Now suppose that we have two (different) points of Z : (p, s) and (q, t) . Then there are three possibilities:

- $s = t$: we must have $p \neq q$, so p, q are distinct and lie in a unique block $\{p, q, r\}$ in \mathcal{B} . There is exactly one block of the first type containing (p, s) and

(q, s) , namely $\{(p, s), (q, s), (r, s)\}$ and no blocks of the second or third types.

- $p = q$: we must have $s \neq t$, so s, t are distinct and lie in a unique block $\{s, t, u\}$ in \mathcal{C} . There is exactly one block of the second type containing (p, s) and (p, t) , namely $\{(p, s), (p, t), (p, u)\}$ and no blocks of the first or third types.
- $p \neq q$ and $s \neq t$: there are no blocks of the first or second types containing (p, s) and (q, t) . A block of the third type would have to be $\{(p, s), (q, t), (r, u)\}$ for some r and u . Now p, q lie in a unique block $\{p, q, r\}$ in \mathcal{B} , and s, t lie in a unique block $\{s, t, u\}$ in \mathcal{C} . Thus there are unique choices for r and u so

that $\{(p, s), (q, t), (r, u)\}$ is a block in \mathcal{D} .

We have a v_1v_2 -set Z and a non-empty set \mathcal{D} of 3-subspaces of Z . We have shown that any pair of points of Z lies in exactly one block in \mathcal{D} . Hence (Z, \mathcal{D}) is a $2 - (v_1v_2, 3, 1)$ design, i.e., an STS of order v_1v_2 .

□

Example 1.30. Construct an STS of order 9.

Solution. We observe that $9 = 3 \times 3$ and that there is an STS of order 3, namely the trivial $2 - (3, 3, 1)$ design. We may take (X, \mathcal{B}) and (Y, \mathcal{C}) as the same design, with points labelled 1, 2, 3 and each with one block, namely $\{1, 2, 3\}$. The set Z is given by

$$\{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}.$$

We construct blocks as indicated above:

- (a) We have only one block in \mathcal{B} , namely $\{1, 2, 3\}$. For $j = 1, 2, 3$ in turn, we get 3-subsets: $\{(1, 1), (2, 1), (3, 1)\}$, $\{(1, 2), (2, 2), (3, 2)\}$, $\{(1, 3), (2, 3), (3, 3)\}$.
- (b) We have only one block in \mathcal{C} , namely $\{1, 2, 3\}$. For $i = 1, 2, 3$ in turn, we get 3-subsets: $\{(1, 1), (1, 2), (1, 3)\}$, $\{(2, 1), (2, 2), (2, 3)\}$, $\{(3, 1), (3, 2), (3, 3)\}$.
- (c) We have only one block, $\{1, 2, 3\}$, in \mathcal{B} and one block, $\{1, 2, 3\}$, in \mathcal{C} . There are six subsets of Z (one for each ordering of 1, 2, 3): $\{(1, 1), (2, 2), (3, 3)\}$, $\{(1, 1), (2, 3), (3, 2)\}$, $\{(1, 2), (2, 1), (3, 3)\}$, $\{(1, 3), (2, 2), (3, 1)\}$, $\{(1, 2), (2, 3), (3, 1)\}$, $\{(1, 3), (2, 1), (3, 2)\}$.

We can see these points in a diagram:

Examples 1.31. For each of the following values of v , determine whether or not there is an STS of order v :

(a) $v = 127$

Solution.

Yes, because $127 = 2^7 - 1$ and there is always an STS with such an order (Binary Projective Space of dimension 6).

(b) $v = 21$

Solution.

Yes, because $21 = 3 \times 7$. There is an STS of order 3

(trivial STS) and an STS of order 7 (Fano Plane), and hence one of order 3×7 .

(c) $v = 35$

Solution.

No, because $35 \equiv 5 \pmod{6}$ (and an STS has order $\equiv 1$ or $3 \pmod{6}$).

(d) $v = 105$

Solution.

Yes, because $105 = 7 \times 15$. There is an STS of order 7 (Fano Plane) and an STS of order 15 (BPS of dimension 3), and hence one of order 7×15 . [Note that using $105 = 5 \times 21$ does not work because there is not an STS of order 5. Similarly using $105 = 3 \times 35$ does not work because there is not an STS of order 35.]

(e) $v = 343$

Solution.

Yes. Observe that $343 = 7^3$. There is an STS of order 7 (Fano Plane), and hence one of order $7 \times 7 = 49$, and therefore one of order $7 \times 49 = 343$.

1.7 Projective Planes

Definition 1.32. A (finite) **projective plane of order n** is a $2 - (n^2 + n + 1, n + 1, 1)$ design.

Remark 1.33. We shall see more of projective planes in a geometric context later in the course. For now it suffices to note:

- There is a projective plane of order q for every prime power q . In fact, for many prime powers q , two or more different examples are known.
- Later we shall see particular examples of projective planes of order p , where p is prime.
- There are no known projective planes having an order that is not a prime power, but it has not yet been proved that no such planes exist.
- The Fano Plane is a projective plane of order 2.
- A projective plane of order 5 is a $2 - (31, 6, 1)$ design (see Example 1.19).

1.8 Fisher's Inequality

Theorem 1.34. Given a $2 - (v, k, \lambda)$ design with $v > k$, the number of blocks b is $\geq v$.

Proof. Later. □

Examples 1.35. (a) Recall the swimming club problem in Section 1.2.

Problem A swimming club sends a squad of 10 to a swimming gala consisting

of $b \leq 20$ races. From this squad it has to enter a team of size k in each race, with different teams for different races. Also any two squad members are to swim together exactly twice. Find b and k so that this is possible.

This calls for a $2 - (10, k, 2)$ design with $b \leq 20$. The

formula $b = \lambda \frac{v(v-1)}{k(k-1)}$ gives

$$b = \frac{2 \times 10 \times 9}{k(k-1)} = \frac{180}{k(k-1)}.$$

But $b \leq 20$ (given) so

$$\frac{180}{k(k-1)} \leq 20, \text{ i.e., } k(k-1) \geq 9.$$

It follows that $k \geq 4$. Also, by Fisher's inequality,

$b \geq v$, i.e., $b \geq 10$, so

$$\frac{180}{k(k-1)} \geq 10 \text{ i.e., } k(k-1) \leq 18.$$

It follows that $k \leq 4$. Hence $k = 4$ and $b = \frac{180}{k(k-1)} = \frac{180}{4 \times 3} = 15$.

Thus, if a solution is possible then we must have $k =$

$4, b = 15$ (but we still don't yet know whether a solu-

tion is possible).

(b) Show that there is no $2 - (136, 51, 10)$ design.

Solution.

We start by checking the arithmetical conditions:

$$r = \lambda \frac{v-1}{k-1} = 10 \times \frac{135}{50} = 27, \quad b = \lambda \frac{v(v-1)}{k(k-1)} = 10 \times \frac{136 \times 135}{51 \times 50} =$$

These are both whole numbers, so we cannot rule out the possibility of a design on these grounds. However we certainly have $v > k$, so Fisher's Inequality should apply, but here $b < v$. Hence no design with these parameters can exist.

1.9 Complementary designs

Theorem 1.36. Let (X, \mathcal{B}) be a $2 - (v, k, \lambda)$ design and let $\bar{\mathcal{B}}$ consist of the complements in X of the blocks in \mathcal{B} , i.e.,

$$\bar{\mathcal{B}} = \{\bar{B} = X \setminus B : B \in \mathcal{B}\}.$$

- (a) If P and Q are distinct points of X then the number of blocks of \mathcal{B} containing one or both of P and Q is $2r - \lambda$. The number of blocks of \mathcal{B} containing neither P nor Q is $b - 2r + \lambda$.
- (b) $(X, \bar{\mathcal{B}})$ is a $2 - (v, v - k, b - 2r + \lambda)$ design.

Proof.

- (a) There are r blocks that contain P and r that contain Q . There are λ blocks that contain both P and Q . Hence there are $r - \lambda$ blocks that contain P but not Q , $r - \lambda$ blocks that contain Q but not P , and λ blocks that contain both P and Q . A block containing one or both of P, Q lies in exactly one of these three subsets. Hence the number of blocks containing one or both of P and Q is

$$(r - \lambda) + (r - \lambda) + \lambda = 2r - \lambda.$$

There are b blocks altogether in \mathcal{B} , so there are $b -$

$(2r - \lambda) = b - 2r + \lambda$ blocks that contain neither P nor Q .

(b) We have a set X with v points and each set in $\bar{\mathcal{B}}$ contains $v - k$ points. The sets in $\bar{\mathcal{B}}$ are distinct because if $B_1 \neq B_2$, then $\bar{B}_1 \neq \bar{B}_2$.

Suppose $B \in \mathcal{B}$. Then the condition: neither P nor Q lies in B is equivalent to the condition: $P, Q \in \bar{B} = X \setminus B$. Hence the number of blocks $\bar{B} \in \bar{\mathcal{B}}$ containing P and Q is equal to the number of blocks $B \in \mathcal{B}$ that contain neither P nor Q , i.e., is $b - 2r + \lambda$. Thus any two points in X lie in $b - 2r + \lambda$ blocks in $\bar{\mathcal{B}}$.

We have now shown that $(X, \bar{\mathcal{B}})$ is a $2 - (v, v - k, b -$

$2r + \lambda$) design.

□

Definition 1.37. The design $(X, \bar{\mathcal{B}})$ is called the *complementary design* to (X, \mathcal{B}) .

Remarks 1.38. (a) If $B \in \mathcal{B}$, then $\bar{B} = X \setminus B$. Thus the complementary design to (X, \mathcal{B}) has X as its set of points and $\bar{\mathcal{B}}$ as its set of blocks, i.e., is $(X, \bar{\mathcal{B}})$.

(b) If there exists a $2 - (v, k, \lambda)$ design, then there exists a $2 - (v, v - k, b - 2r + \lambda)$ design. Conversely, suppose we want to know if there exists a $2 - (v, k, \lambda)$ design and we calculate the numbers $k' = v - k$ and $\lambda' = b - 2r + \lambda$. If there is a $2 - (v, k', \lambda')$ design (with b' blocks and each point in r' blocks), then its complement will be a $2 - (v, v - k', b' - 2r' + \lambda')$ design. We can calculate (EXERCISE!):

$$\lambda' = \frac{\lambda(v - k)(v - k - 1)}{k(k - 1)}, \quad b' = b, \quad r' = \frac{\lambda(v - k)(v - 1)}{k(k - 1)}$$

$$v - k' = k, \quad b' - 2r' + \lambda' = \lambda.$$

Thus if a $2 - (v, k', \lambda')$ design exists, so does a $2 - (v, k, \lambda)$ design.

Example 1.39. Determine whether or not there exists a $2 - (7, 4, 2)$ design.

Solution.

$$b = \frac{2 \times 7 \times 6}{4 \times 3} = 7, \quad r = \frac{2 \times 6}{3} = 4$$

so $v - k = 3$ and $b - 2r + \lambda = 7 - 8 + 2 = 1$. Does there

exist a $2 - (7, 3, 1)$ design? Answer YES (Fano PLane),

so there exists a $2 - (7, 4, 2)$ design.

1.10 Symmetric Designs

Definition 1.40. A $2 - (v, k, \lambda)$ design is called **symmetric** if $b = v$. [We should really call this a 'square' design, but the term 'symmetric' is too well established to change.]

Remark 1.41. If $v = k$, then there is only one block (i.e., $b = 1$). Therefore, in assuming $v \geq 2$ for all designs, we have $v > k$ for all symmetric designs.

Theorem 1.42. In a symmetric design

(a) $k = r$;

(b) $\lambda = \frac{k(k-1)}{v-1}$ and $v = \frac{k(k-1)}{\lambda} + 1$, so $\lambda \mid k(k-1)$.

Proof.

(a) By Theorem 1.16, $bk = vr$. In a symmetric design,

$$b = v, \text{ so } k = r.$$

(b) From Theorem 1.14, $r = \lambda \frac{(v-1)}{(k-1)}$. Rearranging,

we get first $\lambda = \frac{r(k-1)}{(v-1)}$. Applying (a) we get

$\lambda = \frac{k(k-1)}{(v-1)}$. Further rearrangement gives $v-1 =$

$\frac{k(k-1)}{\lambda}$, from which it follows that $\lambda \mid k(k-1)$ and

also $v = \frac{k(k-1)}{\lambda} + 1$.

□

Example 1.43. Show that a symmetric $2 - (v, 8, 1)$ design is a projective plane.

Solution.

Assuming that there exists a symmetric $2 - (v, 8, 1)$ design, Theorem 1.42(b) above implies that

$$v = \frac{k(k-1)}{\lambda} + 1 = \frac{8 \times 7}{1} + 1 = 57.$$

Since $57 = 7^2 + 7 + 1$ and $8 = 7 + 1$, a $2 - (57, 8, 1)$ design would be a projective plane of order 7.

Theorem 1.44. *If there exists a symmetric $2 - (v, k, \lambda)$ design with v even, then $k - \lambda$ must be a perfect square.*

Proof. Later. □

Example 1.45. Show that there is no $2 - (22, 7, 2)$ design.

Solution.

Suppose that such a design exists. Then $b = 2 \frac{22 \times 21}{7 \times 6} =$

22 so the design would be symmetric. Given that $v = 22$

is an even number, if a $2 - (22, 7, 2)$ design existed, then

$k - \lambda = 7 - 2 = 5$ would be a perfect square. But 5 is

not a perfect square, so no such design exists.

There is a corresponding result for v odd, which we now state without proof.

Theorem 1.46. *If there exists a symmetric $2 - (v, k, \lambda)$ design with v odd, then the equation*

$$x^2 = (k - \lambda)y^2 + (-1)^{(v-1)/2} \lambda z^2$$

has a solution in integers x, y, z not all 0.

Proof. Not given. □

Theorem 1.47. *A (finite) projective plane is a symmetric design with an odd number of points.*

Proof. Recall that a projective plane is a $2 - (n^2 + n + 1, n + 1, 1)$ design. The number of blocks is given by

$$b = \lambda \frac{v(v-1)}{k(k-1)} = 1 \times \frac{(n^2 + n + 1)(n^2 + n)}{(n+1)n} = n^2 + n + 1$$

so the design is symmetric. Note that $n^2 + n = n(n+1)$ is always even, so $v = n^2 + n + 1$ is always odd. □

Example 1.48. There is no projective plane of order 14. [Recall that a projective plane of order 14 would be a (symmetric) $2 - (211, 15, 1)$ design.]

Solution.

By Theorem 1.46, if there exists a $2 - (211, 15, 1)$ design,

then the equation

$$x^2 = (15 - 1)y^2 + (-1)^{(211-1)/2} \times 1 \times z^2$$

has a solution in integers x, y, z not all 0. The equation simplifies to $x^2 = 14y^2 - z^2$. Assuming that there is a solution with x, y, z not all 0, x cannot be 0 (because if $x = 0$, then we would have a solution in integers y, z , not both 0, to the equation $z^2 = 14y^2$, which is impossible since $\sqrt{14}$ is irrational), so we can select a solution: $x = x_0, y = y_0, z = z_0$ not all 0, for which $|x|$ has its smallest possible value. Then $x_0^2 + z_0^2 = 14y_0^2 \equiv 0 \pmod{7}$. If we consider the squares $\pmod{7}$:

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 2, 4^2 = 2, 5^2 = 4, 6^2 = 1$$

we see that the only way in which $x_0^2 + z_0^2$ can be 0 $\pmod{7}$ is if $7 \mid x_0$ and $7 \mid z_0$. Then $7^2 \mid x_0^2 + z_0^2 = 14y_0^2$ so $7 \mid 2y_0^2$ and (given that 7 is prime) $7 \mid y_0$. Now $(x_0/7)^2 +$

$(z_0/7)^2 = 14(y_0/7)^2$, so $x = x_0/7, y = y_0/7, z = z_0/7$ is also a solution in integers, not all 0. But $|x_0/7| < |x_0|$ which is a contradiction to the choice of x_0 with $|x_0|$ as small as possible. This contradiction tells us that there can be no $2 - (211, 15, 1)$ design.

1.11 Matrix Multiplication, J-Matrices and Determinants

We begin this section with a reminder about matrix multiplication. As we shall discover, it is often useful to have general arguments regarding matrix multiplication, and for that it is useful to have a general description.

Definition 1.49. Suppose that $A = [a_{ij}]$ is an $m \times n$ matrix and that $B = [b_{ij}]$ is an $n \times p$ matrix. Then the product $C = AB$ is an $m \times p$ matrix, $C = [c_{ij}]$, with

$$c_{ij} = \sum_{k=1}^n a_{ik}b_{kj}.$$

All this means is that c_{ij} is the result of multiplying the i 'th row of A by the j 'th column of B :

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & \cdots & b_{2p} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1} & b_{n2} & \cdots & b_{np} \end{bmatrix}$$

so

$$c_{ij} = [a_{i1} \ a_{i2} \ a_{i3} \ \cdots \ a_{in}] \begin{bmatrix} b_{1j} \\ b_{2j} \\ b_{3j} \\ \vdots \\ b_{nj} \end{bmatrix} = \sum_{k=1}^n a_{ik}b_{kj}.$$

Example 1.50. Let $A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$. Find $A^T A$. [Recall that A^T (the transpose of A) is obtained from A by switching rows and columns (1st row becomes 1st column and vice-versa).]

Solution.

$$A^T A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} =$$

$$= \begin{bmatrix} 3 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 3 \end{bmatrix}.$$

We shall have occasion to study matrices for which the entries in each row add up to the same sum. We can use J-matrices to express this property as a matrix equation.

Definition 1.51. For each $n, p \geq 1$, we let J_{np} denote the $n \times p$ matrix all of whose entries are equal to 1.

Example 1.52.

$$J_{23} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Theorem 1.53. Let A be an $m \times n$ matrix. Then the following statements are equivalent.

- (1) The entries in each row of A add up to r .
- (2) $AJ_{np} = rJ_{mp}$ for some $p \geq 1$.
- (3) $AJ_{np} = rJ_{mp}$ for every $p \geq 1$.

Proof. Let the row-sums of A be denoted by r_1, r_2, \dots, r_m . [That is, if $A = (a_{ij})$, then $r_i = a_{i1} + a_{i2} + \dots + a_{in}$, the sum of the entries in row i of A .] Then

$$AJ_{np} = \begin{bmatrix} r_1 & r_1 & \dots & r_1 \\ r_2 & r_2 & \dots & r_2 \\ \dots & \dots & \dots & \dots \\ r_m & r_m & \dots & r_m \end{bmatrix}_{m \times p} .$$

Also

$$rJ_{mp} = \begin{bmatrix} r & r & \dots & r \\ r & r & \dots & r \\ \dots & \dots & \dots & \dots \\ r & r & \dots & r \end{bmatrix}_{m \times p} .$$

Each of the statements is equivalent to saying that $r = r_1 = r_2 = \dots = r_m$. \square

Theorem 1.53 has a counterpart for columns:

Theorem 1.54. *Let A be an $m \times n$ matrix. Then the following statements are equivalent.*

- (1) *The entries in each column of A add up to c ;*
- (2) *$J_{pm}A = cJ_{pn}$ for some $p \geq 1$;*
- (3) *$J_{pm}A = cJ_{pn}$ for every $p \geq 1$.*

Proof. Recall that for any two matrices X and Y , we can write $(XY)^T$ (the transpose of XY) as $Y^T X^T$. Observe that $J_{pm}^T = J_{mp}$. Then

- (1) is equivalent to: the entries in each row of A^T add up to c .
- (2) is equivalent to: $A^T J_{mp} = cJ_{np}$ for some $p \geq 1$.
- (3) is equivalent to: $A^T J_{mp} = cJ_{np}$ for every $p \geq 1$.

It is now clear the Theorem is an immediate consequence of Theorem 1.53. \square

We now recall some properties of determinants and ways of calculating them.

Fact 1.55. (a) *If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then $\det A = ad - bc$.*

(b) *If $A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$, then $\det A = a(ei - hf) - b(di - gf) + c(dh - ge)$.*

- (c) We can build up to larger matrices by 'expanding' along the first row. Suppose we have a 4×4 matrix A , with first row $A = [a_{11} \ a_{12} \ a_{13} \ a_{14}]$ and suppose that we denote by A_{1j} the 3×3 matrix obtained by deleting the first row and j 'th column. Then

$$\det A = a_{11}A_{11} - a_{12}A_{12} + a_{13}A_{13} - a_{14}A_{14}.$$

- (d) In fact we can expand by any row as long as we use an appropriate pattern of signs. The pattern $+ \ - \ + \ -$ used above comes from the first row of a sign

matrix $\begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}$. The same applies to any column. In each case

the 3×3 determinants arise by deleting the row and column through the appropriate entry. Thus

$$\det A = -a_{21}A_{21} + a_{22}A_{22} - a_{23}A_{23} + a_{24}A_{24}$$

$$= -a_{14}A_{14} + a_{24}A_{24} - a_{34}A_{34} + a_{44}A_{44}.$$

- (e) The $n \times n$ sign matrix is $\begin{bmatrix} + & - & + & \dots \\ - & + & - & \dots \\ + & - & + & \dots \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}$.

- (f) The determinant of a diagonal matrix (i.e., one in which all the non-(leading) diagonal entries are 0) is the product of the diagonal entries.
- (g) The determinant of an upper or lower triangular matrix (i.e., one in which all the entries below or above the leading diagonal are 0) is the product of the diagonal entries.
- (h) Any matrix with a row of 0s or with a column of 0s has determinant 0 (because expansion along that row or column must give 0).
- (i) The following operations do not change the value of the determinant:
- (1) To any row, add or subtract a multiple of another row.
 - (2) To any column, add or subtract a multiple of another column.
- (j) Using these row and column operations, we can 'reduce' a matrix to upper or lower triangular form.

Examples 1.56. (a) Find the determinant of $A = \begin{bmatrix} a & b & 0 \\ d & e & 0 \\ g & h & 0 \end{bmatrix}$ by expanding along an appropriate row or column.

Solution. Expand along the third column. We get $0(dh - ge) - 0(ah - gb) + 0(ae - db) = 0$.

(b) Find the determinant of the following matrix, using row and column reduction to triangular form:

$$M = \begin{bmatrix} 6 & 3 & 3 & 3 & 3 \\ 3 & 6 & 3 & 3 & 3 \\ 3 & 3 & 6 & 3 & 3 \\ 3 & 3 & 3 & 6 & 3 \\ 3 & 3 & 3 & 3 & 6 \end{bmatrix}.$$

Solution. Subtract Column 1 from each of Columns 2, 3, 4, 5 in turn (four operations):

$$\begin{aligned} \det M &= \begin{vmatrix} 6 & 3 & 3 & 3 & 3 \\ 3 & 6 & 3 & 3 & 3 \\ 3 & 3 & 6 & 3 & 3 \\ 3 & 3 & 3 & 6 & 3 \\ 3 & 3 & 3 & 3 & 6 \end{vmatrix} = \begin{vmatrix} 6 & -3 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 \\ 3 & 0 & 6 & 3 & 3 \\ 3 & 0 & 3 & 6 & 3 \\ 3 & 0 & 3 & 3 & 6 \end{vmatrix} = \begin{vmatrix} 6 & -3 & -3 & 3 & 3 \\ 3 & 3 & 0 & 3 & 3 \\ 3 & 0 & 3 & 3 & 3 \\ 3 & 0 & 0 & 6 & 3 \\ 3 & 0 & 0 & 3 & 6 \end{vmatrix} \\ &= \begin{vmatrix} 6 & -3 & -3 & -3 & 3 \\ 3 & 3 & 0 & 0 & 3 \\ 3 & 0 & 3 & 0 & 3 \\ 3 & 0 & 0 & 3 & 3 \\ 3 & 0 & 0 & 0 & 6 \end{vmatrix} = \begin{vmatrix} 6 & -3 & -3 & -3 & -3 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 3 \end{vmatrix}. \end{aligned}$$

Now add each of Rows 2, 3, 4, 5 to Row 1 in turn (four operations):

$$\begin{aligned} \det M &= \begin{vmatrix} 9 & 0 & -3 & -3 & -3 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 12 & 0 & 0 & -3 & -3 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 3 \end{vmatrix} \\ &= \begin{vmatrix} 15 & 0 & 0 & 0 & -3 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 3 \end{vmatrix} = \begin{vmatrix} 18 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & 0 \\ 3 & 0 & 3 & 0 & 0 \\ 3 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 3 \end{vmatrix}. \end{aligned}$$

We arrive at the determinant of a lower triangular matrix, so

$$\det M = 18 \times 3^4 = 1458.$$

1.12 Incidence Matrices

We shall associate a matrix with each $2 - (v, k, \lambda)$ block design. This will allow us to bring our knowledge of matrix theory to bear on our study of designs.

Definition 1.57. Let (X, \mathcal{B}) be a $2 - (v, k, \lambda)$ design with $b = |\mathcal{B}|$ and with each point of X lying in r blocks. Label the points of X : P_1, P_2, \dots, P_v and the blocks of \mathcal{B} : B_1, B_2, \dots, B_b in some order. The **incidence matrix** of the design $2 - (v, k, \lambda)$ is the matrix $A = [a_{ij}]_{b \times v}$ where $a_{ij} = 1$ if $P_j \in B_i$ and $a_{ij} = 0$ if $P_j \notin B_i$.

Thus row i tells you which points are in B_i (it has k 1s and $(v - k)$ 0s). Similarly, column j tells you which blocks P_j belongs to (it has r 1s and $(b - r)$ 0s).

NB: The incidence matrix of a block design is not unique, since it depends on the order in which you number the points and the blocks. But renumbering points corresponds to permuting the columns of the incidence matrix, and renumbering the blocks corresponds to permuting its rows. Thus permuting the rows and columns of the incidence matrix does not change the underlying block design.

Remark 1.58. A $\{0, 1\}$ -*matrix* is a matrix whose entries are

all 0 or 1. Thus an incidence matrix of a design is a $\{0, 1\}$ matrix.

Example 1.59. Write down an incidence matrix for the $2 - (7, 3, 1)$ design in Example 1.6.

Label the points X : $P_1 = 1, P_2 = 2, \dots, P_7 = 7$ and the blocks

$$B_1 = \{1, 6, 2\}, B_2 = \{2, 4, 3\}, B_3 = \{3, 5, 1\}, B_4 = \{1, 7, 4\},$$

$$B_5 = \{2, 7, 5\}, B_6 = \{3, 7, 6\}, B_7 = \{4, 5, 6\}.$$

This design has incidence matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Theorem 1.60. A $b \times v$ $\{0, 1\}$ matrix is the incidence matrix of a $2 - (v, k, \lambda)$ design if and only if

- (a) each row has k 1s;
- (b) all rows are different;
- (c) given any two columns, there are exactly λ rows with a 1 in both columns.

Proof. [\implies] Suppose that a $b \times v$ $\{0, 1\}$ matrix A is the incidence matrix of a $2 - (v, k, \lambda)$ design. Then (a) follows immediately from the fact that each block has k points, and (b) follows from the fact that the blocks are distinct. Given two columns, i and j say, the number of rows with a 1 in each of columns i and j is precisely the number of blocks containing both p_i and p_j , and this number is always λ ; this gives us (c).

[\impliedby] Suppose that a $\{0, 1\}$ matrix A satisfies (a), (b) and (c). Let X be a set of points labelled $1, 2, \dots, v$ and

construct subsets B_1, B_2, \dots, B_b of X by taking B_i to consist of precisely the numbers $j \in X$ such that $a_{ij} = 1$, i.e., such that the i 'th row of A has a 1 in column j . Then (a) says that each block has k members and (b) says that blocks are distinct (so that we have a set of blocks). Condition (c) says that each pair of points lies in precisely λ blocks. Thus we have a $2 - (v, k, \lambda)$ design, and the given matrix A is its incidence matrix. □

Remark 1.61. By Theorem 1.14, each column of an incidence matrix has r 1s, with all other entries 0, where $r = \frac{bk}{v}$.

Example 1.62. Show that there is a $2 - (6, 3, 2)$ design and that it is unique up to the labelling of points and blocks.

Solution

We look for a suitable incidence matrix. Assuming that a design exists, we have

- $v = 6, k = 3, \lambda = 2.$

$$\bullet b = \lambda \cdot \frac{v(v-1)}{k(k-1)} = \frac{2 \times 6 \times 5}{3 \times 2} = 10.$$

$$\bullet r = \frac{(v-1)\lambda}{k-1} = \frac{5 \times 2}{2} = 5.$$

Translating this information into matrix language, we see that we seek a $10 \times 6 \{0, 1\}$ matrix such that:

- (a) each row has 3 1s and 3 0s.
- (b) all rows are different.
- (c) each column has 5 1s and 5 0s.
- (d) any two columns have common 1s in exactly 2 rows.

Also remember that we can permute the columns (renumber the points) and permute the columns (renumber the blocks) without altering the design. We shall talk in terms of choosing labels for points and columns. This is something we can do when we have a collection of points or blocks that are indistinguishable up to the stage of choosing labels, but not when they are distinguishable. We write A for the incidence matrix.

1_A	1_A	1_A	0_A	0_A	0_A
1_B	1_C	0_E	1_E	0_E	0_E
1_B	0_C	1_F	0_L	1_P	0_P
1_B	0_C	0_F	1_I	0_R	1_R
1_B	0_C	0_F	0_L	1_O	1_O
0_B	1_D	1_G	0_M	0_T	1_T
0_B	1_D	0_G	1_J	1_S	0_S
0_B	1_D	0_G	0_M	1_O	1_O
0_B	0_D	1_H	1_K	1_Q	0_Q
0_B	0_D	1_H	1_N	0_Q	1_Q

- (A) Choose a block and label it B_1 , and label the three points in it P_1, P_2, P_3 . Then $a_{11} = a_{12} = a_{13} = 1$ and $a_{14} = a_{15} = a_{16} = 0$. [At this stage, B_1 is distinguishable from the other blocks (rows) but B_2, \dots, B_{10} are indistinguishable. The points P_1, P_2, P_3 are indistinguishable from each other, as are P_4, P_5, P_6 , but each of P_1, P_2, P_3 is distinguishable from each of P_4, P_5, P_6 .]
- (B) Consider the point P_1 . Now P_1 lies in 5 blocks: B_1 and a further 4 blocks that we label B_2, B_3, B_4, B_5 . Thus $a_{i1} = 1$ for $2 \leq i \leq 5$ and $a_{i1} = 0$ for $6 \leq i \leq 10$. [At this stage, P_1 is distinguishable from P_2, P_3 , and B_1 is

- distinguishable from B_2, B_3, B_4, B_5 , but P_2, P_3 are indistinguishable, as are B_2, B_3, B_4, B_5 .]
- (C) Consider the point P_2 . It lies together with P_1 in 2 blocks: B_1 and one other amongst B_2, B_3, B_4, B_5 . We choose to label as B_2 the one containing P_2 . This means that now P_2 does not lie in B_3, B_4, B_5 . Thus $a_{i2} = 1$ for $i = 1, 2$ and $a_{i2} = 0$ for $i = 3, 4, 5$. [At this stage B_3, B_4, B_5 are still indistinguishable.]
- (D) Consider further the point P_2 . It lies in 5 blocks: B_1, B_2 and a further 3 blocks that cannot be B_3, B_4, B_5 and that we therefore label B_6, B_7, B_8 . Thus $a_{i2} = 1$ for $i = 6, 7, 8$ and $a_{i2} = 0$ for $i = 9, 10$.
- (E) The block B_2 must contain 1 more point, but this point cannot be P_3 because $B_2 \neq B_1$. Therefore $a_{23} = 0$. We label as P_4 the other point in B_2 . Thus $a_{24} = 1$ and $a_{25} = a_{26} = 0$.
- (F) Consider the point P_3 . It lies together with P_1 in 2 blocks: B_1 and one other amongst B_3, B_4, B_5 . We choose to label as B_3 the one containing P_3 . This means that now P_3 does not lie in B_4, B_5 . Thus $a_{33} = 1$ and $a_{i3} = 0$ for $i = 4, 5$. [At this stage B_4, B_5 are still indistinguishable.]
- (G) P_3 also lies together with P_2 in 2 blocks: B_1 and one other amongst B_6, B_7, B_8 . We choose to label as B_6 the one containing P_3 . This means that now P_3 does not lie in B_7, B_8 . Thus $a_{36} = 1$ and $a_{i3} = 0$ for $i = 7, 8$. [At this stage B_7, B_8 are still indistinguishable.]
- (H) Consider further the point P_3 . It lies in 5 blocks: B_1, B_3, B_6 and a further 2 blocks that can only be B_9, B_{10} . Thus $a_{i3} = 1$ for $i = 9, 10$.
- (I) Rows 4 and 5 cannot both start 1000 (otherwise the remaining 2 1s will be in cols 5 and 6, and we would have 2 identical rows). Therefore either $a_{44} = 1$ or $a_{54} = 1$, i.e., at least one of B_4, B_5 contains P_4 . We choose to label by B_4 so that it contains P_4 . Thus $a_{44} = 1$.
- (J) Apply the same argument to rows 7 and 8. Label so that B_7 contains P_4 , i.e., $a_{74} = 1$.
- (K) Apply the same argument to rows 9 and 10. Label so that B_9 contains P_4 , i.e., $a_{94} = 1$.
- (L) We already have 2 common 1s in columns 1 and 4, i.e., P_1, P_4 already lie in two blocks (B_2, B_4), so P_4 cannot lie in B_3 or B_5 , i.e., $a_{34} = a_{54} = 0$.

- (M) We already have 2 common 1s in columns 2 and 4, i.e., P_2, P_4 already lie in two blocks (B_2, B_7) , so P_4 cannot lie in B_6 or B_8 , i.e., $a_{64} = a_{84} = 0$.
- (N) Column 4 must have 5 1s, so $a_{10\ 4} = 1$.
- (O) Each row must have 3 1s, so rows 5, 8 must be completed with 1s. Thus $a_{55} = a_{56} = a_{85} = a_{86} = 1$.
- (P) Block 3 has one more point, either P_5 or P_6 . We choose to label P_5 as the point in B_3 . Thus $a_{35} = 1, a_{36} = 0$.
- (Q) Blocks 9 and 10 each have one more point, but it cannot be the same point, so one contains P_5 and the other P_6 . We choose to label B_9 as the block containing P_5 . Thus $a_{95} = a_{10\ 6} = 1, a_{96} = a_{10\ 5} = 0$.
- (R) Points P_1 and P_5 lie in 2 blocks already: B_3 and B_5 ; so $a_{45} = 0$ and $a_{46} = 1$ as every row has 3 points.
- (S) Points P_4, P_5 lie in 2 blocks: B_9 is one, B_7 is the only possibility for the other. This means that B_7 now has 3 points, so P_6 is not in B_7 . Thus $a_{75} = 1, a_{76} = 0$.
- (T) Each column must have 5 1s, so we must have $a_{65} = 0, a_{66} = 1$, i.e., B_6 contains P_6 but not P_5 .

If we followed these instructions correctly we should have the incidence matrix:

1 _A	1 _A	1 _A	0 _A	0 _A	0 _A
1 _B	1 _C	0 _E	1 _E	0 _E	0 _E
1 _B	0 _C	1 _F	0 _L	1 _P	0 _P
1 _B	0 _C	0 _F	1 _I	0 _R	1 _R
1 _B	0 _C	0 _F	0 _L	1 _O	1 _O
0 _B	1 _D	1 _G	0 _M	0 _T	1 _T
0 _B	1 _D	0 _G	1 _J	1 _S	0 _S
0 _B	1 _D	0 _G	0 _M	1 _O	1 _O
0 _B	0 _D	1 _H	1 _K	1 _Q	0 _Q
0 _B	0 _D	1 _H	1 _N	0 _Q	1 _Q

We can now verify by inspection that we have a $2 - (6, 3, 2)$ design: check that

- (i) there are 6 columns;
- (ii) all rows are different;
- (iii) there are 3 1s in each row, and
- (iv) each pair of columns have precisely both have 1s in precisely 2 rows.

The design is unique in that the only choices of label that we have made have been amongst points or blocks that were, at that time, indistinguishable.

Theorem 1.63. Let $A = [a_{ij}]$ be a $\{0, 1\}$ matrix of dimension $b \times v$ and let $M = [m_{ij}]_{v \times v}$ be the matrix $A^T A$. Then m_{ij} is the number of occasions when the i 'th and j 'th columns of A both have entry 1. In particular, m_{ii} is the number of 1s in the i 'th column of A .

Proof. By the definition of matrix multiplication, m_{ij} is the result of multiplying the i 'th row of A^T by the j 'th column of A :

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \dots & a_{b1} \\ a_{12} & a_{22} & \dots & a_{b2} \\ \vdots & \vdots & \dots & \vdots \\ a_{1v} & a_{2v} & \dots & a_{bv} \end{bmatrix}, \quad A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1v} \\ a_{21} & a_{22} & \dots & a_{2v} \\ \vdots & \vdots & \dots & \vdots \\ a_{b1} & a_{b2} & \dots & a_{bv} \end{bmatrix}$$

so

$$m_{ij} = \begin{bmatrix} a_{1i} & a_{2i} & \dots & a_{bi} \end{bmatrix} \begin{bmatrix} a_{1j} \\ a_{2j} \\ a_{3j} \\ \vdots \\ a_{bj} \end{bmatrix} = \sum_{k=1}^b a_{ki} a_{kj}.$$

Each a_{ki} and each a_{kj} is either 0 or 1, so each term $a_{ki}a_{kj}$ is 1 if $a_{ki} = a_{kj} = 1$ and 0 otherwise. Thus each of the terms in $\sum_{k=1}^b a_{ki}a_{kj}$ is 1 or 0, and the sum is just the number of terms that are 1. Hence m_{ij} is the number of occasions when the i 'th and j 'th columns of A both have entry 1. If $i = j$, then this is the number of occasions when the i 'th column of A has entry 1, so is the number of 1s in the column. □

Theorem 1.64. Let $A = [a_{ij}]$ be a $\{0, 1\}$ matrix of dimension $b \times v$ and let $M = [m_{ij}]_{v \times v}$ be the matrix $A^T A$.

(a) If A is the incidence matrix of a $2 - (v, k, \lambda)$ design, then $M = (r - \lambda)I_v + \lambda J_{vv}$.

(b) If A has distinct rows, each with $k < v$ entries equal to 1, and if $M = (r - \lambda)I_v + \lambda J_{vv}$, then A is the incidence matrix of a $2 - (v, k, \lambda)$ design, where $k = \frac{vr}{b}$.

Proof. (a) By Theorem 1.60(c), given any two columns, there

are exactly λ rows with a 1 in both columns. By Re-

mark 1.61, each column has r 1s. Therefore, by The-

orem 1.63, $m_{ii} = r$ for each i , and $m_{ij} = \lambda$ for all i, j

with $i \neq j$. Thus

$$M = \begin{bmatrix} r & \lambda & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & r & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & \lambda & r & \dots & \dots & \lambda & \lambda \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ \lambda & \lambda & \lambda & \dots & \dots & \lambda & r \end{bmatrix} =$$

$$\begin{bmatrix} r - \lambda & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & r - \lambda & 0 & \dots & \dots & 0 & 0 \\ 0 & 0 & r - \lambda & \dots & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \dots & 0 & r - \lambda \end{bmatrix} + \begin{bmatrix} \lambda & \lambda & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & \lambda & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & \lambda & \lambda & \dots & \dots & \lambda & \lambda \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ \lambda & \lambda & \lambda & \dots & \dots & \lambda & \lambda \end{bmatrix}$$

$$= (r - \lambda)I_v + \lambda J_{vv}.$$

(b) By Theorem 1.60, we need only show that: given any

two columns, there are exactly λ rows with a 1 in both

columns. But this follows from Theorem 1.63.

□

Theorem 1.65. Let A be an incidence matrix for a $2 - (v, k, \lambda)$ design and let $M = A^T A$. Then $\det M = (r - \lambda)^{v-1}(r + (v - 1)\lambda)$.

Proof. By Theorem 1.64(a),

$$M = \begin{bmatrix} r & \lambda & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & r & \lambda & \dots & \dots & \lambda & \lambda \\ \lambda & \lambda & r & \dots & \dots & \lambda & \lambda \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ \lambda & \lambda & \lambda & \dots & \dots & \lambda & r \end{bmatrix}.$$

We can perform row and column operations on M that do not change the determinant. First we subtract Column 1 from each of the other columns to give

$$\begin{bmatrix} r & \lambda - r & \lambda - r & \dots & \dots & \lambda - r & \lambda - r \\ \lambda & r - \lambda & 0 & \dots & \dots & 0 & 0 \\ \lambda & 0 & r - \lambda & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ \lambda & 0 & 0 & \dots & \dots & 0 & r - \lambda \end{bmatrix}.$$

Second we add Row 2 to Row 1, then add each subsequent row in turn, to give

$$B = \begin{bmatrix} r + (v-1)\lambda & 0 & 0 & \dots & \dots & 0 & 0 \\ \lambda & r - \lambda & 0 & \dots & \dots & 0 & 0 \\ \lambda & 0 & r - \lambda & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \dots & \dots & \vdots & \vdots \\ \lambda & 0 & 0 & \dots & \dots & 0 & r - \lambda \end{bmatrix}.$$

Now B is a lower triangular matrix, so its determinant is given by the product of the diagonal entries. Thus

$$\det M = \det B = (r - \lambda)^{v-1}(r + (v-1)\lambda).$$

□

Proof of Theorem 1.34, Fisher's Inequality. We need to prove that if $v > k$, then $b \geq v$. Recall that, by Corollary 1.15, we have $r > \lambda$.

Suppose that (X, \mathcal{B}) is a $2 - (v, k, \lambda)$ design with $v > b$ and let A be an incidence matrix for the design. Let A^* be the $v \times v$ matrix formed from A by

adding $v - b$ rows of zeros to the bottom of A . Thus

$$A^* = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1v} \\ a_{21} & a_{22} & \dots & a_{2v} \\ \vdots & \vdots & \dots & \vdots \\ a_{b1} & a_{b2} & \dots & a_{bv} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

Observe that

$$(A^*)^T A^* = \begin{bmatrix} a_{11} & a_{21} & \dots & a_{b1} & 0 & \dots & 0 \\ a_{12} & a_{22} & \dots & a_{b2} & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ a_{1v} & a_{2v} & \dots & a_{bv} & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1v} \\ a_{21} & a_{22} & \dots & a_{2v} \\ \vdots & \vdots & \dots & \vdots \\ a_{b1} & a_{b2} & \dots & a_{bv} \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{bmatrix}.$$

If we write $N = (n_{ij})$ for $(A^*)^T A^*$ and $M = (m_{ij})$ for $A^T A$, then N and M are both $v \times v$ matrices and

$$n_{ij} = \begin{bmatrix} a_{1i} & a_{2i} & \dots & a_{bi} & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} a_{1j} \\ a_{2j} \\ a_{3j} \\ \vdots \\ a_{bj} \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \sum_{k=1}^b a_{ki} a_{kj} = m_{ij}.$$

Therefore $(A^*)^T A^* = A^T A$.

We calculate the determinant of this matrix in two ways.

First way. A^* is square and so it has a determinant (and the same applies to $(A^*)^T$). A^* has a row of zeros, so its determinant is 0. Thus

$$\det((A^*)^T A^*) = \det(A^*)^T \det A^* = \det(A^*)^T \times 0 = 0.$$

Second way. By Theorem 1.65, we know that $\det M = (r - \lambda)^{v-1}(r + (v - 1)\lambda)$. Given that $r > \lambda$, it follows that $\det M > 0$.

The determinant of M does not depend on the way in which it is calculated. Therefore we have a contradiction and we must conclude that the supposition $b < v$ is false.

Hence $b \geq v$.

□

1.13 Symmetric Designs

We return to studying symmetric designs (where $b = v$). We use matrix tools to prove Theorem 1.44.

Proof of Theorem 1.44. Recall that we need to prove: In a symmetric $2-(v, k, \lambda)$ design with v even, $k - \lambda$ must be a perfect square.

Let A be an incidence matrix for a symmetric $2-(v, k, \lambda)$

design and let $M = A^T A$. By Theorem 1.65, $\det M =$

$(r - \lambda)^{v-1}(r + (v - 1)\lambda)$. Given that $r = \lambda \frac{(v - 1)}{(k - 1)}$ for

a symmetric design and we have $r = k$, we can deduce

that $r + (v - 1)\lambda = r + (k - 1)r = rk = k^2$. Thus

$$\det M = (k - \lambda)^{v-1}k^2 = (k - \lambda)(k - \lambda)^{v-2}k^2 = (k - \lambda)[(k - \lambda)^{(v-2)/2}k]^2.$$

When the design is symmetric we have $b = v$ and so A

is a square matrix. Moreover $\det A^T = \det A$. Therefore

$\det M = \det A^T \det A = (\det A)^2$. It follows that

$$(\det A)^2 = (k - \lambda)[(k - \lambda)^{(v-2)/2}k]^2.$$

As $2 \leq k \leq v = b$, there is more than one block and so

$k < v$. Thus $k = r > \lambda$ (by Corollary 1.15) and

$$(k - \lambda) = \left[\frac{\det A}{(k - \lambda)^{(v-2)/2} k} \right]^2$$

so is a perfect square. □

Theorem 1.66. *If A is an incidence matrix for a symmetric $2 - (v, k, \lambda)$ design, then A is invertible.*

Proof. As seen in the proof of Theorem 1.44 above, $(\det A)^2 =$

$(k - \lambda)^{v-1} k^2$. For a symmetric design we have $v > k$ so

that $k = r > \lambda$ and hence $\det A \neq 0$. □

Theorem 1.67 (Ryser). *In a symmetric $2 - (v, k, \lambda)$ design, any two distinct blocks have precisely λ points in common.*

Proof. Let A be an incidence matrix for the design. Then, by Theorem 1.64, $A^T A = (r - \lambda)I_v + \lambda J_{vv}$. By Theorem 1.66, we know that A^{-1} exists. By Theorem's 1.53 and 1.54, we know that $AJ_{vv} = kJ_{vv}$ and $J_{vv}A = rJ_{vv} = kJ_{vv} = AJ_{vv}$. Therefore

$$\begin{aligned} (A^T)^T A^T &= AA^T = A(A^T A)A^{-1} = A((r - \lambda)I_v + \lambda J_{vv})A^{-1} \\ &= (r - \lambda)AI_v A^{-1} + \lambda AJ_{vv} A^{-1} = (r - \lambda)I_v + \lambda J_{vv} AA^{-1} = (r - \lambda)I_v + \lambda J_{vv}. \end{aligned}$$

We now apply Theorem 1.63 to $(A^T)^T A^T$. In this context, $M = A^T A$ is also $(A^T)^T A^T$, and therefore m_{ij} is the number of occasions when the i 'th and j 'th columns of A^T both have entry 1. For $i \neq j$, it follows that $m_{ij} = \lambda$ is the number of occasions when the i 'th and j 'th rows of A both have entry 1, i.e., it is the number of points that lie in both of blocks i and j . □

Example 1.68. Show that there is a projective plane of order 3.

Solution Such a design would be a symmetric 2 – (13, 4, 1) design. We look for a suitable incidence matrix. Assuming that a design exists, we have

- $v = b = 13$, $k = r = 4$, $\lambda = 1$.

- Any two blocks have exactly one point in common.

Translating this information into matrix language, we see that we seek a 13×13 $\{0, 1\}$ matrix such that:

- (a) Each row has 4 1s and 9 0s.

- (b) All rows are different.

- (c) Each column has 4 1s and 9 0s.

- (d) Any two columns have common 1s in exactly 1 row.

- (e) Any two rows have common 1s in exactly 1 column.

Also remember that we can permute the columns (renumber the points) and permute the rows (renumber the blocks) without altering the design. We shall talk in terms of choosing labels for points and columns. This is something we can do when we have a collection of points or blocks that are indistinguishable up the stage of choosing labels, but not when they are distinguishable. We write A for the incidence matrix.

1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	1	1	1	0	0	0
1	0	0	0	0	0	0	0	0	0	1	1	1
0	1	0	0	1	0	0	1	0	0	1	0	0
0	1	0	0	0	1	0	0	1	0	0	1	0
0	1	0	0	0	0	1	0	0	1	0	0	1
0	0	1	0	1	0	0	0	1	0	0	0	1
0	0	1	0	0	1	0	0	0	1	1	0	0
0	0	1	0	0	0	1	1	0	0	0	1	0
0	0	0	1	1	0	0	0	0	1	0	1	0
0	0	0	1	0	1	0	1	0	0	0	0	1
0	0	0	1	0	0	1	0	1	0	1	0	0

- (1) Choose a block and label it B_1 , and label the four points in it P_1, P_2, P_3, P_4 . Then $a_{1j} = 1$ for $1 \leq j \leq 4$ and $a_{1j} = 0$ for $5 \leq j \leq 13$.
- (2) Consider the point P_1 . Now P_1 lies in 4 blocks: B_1 and a further 3 blocks that we label B_2, B_3, B_4 . Thus $a_{i1} = 1$ for $2 \leq i \leq 4$ and $a_{i1} = 0$ for $5 \leq i \leq 13$.
- (3) B_1 meets each of B_2, B_3, B_4 in exactly one point, namely P_1 , so $a_{ij} = 0$ for $2 \leq i, j \leq 4$.

- (4) B_2 contains 3 more points that we label P_5, P_6, P_7 . Thus $a_{2j} = 1$ for $5 \leq j \leq 7$ and $a_{2j} = 0$ for $8 \leq j \leq 13$.
- (5) B_2 meets each of B_3, B_4 in exactly one point, namely P_1 , so $a_{ij} = 0$ for $i = 3, 4, 5 \leq j \leq 7$.
- (6) B_3 contains 3 more points that we label P_8, P_9, P_{10} . Thus $a_{3j} = 1$ for $8 \leq j \leq 10$ and $a_{3j} = 0$ for $11 \leq j \leq 13$.
- (7) B_3 meets B_4 in exactly one point, namely P_1 , so $a_{4j} = 0$ for $8 \leq j \leq 10$.
- (8) B_4 contains 3 more points that can only be P_{11}, P_{12}, P_{13} . Thus $a_{4j} = 1$ for $11 \leq j \leq 13$.
- (9) P_2 lies in 4 blocks: B_1 and a further 3 blocks that we label B_5, B_6, B_7 . Thus $a_{i2} = 1$ for $i = 5, 6, 7$ and $a_{i2} = 0$ for $8 \leq i \leq 13$.
- (10) B_1 meets each of B_5, B_6, B_7 in exactly one point, namely P_2 , so $a_{ij} = 0$ for $5 \leq i \leq 7, j = 3, 4$.
- (11) P_3 lies in 4 blocks: B_1 and a further 3 blocks that we label B_8, B_9, B_{10} . Thus $a_{i3} = 1$ for $8 \leq i \leq 13$ and $a_{i3} = 0$ for $11 \leq i \leq 13$.
- (12) B_1 meets each of B_8, B_9, B_{10} in exactly one point, namely P_3 , so $a_{i4} = 0$ for $8 \leq i \leq 10$.
- (13) P_4 lies in 4 blocks: B_1 and a further 3 blocks that can only be B_{11}, B_{12}, B_{13} . Thus $a_{i4} = 1$ for $11 \leq i \leq 13$.
- (14) P_2 and P_5 lie together in 1 block. This must be one of B_5, B_6, B_7 . These blocks are currently indistinguishable. We choose to label as B_5 the one that contains P_5 . Thus $a_{55} = 1$ and $a_{i5} = 0$ for $i = 5, 6$.
- (15) P_3 and P_5 lie together in 1 block. This must be one of B_8, B_9, B_{10} . These blocks are currently indistinguishable. We choose to label as B_8 the one that contains P_5 . Thus $a_{58} = 1$ and $a_{i5} = 0$ for $i = 9, 10$.
- (16) P_4 and P_5 lie together in 1 block. This must be one of B_{11}, B_{12}, B_{13} . These blocks are currently indistinguishable. We choose to label as B_{11} the one that contains P_5 . Thus $a_{511} = 1$ and $a_{i5} = 0$ for $i = 12, 13$.
- (17) B_5 meets B_2 in exactly one point, namely P_5 , so $a_{5j} = 0$ for $j = 6, 7$.
- (18) P_2 and P_6 lie together in 1 block. This must be one of B_6, B_7 . These blocks are currently indistinguishable. We choose to label as B_6 the one that contains P_5 . Thus $a_{66} = 1$ and $a_{76} = 0$.

- (19) B_6 meets B_2 in exactly one point, namely P_6 , so $a_{67} = 0$.
- (20) P_2 and P_7 lie together in 1 block. This can only be B_7 . Thus $a_{77} = 1$.
- (21) B_8 meets B_2 in exactly one point, namely P_5 , so $a_{8j} = 0$ for $j = 6, 7$.
- (22) P_3 and P_6 lie together in 1 block. This must be one of B_9, B_{10} . These blocks are currently indistinguishable. We choose to label as B_9 the one that contains P_6 . Thus $a_{96} = 1$ and $a_{106} = 0$.
- (23) B_9 meets B_2 in exactly one point, namely P_6 , so $a_{97} = 0$.
- (24) P_3 and P_7 lie together in 1 block. This can only be B_{10} . Thus $a_{107} = 1$.
- (25) B_{11} meets B_2 in exactly one point, namely P_5 , so $a_{11j} = 0$ for $j = 6, 7$.
- (26) P_4 and P_6 lie together in 1 block. This must be one of B_{12}, B_{13} . These blocks are currently indistinguishable. We choose to label as B_{12} the one that contains P_6 . Thus $a_{126} = 1$ and $a_{136} = 0$.
- (27) B_{12} meets B_2 in exactly one point, namely P_6 , so $a_{127} = 0$.
- (28) P_4 and P_7 lie together in 1 block. This can only be B_{13} . Thus $a_{137} = 1$.
- (29) B_3 and B_5 meet in one point. This must be one of P_8, P_9, P_{10} . These points are currently indistinguishable. We choose to label as P_8 the one that lies in B_5 . Thus $a_{85} = 1$ and $a_{5j} = 0$ for $j = 9, 10$.
- (30) B_5 meets each of B_6 and B_7 in one point, namely P_2 , so P_8 is not in B_6, B_7 . Thus $a_{i8} = 0$ for $i = 6, 7$.
- (31) B_3 and B_6 meet in one point. This must be one of P_9, P_{10} . These points are currently indistinguishable. We choose to label as P_9 the one that lies in B_6 . Thus $a_{69} = 1$ and $a_{610} = 0$.
- (32) B_6 meets B_7 in one point, namely P_2 , so P_9 is not in B_7 . Thus $a_{79} = 0$.
- (33) B_3 and B_7 meet in a point and this can only be P_{10} . Thus $a_{710} = 1$.
- (34) B_4 and B_5 meet in one point. This must be one of P_{11}, P_{12}, P_{13} . These points are currently indistinguishable. We choose to label as P_{11} the one that lies in B_5 . Thus $a_{511} = 1$ and $a_{5j} = 0$ for $j = 12, 13$.
- (35) B_5 meets each of B_6 and B_7 in one point, namely P_2 , so P_{11} is not in B_6, B_7 . Thus $a_{i11} = 0$ for $i = 6, 7$.

- (36) B_4 and B_6 meet in one point. This must be one of P_{12}, P_{13} . These points are currently indistinguishable. We choose to label as P_{12} the one that lies in B_6 . Thus $a_{6\ 12} = 1$ and $a_{6\ 13} = 0$.
- (37) B_6 meets B_7 in one point, namely P_2 , so P_{12} is not in B_7 . Thus $a_{7\ 12} = 0$.
- (38) B_4 and B_7 meet in a point and this can only be P_{13} . Thus $a_{7\ 13} = 1$. [Alternatively, B_7 has one more point.]
- (39) B_5 and B_8 meet in one point, namely P_5 , so P_8 and P_{11} do not lie in B_8 .
- (40) B_6 and B_9 meet in one point, namely P_6 , so P_9 and P_{12} do not lie in B_9 .
- (41) B_7 and B_{10} meet in one point, namely P_7 , so P_{10} and P_{13} do not lie in B_{10} .
- (42) B_3 and B_8 meet in one point, either P_9 or P_{10} . We choose P_9 . At this stage, P_9 and P_{10} are distinguishable, so in making this choice we hope to be able to complete the matrix and show the existence of a design, but the choice is not just one of labelling so the resulting design is not necessarily unique.
- (43) B_8 and B_{10} meet in one point, namely P_3 , so P_9 does not lie in B_{10} .
- (44) B_3 and B_{10} meet in one point, this can only be P_8 .
- (45) B_9 and B_{10} meet in one point, namely P_3 , so P_8 does not lie in B_9 .
- (46) B_3 and B_9 meet in one point, this can only be P_{10} .
- (47) B_6 and B_8 meet in one point, namely P_9 , so P_{12} does not lie in B_8 .
- (48) B_7 and B_9 meet in one point, namely P_{10} , so P_{13} does not lie in B_9 .
- (49) B_5 and B_{10} meet in one point, namely P_8 , so P_{11} does not lie in B_{10} .
- (50) B_8, B_9, B_{10} each need one more point, but in each case only one is possible: B_8 contains P_{13} , B_9 contains P_{11} and B_{10} contains P_{12} .
- (51) B_5 and B_{11} meet in one point, namely P_5 , so P_8 does not lie in B_{11} .
- (52) B_8 and B_{11} meet in one point, namely P_5 , so P_9 does not lie in B_{11} .
- (53) B_3 and B_{11} meet in one point, this can only be P_{10} .
- (54) B_9 and B_{11} meet in one point, namely P_{10} , so P_{11} does not lie in B_{11} .
- (55) B_8 and B_{11} meet in one point, namely P_5 , so P_{13} does not lie in B_{11} .

- (56) B_4 and B_{11} meet in one point, this can only be P_{12} .
- (57) B_{11} meets each of B_{12}, B_{13} in P_4 , so P_{10} and P_{12} do not lie in B_{12}, B_{13} .
- (58) B_{10} and B_{13} meet in one point, namely P_7 , so P_8 does not lie in B_{13} .
- (59) B_3 and B_{13} meet in one point, this can only be P_9 .
- (60) P_8 must lie in one more block, and this can only be B_{12} .
- (61) P_9 already lies in 4 blocks, so P_9 does not lie in B_{12} .
- (62) B_5 and B_{12} meet in one point, namely P_8 , so P_{11} does not lie in B_{12} .
- (63) P_{11} must lie in one more block, and this can only be B_{13} .
- (64) B_{12} has one more point and this can only be P_{13} .
- (65) P_{13} already lies in 4 blocks, so P_{13} does not lie in B_{13} .

This gives the incidence matrix

1	1	1	1	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	1	1	1	0	0	0
1	0	0	0	0	0	0	0	0	0	1	1	1
0	1	0	0	1	0	0	1	0	0	1	0	0
0	1	0	0	0	1	0	0	1	0	0	1	0
0	1	0	0	0	0	1	0	0	1	0	0	1
0	0	1	0	1	0	0	0	1	0	0	0	1
0	0	1	0	0	1	0	0	0	1	1	0	0
0	0	1	0	0	0	1	1	0	0	0	1	0
0	0	0	1	1	0	0	0	0	1	0	1	0
0	0	0	1	0	1	0	1	0	0	0	0	1
0	0	0	1	0	0	1	0	1	0	1	0	0

We can now verify by inspection that we have a 2 –

(13, 4, 1) design: check that

- (i) there are 13 columns;
- (ii) all rows are different;
- (iii) there are 4 1s in each row, and
- (iv) each pair of columns have precisely both have 1s in precisely 1 row.

We have not shown that the design is unique.

Remarks 1.69. (a) Observe that the matrix we have obtained is square, but it is not symmetric (this is why the term 'symmetric' for such designs is misleading).

- (b) In fact, there is a unique $2 - (13, 4, 1)$ design. To see this we have to note that the only arbitrary choice of label was in line (42). If we had chosen the other way, we should have arrived at another matrix (actually the transpose of the given one). We can pass from one to the other by the following row and column operations (performed in the given order): $C_9 \leftrightarrow C_{10}$, $R_6 \leftrightarrow R_7$, $C_6 \leftrightarrow C_7$, $R_9 \leftrightarrow R_{10}$, $R_{12} \leftrightarrow R_{13}$, $C_{12} \leftrightarrow C_{13}$.
- (c) When we made the arbitrary choice, conceivably we could have arrived at no allowable matrix. In that case we would have returned to line (42) and made the other choice.
- (d) If we find that we cannot construct an allowable matrix, then we would conclude that no design existed with the given parameters.

2 Geometry Of The Projective Plane

In 1812 Napoleon invaded Russia. Unlike Hitler 129 years later, he succeeded in capturing Moscow. On the other hand, like Hitler, he found that the Russian winter was a more formidable enemy than the Russian army. His Russian adventure turned into a disaster. Among the French officers captured by the Russians was one J.V. Poncelet. To pass the time in his Russian jail he decided to write down all the geometry that he could remember. This led him to invent Projective Geometry

2.1 The Euclidean Plane \mathbb{E}

Poncelet's starting point was the familiar Euclidean plane. The Euclidean plane consists of points $P = (\alpha, \beta)$, where α and β are real numbers (these are cartesian coordinates).

Definition 2.1. A line in the Euclidean plane consists of all points (x, y) satisfying an equation of the form

$$ax + by + c = 0 \quad (*)$$

where $(a, b) \neq (0, 0)$. (When we write $(a, b) \neq (0, 0)$ we mean that either $a \neq 0$ or $b \neq 0$ or both.)

Since the line above is completely specified by the equation (*), we often refer to “the line $ax + by + c = 0$ ”.

Of course, if $k \neq 0$, this is just the same line as the line $kax + kby + kc = 0$. We say that two lines $ax + by + c = 0$

and $Ax + By + C = 0$ are the same precisely when

$A = ka, B = kb, C = kc$ for some $k \neq 0$.

The **gradient** of (*) is defined to be

$$-\frac{a}{b} \text{ if } b \neq 0$$

and to be

$$\infty \text{ if } b = 0.$$

Note:

- The symbol ∞ is just that: a symbol. It is not the result of a calculation $\frac{a}{0}$ and it is neither positive nor negative.
- If $b \neq 0$ then (*) becomes $y = -\frac{a}{b}x - \frac{c}{b}$; if $b = 0$ it becomes $x = -\frac{c}{a}$.

Definition 2.2. Distinct lines

$$\begin{aligned} ax + by + c &= 0 \\ Ax + By + C &= 0 \end{aligned}$$

are said to be **parallel** if $Ab = aB$.

Thus distinct lines are parallel if and only if they have the same gradient. To see this, let $Ab = aB$. Then

(i) If $b = 0$, then $a \neq 0$ and $aB = Ab = 0$, so $B = 0$.

Thus both gradients are ∞ .

(ii) If $b \neq 0$, then $B \neq 0$ (because $B = 0$ implies $b = 0$,

arguing as in (i)), which implies $-\frac{a}{b} = -\frac{A}{B}$ so that

the gradients are equal.

Exercise 2.3. (a) Show that if lines $ax + by + c = 0$ and $Ax + By + C = 0$ with $Ab = aB$ have at least one point in common, then they are equal. [Thus parallel lines do not intersect.]

(b) Show that distinct non-parallel lines $ax + by + c = 0$ and $Ax + By + C = 0$ both pass through the point $\left(\frac{bC - cB}{Ba - bA}, \frac{Ac - aC}{Ba - bA}\right)$.

N.B.: This shows that lines in the Euclidean plane are parallel if and only if they do not intersect.

Theorem 2.4. Given a pair of (distinct) points (p, q) and (u, v) in \mathbb{E} there is a unique line containing them, and it has equation

$$\begin{vmatrix} x & y & 1 \\ p & q & 1 \\ u & v & 1 \end{vmatrix} = 0.$$

Proof. **Begin by noting that determinant equation is $(q - v)x - (p - u)y + (vp - uq) = 0$. Let this be the line m .**

Consider a line $ax + by + c = 0$ passing through (p, q) and (u, v) : we have equations

$$au + bv + c = 0$$

$$ap + bq + c = 0$$

from which we deduce that

$$a(u - p) + b(v - q) = 0.$$

Suppose first that $u \neq p$. Then

$$a = -\frac{(v - q)}{(u - p)}b, \quad c = \frac{(vp - uq)}{(u - p)}b$$

which implies that $b \neq 0$ since a, b cannot both be 0, and

then the line is

$$-\frac{(v - q)}{(u - p)}bx + by + \frac{(vp - uq)}{(u - p)}b = 0$$

i.e.,

$$-(v - q)x + (u - p)y + (vp - uq) = 0.$$

In other words the line must be m .

Now suppose that $u = p$. Then $v \neq q$. In this case we have $b(v - q) = 0$, which implies that $b = 0$ (so that

necessarily $a \neq 0$) and $c = -au = -ap$ so that the line is

$$ax - ap = 0,$$

in other words $x - p = 0$. Observe that in this case m is given by $(q-v)x + (vp-pq) = 0$, i.e., $(q-v)x - p(q-v) = 0$, so by $x - p = 0$.

In each case there is a unique line through the given points and it is the line m .

□

Example 2.5. Find the equation of the line through the points $(-5, 6)$ and $(6, -7)$.

Solution.

The line has equation

$$\begin{vmatrix} x & y & 1 \\ -5 & 6 & 1 \\ 6 & -7 & 1 \end{vmatrix} = 0,$$

i.e.,

$$(6 + 7)x - y(-5 - 6) + 1(35 - 36) = 0,$$

i.e.,

$$13x + 11y - 1 = 0.$$

(Check that the line passes through the two given points!)

2.2 The Line At Infinity

\mathbb{E} is awkward to handle because of special cases:

- 2 lines meet at a unique point, unless they are parallel;
- $ax + by + c = 0$ is not a line if $a = b = 0$;
- gradient has a special definition if $b = 0$.

Poncelet had the bright idea of adding “points at infinity” where parallel lines would meet. We shall see that this removes the special cases. This new projective geometry had been foreshadowed by Renaissance painters such as Leonardo da Vinci, as they strove to make paintings more realistic. If you stand in the middle of a straight railroad track stretching into the distance, you will see that the two rails appear to converge “at infinity”. We shall begin by introducing homogeneous coordinates. We shall represent a point of \mathbb{E} not by a pair of real numbers (x, y) but by a triple (x, y, z) where $z \neq 0$.

Definition 2.6. ?? In \mathbb{E} , the triple (x, y, z) , with $z \neq 0$, is a **homogeneous coordinate representation** of the point with cartesian coordinates

$$\left(\frac{x}{z}, \frac{y}{z}\right).$$

Note that every point (u, v) of \mathbb{E} has homogeneous coordinates $(u, v, 1)$. Also, if $k \neq 0$ then the triples (x, y, z) and (kx, ky, kz) represent the same point.

Homogeneous Coordinates		Cartesian Coordinates
$(9, -33, 1)$	\longleftrightarrow	$(9, -33)$
$(0, 0, 1)$	\longleftrightarrow	$(0, 0)$
$(35, 15, 5)$	\longleftrightarrow	$(7, 3)$
$(7, 3, 1)$	\longleftrightarrow	$(7, 3)$
$(14, -21, 7)$	\longleftrightarrow	$(2, -3)$
$(10, -15, 5)$	\longleftrightarrow	$(2, -3)$
$(2, -3, 1)$	\longleftrightarrow	$(2, -3)$
$(0, 0, 5)$	\longleftrightarrow	$(0, 0)$
$(\lambda x, \lambda y, \lambda z)$	\longleftrightarrow	$\left(\frac{x}{z}, \frac{y}{z}\right)$ if $\lambda \neq 0$.

Thus (x, y, z) and (u, v, w) represent the same point of the Euclidean plane if and only if there exists a number λ such that $u = \lambda x$, $v = \lambda y$, $w = \lambda z$. We write simply $(x, y, z) = (u, v, w)$.

Example 2.7. We can introduce homogeneous coordinates in other planes, e.g., in

$$\mathbb{C}^2 = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{C}\}.$$

Here the homogeneous coordinates take the form (ξ, η, ζ) , where $\xi, \eta, \zeta \in \mathbb{C}$ and $\zeta \neq 0$, representing the point $\left(\frac{\xi}{\zeta}, \frac{\eta}{\zeta}\right) \in \mathbb{C}^2$.

For example, the two sets of homogeneous coordinates

$(1 + i, 1 - i, 2)$, $(1, -i, 1 - i)$ represent the same point in

\mathbb{C}^2 since

$$(1 + i)1 = 1 + i$$

$$(1 + i)(-i) = 1 - i$$

$$(1 + i)(1 - i) = 2.$$

In fact, \mathbb{R} or \mathbb{C} can be replaced by any field \mathbb{K} .

We shall now extend \mathbb{E} by allowing points with $z = 0$. In fact, we allow all points (x, y, z) except $(0, 0, 0)$. As before, we have $(x, y, z) = (\lambda x, \lambda y, \lambda z)$ if $\lambda \neq 0$.

Definition 2.8. Let \mathbb{K} be any field. Then the **projective plane** $\mathbb{P}_2(\mathbb{K})$ consists of all triples $(x, y, z) \neq (0, 0, 0)$, with $x, y, z \in \mathbb{K}$, and where

$$(x, y, z) = (\lambda x, \lambda y, \lambda z)$$

for every $\lambda \in \mathbb{K}$ with $\lambda \neq 0$. We call (x, y, z) the **homogeneous coordinates** of a point in $\mathbb{P}_2(\mathbb{K})$.

Note that the points of $\mathbb{P}_2(\mathbb{K})$ are of two types:

(i) the points of \mathbb{E} : (x, y, z) with $z \neq 0$;

(ii) the new points $(x, y, 0)$ with $(x, y) \neq (0, 0)$.

2.3 Lines in $\mathbb{P}_2(\mathbb{K})$

Recall that the lines in \mathbb{E} are of the form $ax + by + c = 0$ with $(a, b) \neq (0, 0)$, i.e., if we let $x = X/Z, y = Y/Z$,

$$a \left(\frac{X}{Z} \right) + b \left(\frac{Y}{Z} \right) + c = 0$$

i.e.,

$$aX + bY + cZ = 0.$$

This prompts the following definition:

Definition 2.9. Let $(l, m, n) \neq (0, 0, 0)$. Then the points (x, y, z) of $\mathbb{P}_2(\mathbb{K})$ such that $lx + my + nz = 0$ form a **line** in $\mathbb{P}_2(\mathbb{K})$ with homogeneous coordinates

$$[l, m, n].$$

Note the use of round brackets for points and square brackets for lines.

Remarks 2.10. (a) **This definition makes sense because, if $\lambda \neq$**

0, then $(\lambda x, \lambda y, \lambda z)$ lies on the line $[l, m, n]$

$$\iff l(\lambda x) + m(\lambda y) + n(\lambda z) = 0$$

$$\iff \lambda(lx + my + nz) = 0$$

$$\iff lx + my + nz = 0$$

i.e. $\iff (x, y, z)$ lies on the line $[l, m, n]$. [Thus we

don't find that (x, y, z) lies on a line, but that $(\lambda x, \lambda y, \lambda z)$

(which is supposed to be the same point) doesn't.]

(b) Note that if $\lambda \neq 0$ then $[\lambda l, \lambda m, \lambda n] = [l, m, n]$. For if

$\lambda \neq 0$, then (x, y, z) lies on the line $[\lambda l, \lambda m, \lambda n]$

$$\iff (\lambda l)x + (\lambda m)y + (\lambda n)z = 0$$

$$\iff \lambda(lx + my + nz) = 0$$

$$\iff lx + my + nz = 0$$

i.e. $\iff (x, y, z)$ lies on the line $[l, m, n]$.

(c) The point (x, y, z) lies on the line $[l, m, n]$ precisely

when $lx + my + nz = 0$, i.e, precisely when

$$(x \ y \ z) \begin{pmatrix} l \\ m \\ n \end{pmatrix} = (x \ y \ z) (l \ m \ n)^T = 0.$$

Summary

\mathbb{E} : **Points** All (x, y, z) with $z \neq 0$ (with $(x, y, z) = (\lambda x, \lambda y, \lambda z)$ whenever $\lambda \neq 0$).

Lines All $[l, m, n]$ with $(l, m) \neq (0, 0)$ (with $[l, m, n] = [\lambda l, \lambda m, \lambda n]$ whenever $\lambda \neq 0$).

$\mathbb{P}_2(\mathbb{K}) - \mathbb{E}$: **Points** All $(x, y, 0)$ with $(x, y) \neq (0, 0)$ (with $(x, y, 0) = (\lambda x, \lambda y, 0)$ whenever $\lambda \neq 0$).

Lines The line $[0, 0, 1]$, also known as $z = 0$ (the same as $[0, 0, n]$ for any $n \neq 0$).

$\mathbb{P}_2(\mathbb{K})$: **Points** All $(x, y, z) \neq (0, 0, 0)$ (with $(x, y, z) = (\lambda x, \lambda y, \lambda z)$ whenever $\lambda \neq 0$).

Lines All $[l, m, n] \neq [0, 0, 0]$ (with $[l, m, n] = [\lambda l, \lambda m, \lambda n]$ whenever $\lambda \neq 0$).

Definition 2.11. The new line $[0, 0, n]$ is called l_∞ , the **line at infinity**. The points that lie on it, i.e., $(x, y, 0)$ with $(x, y) \neq (0, 0)$, are called the **points at infinity**.

Theorem 2.12. Any two distinct lines in a projective plane meet in exactly one point. (Thus there are no parallel lines in the projective plane.)

Proof. Take two lines in $\mathbb{P}_2(\mathbb{K})$.

(a) Suppose that one line is l_∞ ($z = 0$) and the other is in

\mathbb{E} , say $lx + my + nz = 0$ with $(l, m) \neq (0, 0)$. Either

$l = 0$ and then $m \neq 0$, in which case $my + nz = 0$

and $z = 0$ implies that $y = z = 0$ so that the two

lines have precisely $(1, 0, 0)$ in common; or $l \neq 0$ and

a point on both lines satisfies $x = -my/l$ so that the

two lines have precisely $(-m/l, 1, 0)$ in common; in either case the lines intersect (uniquely) at $(-m, l, 0)$.

(b) Now suppose that $[l_1, m_1, n_1]$ and $[l_2, m_2, n_2]$ are lines of \mathbb{E} that meet in a point on l_∞ . The first line meets l_∞ at $(-m_1, l_1, 0)$ and the second at $(-m_2, l_2, 0)$. These points must be the same so $m_2 = \lambda m_1$ and $l_2 = \lambda l_1$ for some $\lambda \neq 0$. Therefore $l_1 m_2 = l_2 m_1$ and the lines are parallel in \mathbb{E} . This means that they have no points in common in \mathbb{E} and have a unique point in common on l_∞ , i.e., they meet in exactly one point.

(c) It remains to consider two lines that do not meet at a point on l_∞ . These must be non-parallel lines in \mathbb{E} , and so they intersect in a unique point of \mathbb{E} . [Distinct

parallel lines $ax + by + c = 0$ and $Ax + By + C = 0$ of $\mathbb{E}_2(\mathbb{K})$ satisfy $aB = bA$. They correspond to lines $ax + by + cz = 0$ and $Ax + By + CZ = 0$ of $\mathbb{P}_2(\mathbb{K})$ that meet at $(-B, A, 0) = (-b, a, 0)$ on l_∞ .]

□

Fact 2.13. *Suppose that A is a square matrix. If one row of A is a scalar multiple of another or if one column of A is a scalar multiple of another, then $\det A = 0$. This is because subtracting a scalar multiple of one of the rows from another (or a scalar multiple of one of the columns from another) doesn't change the determinant, but leads to a matrix with a row or column of 0s. Switching two rows or switching two columns has the consequence of multiplying the determinant by -1 .*

Theorem 2.14. *Let (x_1, y_1, z_1) and (x_2, y_2, z_2) be distinct points of $\mathbb{P}_2(\mathbb{K})$. Then there is one and only one line which passes through these points. Its equation is*

$$\begin{vmatrix} x & y & z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0.$$

This is the line

$$\left[\begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix}, \begin{vmatrix} z_1 & x_1 \\ z_2 & x_2 \end{vmatrix}, \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \right].$$

Proof. The determinant equation clearly gives a line with

the co-ordinates indicated. If we substitute the co-ordinates

of each point into the determinant, we get 0 by Fact 2.13.

Hence these two points do indeed lie on the given line.

By Theorem 2.12, two lines have only one point in common, so there is not another line passing through both of the given points.

[If we expand the determinant, we get

$$\begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix} x - \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix} y + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} z = 0$$

i.e.,

$$\begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix} x + \begin{vmatrix} z_1 & x_1 \\ z_2 & x_2 \end{vmatrix} y + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} z = 0.$$

We use the fact that swapping two columns of a matrix multiplies the determinant by -1 .] □

Definition 2.15. A set of two or more points are said to be **collinear** if they lie on a common line. A set of two or more lines are said to be **concurrent** if they pass through a common point. Any two distinct points lie on a line, so are collinear. Any two distinct lines meet in a point so are concurrent.

Theorem 2.16. *Suppose that the points $P_1 = (x_1, y_1, z_1)$, $P_2 = (x_2, y_2, z_2)$ and $P_3 = (x_3, y_3, z_3)$ of $\mathbb{P}_2(\mathbb{K})$ are not all the same. They are collinear if and only if*

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0.$$

Proof. If two of the points are the same, then we have just two points and they are collinear. At the same time the given matrix has one row a scalar multiple of another, so the determinant is 0. Suppose now that the points are distinct. Then the line P_2P_3 containing P_2 and P_3 is given by

$$\begin{vmatrix} x & y & z \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0.$$

This is the only line that could possibly contain P_1 , P_2 and P_3 . Therefore P_1, P_2, P_3 are collinear if and only if P_1 lies on P_2P_3 , if and only if

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = 0.$$

□

2.4 Duality

Notice that the points and lines of $\mathbb{P}_2(\mathbb{K})$ resemble each other. Both are composed of triples with at least one nonzero component, and both are unchanged

if we multiply each component by a nonzero number. In fact the lines $[l, m, n]$ of $\mathbb{P}_2(\mathbb{K})$ can be regarded as “points” in another $\mathbb{P}_2(\mathbb{K})$, called the **dual plane**. The “lines” in the dual plane are given by triples $(x, y, z) \neq (0, 0, 0)$ such that $xl + ym + zn = 0$, i.e., by the points in the original plane. We can construct a dictionary to translate concepts from one plane to the other

Original Plane	Dual Plane
Points	Lines
Lines	Points
Two lines intersect in a point	Two points lie on a line
Two points lie on a line	Two lines intersect in a point
Points are collinear	Lines are concurrent
Lines are concurrent	Points are collinear

Principle 2.17 (Principle of Duality). *Suppose we have proved a theorem about $\mathbb{P}_2(\mathbb{K})$, such as Theorem 2.14. Then it is true in the dual plane, since the dual plane is a copy of $\mathbb{P}_2(\mathbb{K})$. But recall that the points [respectively lines] of the dual plane are the lines [respectively points] of the original plane, and so on. We use the above dictionary to translate our theorem into a theorem about the original plane. In this way we get a new theorem, called the **dual** of the first. The Principle of Duality says that if a theorem is*

true then its dual is also true.

Thus we have

Theorem 2.18. *Let $[l_1, m_1, n_1]$ and $[l_2, m_2, n_2]$ be distinct lines of \mathbb{P}_2 . Then there is one and only one point of intersection of these two lines. It is given by the equation*

$$\begin{vmatrix} l & m & n \\ l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \end{vmatrix} = 0.$$

This is the point with coordinates $\left(\begin{vmatrix} m_1 & n_1 \\ m_2 & n_2 \end{vmatrix}, \begin{vmatrix} n_1 & l_1 \\ n_2 & l_2 \end{vmatrix}, \begin{vmatrix} l_1 & m_1 \\ l_2 & m_2 \end{vmatrix} \right)$.

Proof. Apply the Principle of Duality to Theorem 2.14. \square

Example 2.19. Find the line in $\mathbb{P}_2(\mathbb{R})$ through $(1, 1, 1)$ and $(1, 5, 6)$ and the point where this line meets $x + y + z = 0$.

Solution:

The line through the two given points is

$$\begin{vmatrix} x & y & z \\ 1 & 1 & 1 \\ 1 & 5 & 6 \end{vmatrix} = 0,$$

i.e., $x \cdot 1 - y \cdot (5) + z \cdot 4 = 0$, i.e., $x - 5y + 4z = 0$. The

point where this line meets $x + y + z = 0$ is given by

$$\begin{vmatrix} l & m & n \\ 1 & -5 & 4 \\ 1 & 1 & 1 \end{vmatrix} = 0,$$

i.e., $l \cdot (-9) - m \cdot (-3) + n \cdot 6 = 0$, i.e., $-9l + 3m + 6n = 0$.

Thus it is the point $(-9, 3, 6)$, equivalently $(3, -1, -2)$.

We can check that this point lies on both of $x - 5y + 4z = 0$ and $x + y + z = 0$.

Remark 2.20. *The equation*

$$\begin{vmatrix} l & m & n \\ l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \end{vmatrix} = 0$$

calls for comment. In what sense is it the equation of a point? Recall that the equation

$$\begin{vmatrix} x & y & z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0$$

specifies a line by telling us precisely which points (x, y, z) lie on it. In exactly the same way, the above equation specifies a point by telling us precisely which lines $[l, m, n]$ pass through it.

2.5 The Projective Planes $\mathbb{P}_2(\mathbb{K})$

Recall that if p is a prime then \mathbb{Z}_p (also known as $GF(p)$) is the field consisting of the elements

$$0, 1, 2, \dots, p-1$$

with addition and multiplication performed $(\text{mod } p)$. Thus for example, in \mathbb{Z}_{11} ,

$$8 + 7 = 4, 8 \times 7 = 1.$$

We can therefore construct $\mathbb{P}_2(GF(p)) = \mathbb{P}_2(\mathbb{Z}_p)$, which we write simply as $\mathbb{P}_2(p)$.

Lemma 2.21. (a) $\mathbb{P}_2(p)$ has $p^2 + p + 1$ points.

(b) Each line contains $p + 1$ points.

Proof

(a) Since \mathbb{Z}_p has p elements, there are p^3 triples (x, y, z) with $x, y, z \in \mathbb{Z}_p$. But we exclude $(0, 0, 0)$. This

leaves $p^3 - 1$ triples. Also recall that

$$(x, y, z) = (\lambda x, \lambda y, \lambda z)$$

if $\lambda \neq 0$, i.e., if $\lambda = 1, 2, 3, \dots, p - 1$. Thus each point is represented by $p - 1$ triples. Therefore the number of points is

$$\frac{p^3 - 1}{p - 1} = p^2 + p + 1.$$

(b) Let $[l, m, n]$ be a line. Suppose that $l \neq 0$ (the arguments are very similar if $m \neq 0$ or if $n \neq 0$). Then the points (x, y, z) on the line are precisely those satisfying

$$xl + ym + zn = 0.$$

There is a point on the line for each choice of y and z , with x given by $x = -(ym + zn)/l$, except for

$y = z = 0$, and each point on the line can be so expressed (note that $(x, 0, 0)$ cannot lie on the line).

There are p choices for y and p choices for z , so there are $p^2 - 1$ combinations of y and z (excluding $y = z = 0$). Therefore there are $p^2 - 1$ triples (x, y, z) such that $xl + ym + zn = 0$. Each point is represented by $p - 1$ triples. Therefore the number of points on the line is

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

Lemma 2.22.

(a) $\mathbb{P}_2(p)$ has $p^2 + p + 1$ lines.

(b) Each point lies on $p + 1$ lines.

Proof. Dualise Lemma 2.21. This completes the proof, but we prove (b) as an example of the application of the Principle of Duality.

Let (x, y, z) be a point. Suppose that $x \neq 0$ (the arguments are very similar if $y \neq 0$ or if $z \neq 0$). Then the lines $[l, m, n]$ through the point are precisely those satisfying

$$xl + ym + zn = 0.$$

There is a line through the point for each choice of m and n , with l given by $l = -(ym + zn)/x$, except for $m = n = 0$, and each point on the line can be so

expressed (note that $[l, 0, 0]$ cannot pass through the point). There are p choices for m and p choices for n , so there are $p^2 - 1$ combinations of m and n (excluding $m = n = 0$). Therefore there are $p^2 - 1$ triples $[l, m, n]$ such that $xl + ym + zn = 0$. Each line is represented by $p - 1$ triples. Therefore the number of lines through the point is

$$\frac{p^2 - 1}{p - 1} = p + 1.$$

□

Theorem 2.23. Assume that $K = \mathbb{Z}_p$.

(a) If $P = (x_1, y_1, z_1)$ and $Q = (x_2, y_2, z_2)$ are distinct points then the line PQ consists of all points of the form

$$\lambda P + \mu Q = (\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2)$$

with $(\lambda, \mu) \neq (0, 0)$.

(b) The points other than Q are precisely those of the form $P + \lambda Q = (x_1 + \lambda x_2, y_1 + \lambda y_2, z_1 + \lambda z_2)$.

Proof. Since P and Q are distinct, neither of (x_1, y_1, z_1) , (x_2, y_2, z_2) is a scalar multiple of the other. Observe that

$$\begin{vmatrix} x_1 + \lambda x_2 & y_1 + \lambda y_2 & z_1 + \lambda z_2 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix} = 0$$

(first subtracting λ Row 3 from Row 1, then Row 2 from Row 1).

Thus each of the $p + 1$ points $P + \lambda Q$ together with Q lies on the line PQ . Next observe that these points are distinct, for if

$$(x_1 + \lambda x_2, y_1 + \lambda y_2, z_1 + \lambda z_2) = \alpha (x_1 + \mu x_2, y_1 + \mu y_2, z_1 + \mu z_2),$$

then

$$(1 - \alpha)(x_1, y_1, z_1) = (\alpha\mu - \lambda)(x_2, y_2, z_2)$$

which can only happen if $\alpha = 1$ and $\mu = \lambda$. Similarly if

$$(x_1 + \lambda x_2, y_1 + \lambda y_2, z_1 + \lambda z_2) = \alpha(x_2, y_2, z_2),$$

then

$$(x_1, y_1, z_1) = (\alpha - \lambda)(x_2, y_2, z_2)$$

which can't happen at all. Hence the $p + 1$ points on PQ are precisely the points $P + \lambda Q$ together with Q .

Now scalar multiples of $P + \alpha Q$ have the form $\lambda P + \mu Q$. Moreover $\lambda P + \mu Q$ is the same point as $P + (\mu/\lambda)Q$ if $\lambda \neq 0$ and as Q if $\lambda = 0$. Hence PQ consists of all $\lambda P + \mu Q$ (with repetitions).

□

Remark 2.24. *The above theorem is actually true for any field, but the proof is more tricky.*

Example 2.25. In $\mathbb{P}_2(11)$, find the coordinates of the point of intersection of the line p passing through $(1, 1, 0)$ and $(2, 1, 2)$, and the line q passing through $(0, 1, 1)$ and $(2, 1, 5)$.

Solution

By Theorem 2.14, p has equation

$$\begin{vmatrix} x & y & z \\ 1 & 1 & 0 \\ 2 & 1 & 2 \end{vmatrix} = 0,$$

i.e.,

$$2x - 2y - z = 0.$$

Similarly, q has equation

$$\begin{vmatrix} x & y & z \\ 0 & 1 & 1 \\ 2 & 1 & 5 \end{vmatrix} = 0,$$

i.e.,

$$4x + 2y - 2z = 0,$$

i.e., $2x + y - z = 0$. By Theorem 2.18, p and q intersect

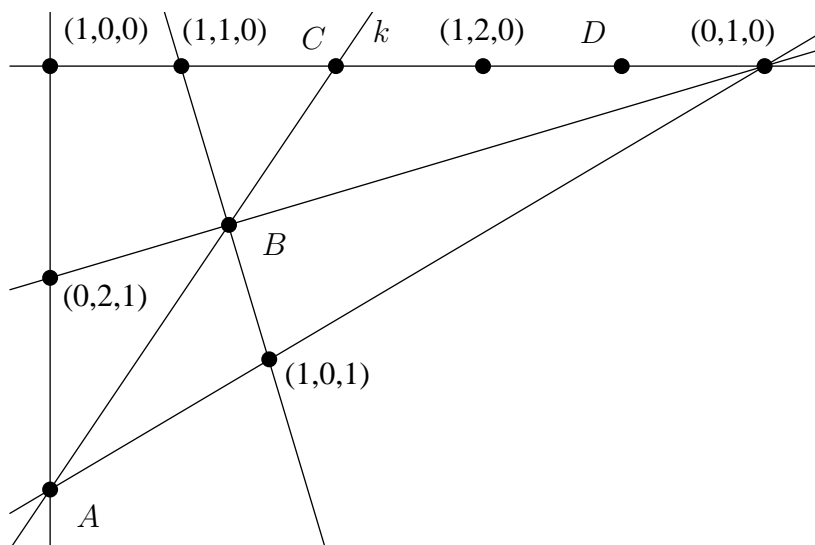
at the point

$$\left(\begin{array}{c|c|c} \left| \begin{array}{cc} -2 & -1 \\ 1 & -1 \end{array} \right|, & \left| \begin{array}{cc} -1 & 2 \\ -1 & 2 \end{array} \right|, & \left| \begin{array}{cc} 2 & -2 \\ 2 & 1 \end{array} \right| \end{array} \right) = (3, 0, 6) = (1, 0, 2).$$

Example 2.26. Identify the lines of the Fano Plane having equations.

- A: $z = 0$
- B: $y + z = 0$
- C: $y = 0$
- D: $x + z = 0$
- E: $x = 0$
- F: $x + y = 0$
- G: $x + y + z = 0$.

Example 2.27. Identify the marked points and line in $\mathbb{P}_2(5)$ in the following diagram.



Solution.

A lies on $y = 2z$ and $x = z$ so $A = (1, 2, 1)$.

B lies on $x - y - z = 0$ and $x = 0$ so $B = (0, 1, -1)$.

k is the line $\begin{vmatrix} x & y & z \\ 0 & 1 & -1 \\ 1 & 2 & 1 \end{vmatrix} = 0$, i.e. $3x - y - z = 0$.

C lies on $3x - y - z = 0$ and $z = 0$ so $C = (1, 3, 0)$.

D must be $(1, 4, 0)$.

Theorem 2.28. *The points of $\mathbb{P}_2(p)$, with lines as blocks, form a $2 - (p^2 + p + 1, p + 1, 1)$ design.*

Proof

There are $p^2 + p + 1$ points (by Lemma 2.21), so $v = p^2 + p + 1$. Each line has $p + 1$ points (Lemma 2.21) so $k = p + 1$. Any two points lie on precisely one line (Theorem 2.14), so $\lambda = 1$.

Examples 2.29. (a) Take $p = 2$. Then we get a $2 - (7, 3, 1)$ design.

(b) Take $p = 3$. Then we get a $2 - (13, 4, 1)$ design.

(c) Take $p = 5$. Then we get a $2 - (31, 6, 1)$ design.

(d) Take $p = 7$. Then we get a $2 - (57, 8, 1)$ design.

Theorem 2.30. *If p is a prime then a $2 - (p^2, p, 1)$ design exists.*

Proof. (We “remove a line at infinity”). Select a particular line L of $\mathbb{P}_2(p)$, and let

$$X = \mathbb{P}_2(p) \setminus L.$$

Then $|X| = (p^2 + p + 1) - (p + 1) = p^2$.

Let the blocks consist of all points of X which lie on a line L' other than L :

$$\mathcal{B} = \{L' \cap X : L' \neq L\}.$$

Since L' meets L in one point (which is omitted from X) the block $L' \cap X$ has $(p + 1) - 1 = p$ points.

Finally, any two points of X determine a unique line L' of $\mathbb{P}_2(p)$ which is different from L . They therefore lie in a unique block. Thus (X, \mathcal{B}) is a $2 - (p^2, p, 1)$ design.

□

Example 2.31. It follows that there exist $2 - (4, 2, 1)$, $2 - (9, 3, 1)$, $2 - (25, 5, 1)$ and $2 - (49, 7, 1)$ designs.

Example 2.32. In a projective plane, a **triangle** is a set of three non-collinear points, and a **quadrangle** is a set of four points, no three of which are collinear. How many triangles does $\mathbb{P}_2(2)$ contain? How many quadrangles does it contain?

Solution

Recall that each line of $\mathbb{P}_2(2)$ contains 3 points. To construct a triangle PQR in $\mathbb{P}_2(2)$,

1. there are 7 choices for P ;
2. this leaves 6 choices for Q ;
3. this leaves 4 choices for R (we cannot choose the third point on PQ),

making $7 \times 6 \times 4 = 168$ choices in all. But PQR can be ordered in $3! = 6$ ways, so every triangle is represented by 6 choices of triples. Therefore the number of triangles

is

$$\frac{168}{6} = 28.$$

To construct a quadrangle $PQRS$ in $\mathbb{P}_2(2)$,

1. there are 7 choices for P ;
2. this leaves 6 choices for Q ;
3. this leaves 4 choices for R (we cannot choose the third point on PQ);
4. this leaves 1 choice for S (we cannot choose the third points on PQ , QR , and RP).

making $7 \times 6 \times 4 \times 1 = 168$ choices in all. But $PQRS$ can be ordered in $4! = 24$ ways, so every quadrangle is represented by 24 choices of quadruples. Therefore the

number of quadrangles is

$$\frac{168}{24} = 7.$$

Example 2.33. How many points in total lie on the three sides of a triangle in $\mathbb{P}_2(p)$?

Solution

If A, B, C are the ‘vertices’ of the triangle, then we can count the points by first excluding A, B, C : we get $3 \times (p - 1) = 3p - 3$; and then including A, B, C to get 3 more, and thus $3p$ in total.

Definition 2.34. The set of lines passing through a point V is called the **pencil of lines** with vertex V .

Theorem 2.35. (a) If $[l_1, m_1, n_1]$ and $[l_2, m_2, n_2]$ are distinct lines then the lines concurrent with them are precisely those of the form

$$[\lambda l_1 + \mu l_2, \lambda m_1 + \mu m_2, \lambda n_1 + \mu n_2]$$

with $(\lambda, \mu) \neq (0, 0)$.

(b) The lines in this set other than $[l_2, m_2, n_2]$ are precisely those of the form

$$[l_1 + \lambda l_2, m_1 + \lambda m_2, n_1 + \lambda n_2]$$

Proof. Dualise Theorem 2.23. \square

Example 2.36. In $\mathbb{P}_2(\mathbb{R})$, the lines $3x - 7y + 15z = 0$ and $45x + 51y - 37z = 0$ meet at a point A . Find the equation of the line joining A to the point $B = (1, 2, 3)$.

Solution

The lines through A have co-ordinates $[3, -7, 15]$ and $[45 + 3\lambda, 51 - 7\lambda, -37 + 15\lambda]$, so we need only find the value of λ for which the line passes through $(1, 2, 3)$.

$$(45 + 3\lambda)x + (51 - 7\lambda)y + (-37 + 15\lambda)z = 0$$

passes through $(1, 2, 3)$ when

$$(45 + 3\lambda) + (51 - 7\lambda)2 + (-37 + 15\lambda)3 = 0$$

i.e., $36 + 34\lambda = 0$, i.e., $\lambda = -18/17$. Thus the line is

$$(711/17)x + (993/17)y - (899/17)z = 0$$

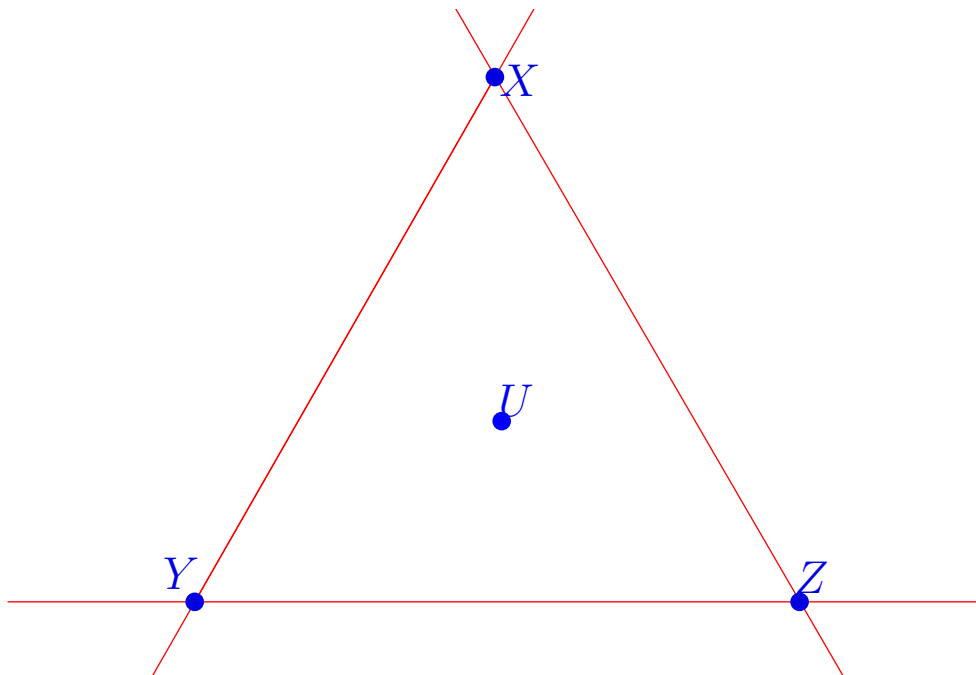
i.e.,

$$711x + 993y - 899z = 0.$$

2.6 The Triangle of Reference and the Unit Point

Definition 2.37. In $\mathbb{P}_2(\mathbb{K})$, the triangle with vertices $X = (1, 0, 0)$, $Y = (0, 1, 0)$ and $Z = (0, 0, 1)$ is called the **triangle of reference**. Its sides are the lines $x = 0$, $y = 0$, $z = 0$.

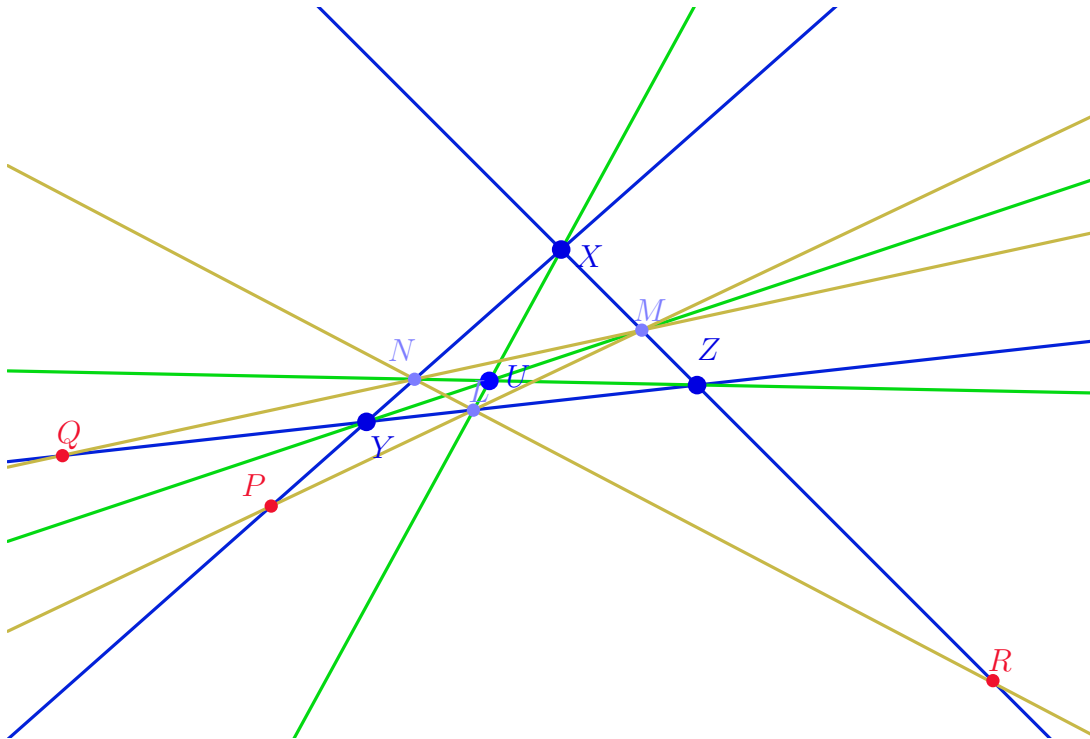
The point $U = (1, 1, 1)$ is called the **unit point**. Note that the unit point does NOT lie on any side of the Δ of reference. A **quadrangle** is a set of four points, no three of which are collinear. Thus the vertices of the triangle of reference and the unit point form a quadrangle.



Theorem 2.38. In any projective plane, given a quadrangle A, B, C, D , a coordinate system may be chosen so that $A = (1, 0, 0)$, $B = (0, 1, 0)$, $C = (0, 0, 1)$ and $D = (1, 1, 1)$.

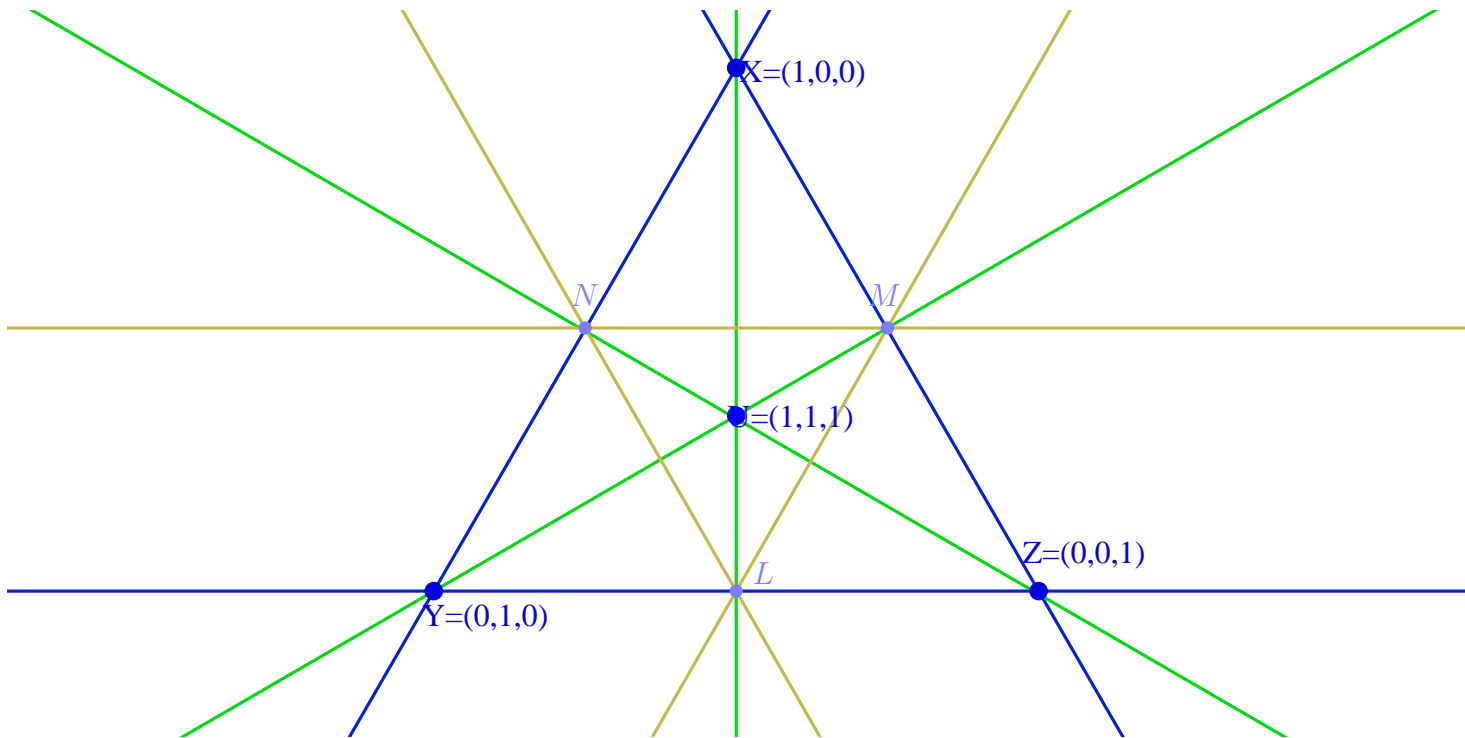
Proof. Not given. □

Example 2.39. Suppose we are given a triangle ΔXYZ , with points L on YZ , M on XZ and N on XY , such that the lines XL , YM and NZ intersect in the point U not on a side of ΔXYZ . Let the lines XY and ML intersect at P , the lines YZ and MN intersect at Q , and the lines ZX and LN intersect at R . Show that the points P , Q and R are collinear.



Solution We start by choosing coordinates so that ΔXYZ is the triangle of reference and U is the unit point. Thus

$$X = (1, 0, 0), Y = (0, 1, 0), Z = (0, 0, 1), U = (1, 1, 1).$$



We shall find coordinates of

- (i) Line XU .
- (ii) Point L .
- (iii) Points M and N .
- (iv) Line LM .
- (v) Point P .
- (vi) Points Q, R .

(i) **Either:** by inspection both X and U satisfy $y = z$ and

so this is the line XU . Or: XU has equation

$$\begin{vmatrix} x & y & z \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 0$$

i.e., $y - z = 0$, equivalently $y = z$.

(ii) L is the point of intersection of XU and YZ , i.e., of

$y = z$ and $x = 0$. Therefore $L = (0, 1, 1)$.

(iii) **Key Idea:** Exploit the symmetry of the situation. Use the map σ of $\mathbb{P}_2(\mathbb{K})$ to itself given by $(x, y, z) \mapsto (z, x, y)$. Note that if point (x, y, z) lies on line $[l, m, n]$ then $\sigma(x, y, z) = (z, x, y)$ lies on $[n, l, m] = \sigma[l, m, n]$ (where the second σ is applied to the dual plane). Thus σ , which is clearly a bijection, maps lines to lines.

Depict σ schematically by a directed circle labelled

$x \longrightarrow y \longrightarrow z \longrightarrow x$.

Under σ : $X \longrightarrow Y \longrightarrow Z \longrightarrow X$ and U is fixed.

Therefore $L \longrightarrow M \longrightarrow N \longrightarrow L$ and so $M =$

$(0, 1, 1)$ and $N = (1, 1, 0)$.

(iv) LM has equation

$$\begin{vmatrix} x & y & z \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 0$$

i.e., $x + y - z = 0$.

(v) P is the intersection point of LM and XY , that is, of

$x + y - z = 0$ and $z = 0$. Thus $P = (1, -1, 0)$.

(vi) P is on $z = 0$ and LM ,
 Q is on $x = 0$ and MN , and
 R is on $y = 0$ and NL ,
 so under $\sigma: P \rightarrow Q \rightarrow R \rightarrow P$. Thus $Q = (0, 1, -1)$ and $R = (-1, 0, 1)$.

Since P, Q and R all lie on the line $x + y + z = 0$, they
 are collinear.

Example 2.40. Let $\triangle ABC$ be any triangle, and let D be any point which is not on a side of this triangle. Let the lines AD, BD, CD meet the lines BC, CA, AB in E, F, G , respectively. Let H be any point not on a side of $\triangle EFG$. Let the lines EH, FH, GH meet the lines FG, GE, EF in the points I, J, K , respectively. Show that the lines AI, BJ, CK are concurrent.

Solution Choose coordinates so that $\triangle ABC$ is the triangle of reference, and D is the unit point: $A = (1, 0, 0), B = (0, 1, 0), C = (0, 0, 1), D = (1, 1, 1)$.

E : The line AD has equation:

$$y = z.$$

The line BC has equation:

$$x = 0.$$

Their point of intersection is $E =$

$$(0, 1, 1).$$

F : Similarly $F =$

$$(1, 0, 1).$$

G : Similarly $G = (1, 1, 0)$.

FG : By inspection, FG has equation

$$y + z = x, \text{ i.e. } x - y - z = 0.$$

Let $H = (p, q, r)$. Since H does not lie on any side of $\triangle EFG$ $p + q - r \neq 0$, $q + r - p \neq 0$ and $r + p - q \neq 0$.

EH : The line EH has equation

$$\begin{vmatrix} x & y & z \\ 0 & 1 & 1 \\ p & q & r \end{vmatrix} = 0$$

i.e., $(r - q)x + py - pz = 0$.

AI: The lines $EH : (q - r)x - py + pz = 0$ and $FG : x - y - z = 0$ meet at I , so from Theorem 2.35 lines through I have form

$$\lambda(x - y - z) + \mu((r - q)x + py - pz) = 0,$$

(where $(\lambda, \mu) \neq (0, 0)$).

$A = (1, 0, 0)$ lies on such a line where $\lambda + \mu(r - q) = 0$, so $\mu \neq 0$ and we may set $\mu = 1$ and then $\lambda = q - r$.

Therefore *AI* is the line

$$(q - r)(x - y - z) + (r - q)x + py - pz = 0,$$

that is

$$(p - q + r)y - (p + q - r)z = 0 \text{ or } (p - q + r)y + (r - p - q)z = 0.$$

BJ and *CK* Under σ : $x \longrightarrow y \longrightarrow z \longrightarrow x$ and $p \longrightarrow q \longrightarrow$

$r \longrightarrow p$,

so $AI \longrightarrow BJ \longrightarrow CK \longrightarrow AI$

thus BJ is the line $(q - r + p)z + (p - q - r)x = 0$

and

CK is the line $(r - p + q)x + (q - r - p)y = 0$.

[Recall that three lines $[l_i, m_i, n_i]$ ($i = 1, 2, 3$) are concurrent if and only if

$$\begin{vmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \\ l_3 & m_3 & n_3 \end{vmatrix} = 0.]$$

In this case the determinant takes the form

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

Now calculate this determinant:

Add Row 2 and then Row 3 to Row 1: we get a row of 0s, so the determinant is 0.

Note: we could have shown that the intersection of the first two lines lies on the third.

2.7 Desargues' Theorem

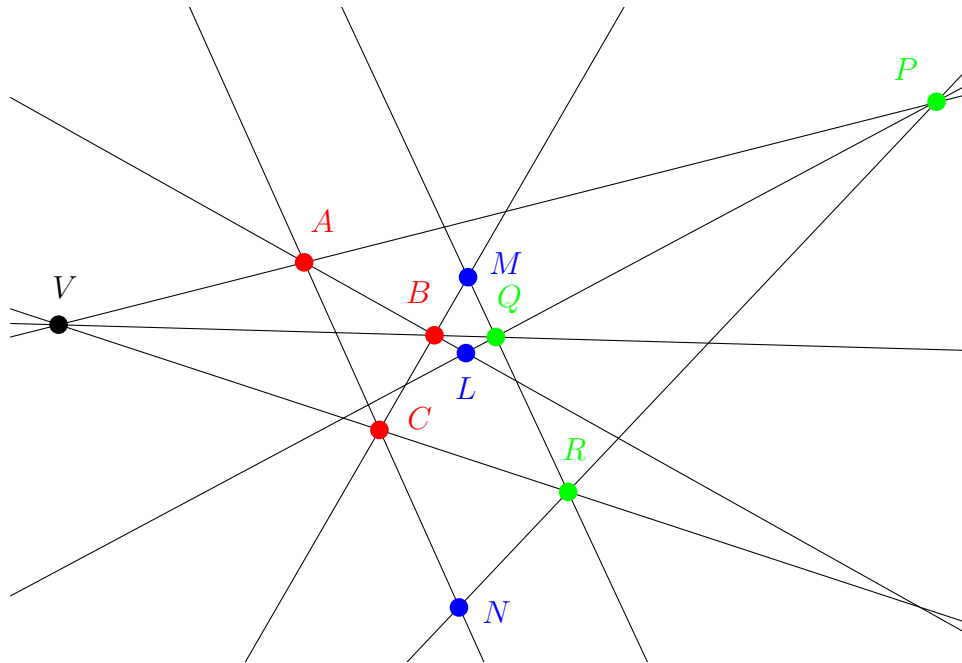
Definition 2.41. Two triangles $\triangle ABC$ and $\triangle PQR$ are said to be **in perspective from the point** V if the lines AP , BQ and CR are concurrent at V .

In this definition it is assumed that the points A, B, C, D, P, Q, R are distinct and that the lines AP, BQ, CR are distinct.

Theorem 2.42 (Desargues). *If the triangles $\triangle ABC$ and $\triangle PQR$ are in perspective from the point V then the points of intersection of corresponding sides:*

(i) AB, PQ , (ii) BC, QR ; (iii) CA, RP

are collinear.



Proof. Choose coordinates so that $\triangle ABC$ is the triangle of reference and V is the unit point. Thus $A = (1, 0, 0)$, $B = (0, 1, 0)$, $C = (0, 0, 1)$, $V = (1, 1, 1)$.

P lies on VA and is distinct from V, A so it is a linear combination of $(1, 1, 1)$ and $(1, 0, 0)$. It follows that $P = (\alpha, 1, 1)$ for some $\alpha \neq 1$.

Q lies on VB and is distinct from V, B so it is a linear combination of $(1, 1, 1)$ and $(0, 1, 0)$. It follows that $Q = (1, \beta, 1)$ for some $\beta \neq 1$.

R lies on VC and is distinct from V, C so it is a linear combination of $(1, 1, 1)$ and $(0, 0, 1)$. It follows that $R = (1, 1, \gamma)$ for some $\gamma \neq 1$.

L: AB is the line $z = 0$, so we need a linear combination of $(\alpha, 1, 1)$ and $(1, \beta, 1)$ lying on $z = 0$: this can only be $(\alpha, 1, 1) - (1, \beta, 1) = (\alpha - 1, 1 - \beta, 0)$ so $L = (\alpha - 1, 1 - \beta, 0)$.

M: BC is the line $x = 0$, so we need a linear combination of $(1, \beta, 1)$ and $(1, 1, \gamma)$ lying on $x = 0$: this can only be $(1, \beta, 1) - (1, 1, \gamma) = (0, \beta - 1, 1 - \gamma)$ so $M = (0, \beta - 1, 1 - \gamma)$.

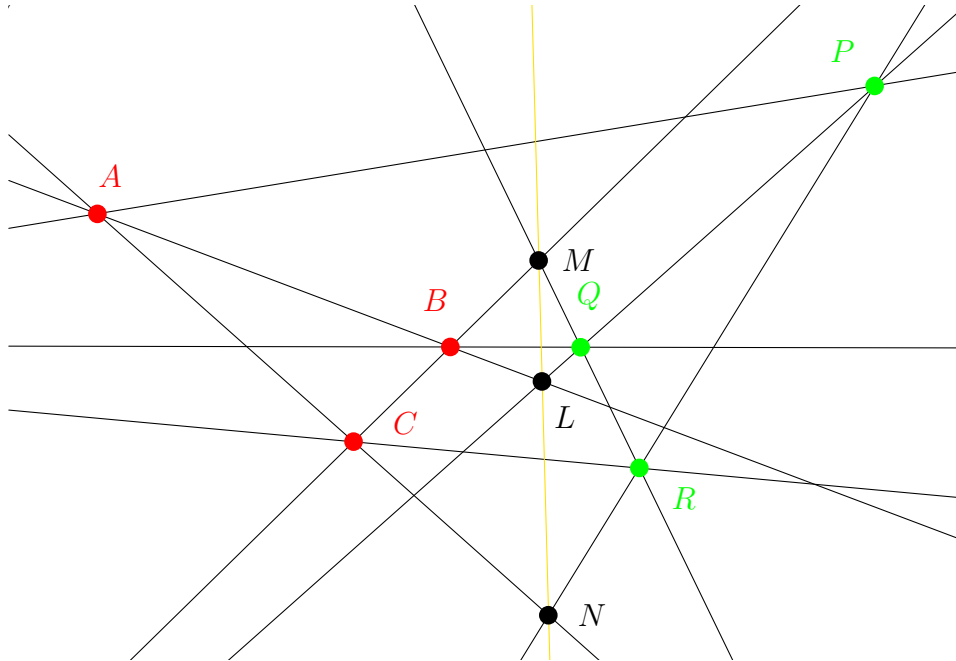
N: AC is the line $y = 0$, so we need a linear combination of $(\alpha, 1, 1)$ and $(1, 1, \gamma)$ lying on $y = 0$: this can only be $(\alpha, 1, 1) - (1, 1, \gamma) = (\alpha - 1, 0, 1 - \gamma)$ so $N = (\alpha - 1, 0, 1 - \gamma)$.

To show that L, M, N are collinear, it suffices to show that one of the points is a linear combination of the others. We can clearly see that $N = M + L$. so indeed the three points are collinear. □

Theorem 2.43 (Converse of Desargues). *If the triangles $\triangle ABC$ and $\triangle PQR$ are such that intersection of corresponding sides:*

(i) AB, PQ , (ii) BC, QR ; (iii) CA, RP

are collinear, then the triangles are in perspective from a point.



Proof. We dualise Desargues' Theorem.

Desargues' Theorem says that, given two triangles $\triangle PQR$ and $\triangle ABC$, if the lines joining corresponding vertices, i.e.,

$$(i) AP \quad (ii) BQ \quad (iii) CR$$

are concurrent then the points of intersection of corresponding sides

$$AB, PQ \text{ and } BC, QR \text{ and } CA, RP$$

are collinear.

Since Desargues' Theorem is true, the same must be the case for its dual.

To begin with, let us consider the dual of a triangle. A triangle is defined as a set of three non-collinear points. Thus when we have a triangle XYZ , the lines XY, XZ, YZ are distinct non-concurrent lines. The dual of a triangle is a set of three non-concurrent lines. We call such an object a trilateral. When we have a trilateral abc we can construct the points of intersection $C = a \wedge b$, $A = b \wedge c$ and $B = a \wedge c$ and ABC is a triangle. [Notice that we write $a \wedge b$ for the point of intersection of the lines a and b .]

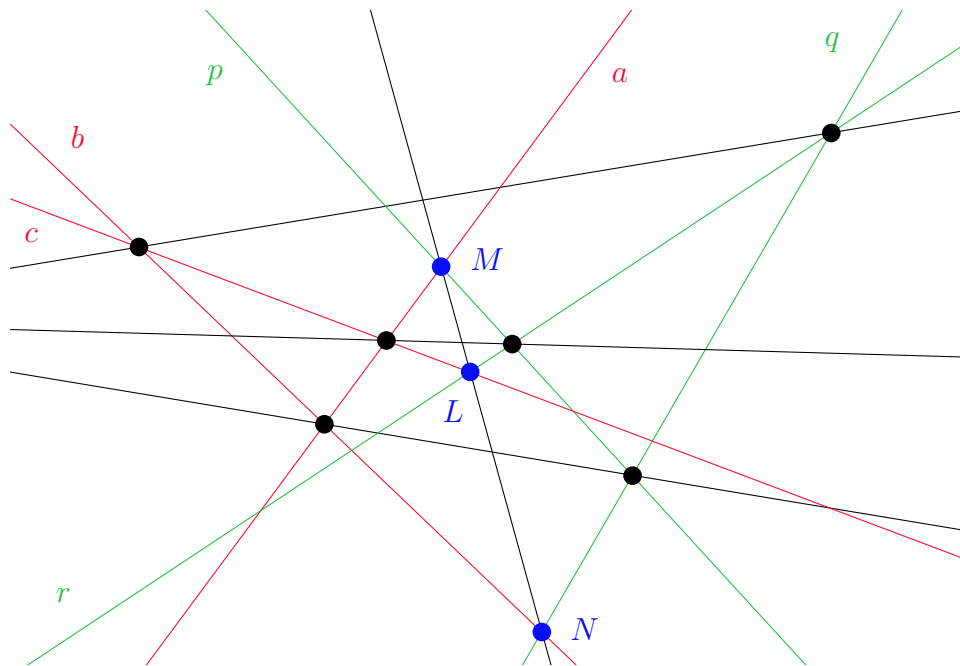
The dual of Desargues' Theorem says that, given two trilaterals pqr and abc , if the points of intersection of corresponding sides, i.e.,

$$(i) a \wedge p \quad (ii) b \wedge q \quad (iii) c \wedge r$$

are collinear then the lines joining of corresponding points

$$a \wedge b, p \wedge q \text{ and } b \wedge c, q \wedge r \text{ and } c \wedge a, r \wedge p$$

are concurrent.



Let us write $C = a \wedge b$, $A = b \wedge c$, $B = a \wedge c$, $R = p \wedge q$,

$P = q \wedge r$ and $Q = p \wedge r$. Further let us write $L = c \wedge r$,

$M = a \wedge p$ and $N = b \wedge q$. If we mark these points on the

diagram above, we find that we have precisely the dia-

gram for the converse of Desargues' Theorem. Further

$$a = BC, b = AC, c = AB, p = QR, q = PR, r = PQ.$$

We can then rewrite the dual of Desargues' Theorem as:

Given two trilaterals pqr and abc , with corresponding triangles PQR and ABC , if the points of intersection of corresponding sides, i.e., the points of intersection of

(i) AB and PQ (ii) BC and QR (iii) CA and RP

are collinear, then the lines joining points of intersection of

(i) AB, BC and PQ, QR (ii) BC, CA and QR, RP

(iii) CA, AB and RP, PQ

i.e., the lines

(i) BQ (ii) CR (iii) AP

are concurrent.

Hence the dual of Desargues' Theorem is simply its converse.

□

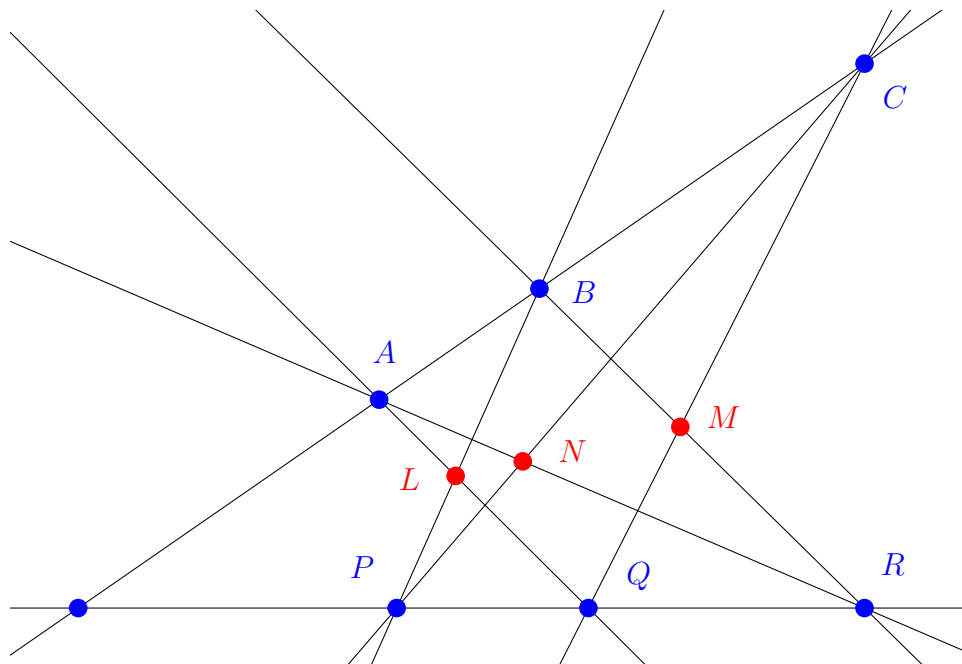
2.8 Pappus' Theorem

Theorem 2.44 (Pappus). *Let the distinct points A, B, C lie on a line l , and let the distinct points P, Q, R lie on a line m (but not on l). Let*

(i) AQ, BP meet at L , (ii) BR, CQ meet at M , (iii) CP, AR meet at N .

Then the points L, M, N are collinear.

Proof 1. The points A, B, C are distinct. We assume that A, B are not on m .



We take A, B, P, Q to be the triangle of reference and the unit point, so

$$A = (1, 0, 0), B = (0, 1, 0), P = (0, 0, 1), Q = (1, 1, 1).$$

The point C lies on AB so is a linear combination of $(1, 0, 0)$ and $(0, 1, 0)$, and is distinct from A, B , so $C = (1, \alpha, 0)$ for some $\alpha \neq 0$.

The point R lies on PQ so is a linear combination of $(0, 0, 1)$ and $(1, 1, 1)$, and is distinct from P, Q , so $R = (1, 1, \beta)$ for some $\beta \neq 1$.

L: AQ is the line $y = z$, BP is the line $x = 0$. The intersection of these lines is $L = (0, 1, 1)$.

M: BR is the line $z = \beta x$, CQ is the line $\alpha x - y + (1 - \alpha)z = 0$. Thus at the intersection $y = \alpha x + (1 -$

$\alpha)z = \alpha x + (1 - \alpha)\beta x = (\alpha + \beta - \alpha\beta)x$. Hence the intersection is $(x, (\alpha + \beta - \alpha\beta)x, \beta x)$. Taking a scalar multiple, $M = (1, (\alpha + \beta - \alpha\beta), \beta)$.

N: AR is the line $z = \beta y$, CP is the line $y = \alpha x$. The intersection of these lines is $N = (1, \alpha, \beta\alpha)$.

To show that L, M, N are collinear, it suffices to show that one is a linear combination of the other two. The only linear combination of M, N that could give L is

$$M - N = (1, (\alpha + \beta - \alpha\beta), \beta) - (1, \alpha, \beta\alpha) = (0, \beta - \alpha\beta, \beta - \beta\alpha).$$

If $\beta - \beta\alpha \neq 0$, then we see that $M - N$ is the point $(0, 1, 1)$ (i.e., L). If $\beta - \beta\alpha = 0$, then $M = N$. In either case L, M, N are collinear.

Alternatives:

- For the line CQ we could calculate

$$\begin{vmatrix} x & y & z \\ 1 & \alpha & 0 \\ 1 & 1 & 1 \end{vmatrix} = 0,$$

i.e., $x.\alpha - y.1 + z.(1 - \alpha) = 0$.

- To show that L, M, N are collinear we could calculate

$$\begin{vmatrix} 0 & 1 & 1 \\ 1 & (\alpha + \beta - \alpha\beta) & \beta \\ 1 & \alpha & \beta\alpha \end{vmatrix} \\ = ((\alpha + \beta - \alpha\beta).\alpha\beta - \alpha.\beta) - 1.(\beta\alpha - \beta) + 1.(\alpha - (\alpha + \beta - \alpha\beta)) = 0.$$

□

Proof 2. Let the lines l and m meet at D . Choose coordinates so that $\triangle CDR$ is the triangle of reference and M is the unit point. Thus

$$C = (1, 0, 0), R = (0, 1, 0), D = (0, 0, 1), M = (1, 1, 1).$$

DC is the line $y = 0$ and MR is the line $x = z$. They meet at B , whose coordinates are therefore $(1, 0, 1)$.

DR is the line $x = 0$ and MC is the line $y = z$. They meet at Q , whose coordinates are therefore $(0, 1, 1)$.

A lies on DC so has coordinates of the form $(1, 0, a)$.

P lies on DR so has coordinates of the form $(0, 1, p)$.

CP has equation

$$\begin{vmatrix} x & y & z \\ 1 & 0 & 0 \\ 0 & 1 & p \end{vmatrix} = 0$$

i.e., $py - z = 0$.

AR has equation

$$\begin{vmatrix} x & y & z \\ 0 & 1 & 0 \\ 1 & 0 & a \end{vmatrix} = 0$$

i.e., $-ax + z = 0$.

CP and AR meet at $N = (1/a, 1/p, 1) = (p, a, ap)$.

BP has equation

$$\begin{vmatrix} x & y & z \\ 1 & 0 & 1 \\ 0 & 1 & p \end{vmatrix} = 0$$

i.e., $-x - py + z = 0$, or $z = x + py$.

AQ has equation

$$\begin{vmatrix} x & y & z \\ 0 & 1 & 1 \\ 1 & 0 & a \end{vmatrix} = 0$$

i.e., $-ax - y + z = 0$, or $z = ax + y$.

BP and AQ meet at L , where $x + py = ax + y$, or $(1 - a)x = (1 - p)y$. Set $x = 1 - p$. Then $y = 1 - a$ and $z = ax + y = a - ap + 1 - a = 1 - ap$. Therefore $L = (1 - p, 1 - a, 1 - ap)$.

Now L, M, N will be collinear if and only if

$$\begin{vmatrix} 1 - p & 1 - a & 1 - ap \\ 1 & 1 & 1 \\ p & a & ap \end{vmatrix} = 0.$$

But if we first subtract Row 2 from Row 1 and then add Row 3 to Row 1, we get a top row consisting entirely of zeros. Therefore the determinant has value 0, and so L, M, N are collinear. \square

3 Conics

We shall assume that the underlying field is \mathbb{C} or \mathbb{Z}_p with $p \neq 2$. Conics over \mathbb{R} or \mathbb{Z}_2 need special treatment: for example, they may have no points. Also, excluding $p = 2$ means that we can divide by 2 whenever we wish.

3.1 Introduction

Conic sections were first identified by the ancient Greeks, who made an extensive study of them. The Greeks defined them as the curves you get when you section (slice through) a double sided cone. We shall define them algebraically. A **conic** in \mathbb{E} (over \mathbb{R}) is given by an equation of the form

$$ax^2 + by^2 + 2fxy + 2gx + 2hx + c = 0,$$

where at least one of $a, b, f \neq 0$.

Examples 3.1. (a) Circle:

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

(b) Parabola:

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

(c) Ellipse:

$$ax^2 + by^2 - c = 0.$$

(d) Hyperbola:

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

(e) A Single Point:

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

(f) Two intersecting lines:

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

(g) Two identical lines:

$$x^2 = 0.$$

(h) Empty set:

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

3.2 Conics in $\mathbb{P}_2(\mathbb{K})$

Definition 3.2. A conic in $\mathbb{P}_2(\mathbb{K})$ is given by an equation of the form

$$\phi(x, y, z) = ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = 0,$$

where at least one of $a, b, c, f, g, h \neq 0$. This means that the conic is the set of points (x, y, z) satisfying $\phi(x, y, z) = 0$.

Remark 3.3. *If we allowed $\mathbb{K} = \mathbb{R}$ then we could have a conic with no points. Consider, for example, the conic*

with equation $x^2 + y^2 + z^2 = 0$. In \mathbb{R} , the equation $x^2 + y^2 + z^2 = 0$ has a unique solution $x = y = z = 0$, giving $(x, y, z) = (0, 0, 0)$, and there is no such point in $\mathbb{P}_2(\mathbb{K})$. But if $\mathbb{K} = \mathbb{C}$ or \mathbb{Z}_p ($p > 2$) then all conics have points, indeed they all have more than one point. The proof of this is easy for \mathbb{C} but involves a detour into number theory for \mathbb{Z}_p ($p > 2$). So we shall simply assume from now on that every conic has at least two points.

Let us emphasise:

- We shall assume that $\mathbb{K} = \mathbb{C}$ or \mathbb{Z}_p where $p > 2$. We shall assume that every conic has at least two points.

3.3 Singular and Nonsingular Conics

Proposition 3.4. Let M denote the matrix

$$\begin{pmatrix} a & f & h \\ f & b & g \\ h & g & c \end{pmatrix}.$$

Then the equation of the conic can be recast in matrix form as $XM X^T = 0$, where $X = (x, y, z)$.

Proof.

$$XMX^T = \begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} a & f & h \\ f & b & g \\ h & g & c \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = [ax^2 + by^2 + cz^2 + 2fxy -$$

□

We call M the matrix of the conic. Note that it is symmetric: $M^T = M$.

Remark 3.5. *Given any two points X and Y , we can calculate XY^T . It might or might not be 0, but notice that XY^T is a number (i.e., a 1×1 matrix), so*

$$XY^T = (XY^T)^T = (Y^T)^T M^T X^T = YMX^T.$$

Definition 3.6. A conic is **singular** if its equation factors into a product of linear expressions:

$$ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z),$$

so the conic is in fact a pair of lines (which could be the same!). All other conics are **non-singular**. Note: the terms **degenerate** and **non-degenerate** are sometimes used in place of singular and non-singular.

Theorem 3.7. *A conic is singular if and only if it contains three collinear points.*

Proof. We have just seen that a singular conic consists of a pair of lines, and any line has at least three points (this

follows from Theorem 2.23); so a singular conic must contain three collinear points. For the converse, suppose that the conic \mathcal{C} contains three collinear points. Let us choose a triangle of reference so that $(1, 0, 0)$ and $(0, 1, 0)$ lie on this line and $(0, 0, 1)$ is any point not on this line. The third point of \mathcal{C} on this line has co-ordinates $(1, \lambda, 0)$ for some $0 \neq \lambda \in \mathbb{K}$. Let the equation of \mathcal{C} be

$$\phi(x, y, z) = ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = 0.$$

- Since $(1, 0, 0)$ lies on the conic, $0 = \phi(1, 0, 0) = a$.
- Since $(0, 1, 0)$ lies on the conic, $0 = \phi(0, 1, 0) = b$.
- Since $(1, \lambda, 0)$ lies on the conic, $0 = \phi(1, \lambda, 0) = a + \lambda^2 b + 2f\lambda$. This implies that $f = 0$.

The equation of the conic is now

$$\phi(x, y, z) = cz^2 + 2gyz + 2hzx = 0,$$

i.e., $z(cz + 2gy + 2hx) = 0$. This is the product of two linear factors. Therefore the conic is singular. \square

Definition 3.8. Recall that a square matrix is **singular** if and only if it is not invertible, i.e., if and only if its determinant is 0.

Theorem 3.9. A conic is singular if and only if its matrix is singular.

Proof. We don't prove this. \square

Remark 3.10. The matrix of a conic depends on the co-ordinate system chosen. However if the conic is non-singular, then the matrix is always non-singular.

Theorem 3.11. Suppose that \mathcal{C} is a non-singular conic, with matrix M . Let P be any point of $\mathbb{P}_2(\mathbb{K})$. Then the points X that satisfy $XM P^T = 0$ are all the points of a line. Conversely any line of $\mathbb{P}_2(\mathbb{K})$ can be described in this way.

Proof. Given P , observe that $M P^T \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. This is because M^{-1} exists and if $M P^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, then $P^T = M^{-1} M P^T = M^{-1} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Therefore $M P^T =$

$\begin{pmatrix} l \\ m \\ n \end{pmatrix}$ for some l, m, n not all 0. Thus the points $X = (x, y, z)$ that satisfy $XM P^T = 0$ are precisely the points satisfying $(x, y, z) \begin{pmatrix} l \\ m \\ n \end{pmatrix} = 0$, i.e., the points satisfying $lx + my + nz = 0$, i.e., the points of a line.

Conversely, suppose that we are given a line $lx + my + nz = 0$. Let P be the point (x_1, x_2, x_3) given by $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = M^{-1} \begin{pmatrix} l \\ m \\ n \end{pmatrix}$. Then $M P^T = \begin{pmatrix} l \\ m \\ n \end{pmatrix}$ (which shows that $P \neq (0, 0, 0)$) and the line given by $XM P^T = 0$ is precisely $lx + my + nz = 0$. Hence every line has this form. \square

Theorem 3.12. *If C is a non-singular conic with matrix M and if P, Q are distinct points of $\mathbb{P}_2(\mathbb{K})$, then the lines given by $XM P^T = 0$ and $XM Q^T = 0$ are distinct.*

Proof. We can prove this by showing that if the lines are the same, then the points are the same.

The line $XM P^T = 0$ has co-ordinates $[l_1, m_1, n_1]$ where $M P^T = \begin{pmatrix} l_1 \\ m_1 \\ n_1 \end{pmatrix}$. Similarly the line $XM Q^T = 0$ has co-ordinates $[l_2, m_2, n_2]$ where $M Q^T = \begin{pmatrix} l_2 \\ m_2 \\ n_2 \end{pmatrix}$. If $[l_1, m_1, n_1]$ and $[l_2, m_2, n_2]$ are the same line, then $[l_2, m_2, n_2] = \lambda[l_1, m_1, n_1]$ for some $\lambda \neq 0$ and so $M P^T = \lambda M Q^T$. It now follows that $M^{-1} M P^T = \lambda M^{-1} M Q^T$, so $P = \lambda Q$, i.e., P and Q are the same point. □

Definition 3.13. A line which meets a conic in precisely one point P is called a **tangent** to the conic at P .

Theorem 3.14. *There is a unique tangent at each point of a non-singular conic \mathcal{C} . The tangent at a point P of \mathcal{C} is given by $XM P^T = 0$.*

Proof. Let P be a point on \mathcal{C} and let ℓ be a line through P . Then ℓ contains at most two points of \mathcal{C} (by Theorem 3.7), but at least three points of $\mathbb{P}_2(\mathbb{K})$, so there is a point Q on ℓ but not on \mathcal{C} . By Theorem 2.23 and Remark 2.24,

the points on ℓ are precisely P and $Q + \lambda P$ with $\lambda \in \mathbb{K}$.

We know that P lies on \mathcal{C} (so this is one point of ℓ on \mathcal{C}).

The point $Q + \lambda P$ lies on \mathcal{C} precisely when

$$\begin{aligned} 0 &= (Q + \lambda P)M(Q + \lambda P)^T = (Q + \lambda P)M(Q^T + \lambda P^T) \\ &= QMQ^T + \lambda QMP^T + \lambda PMQ^T + \lambda^2 PMP^T = QMQ^T + 2\lambda QMP^T. \end{aligned}$$

We have chosen Q not on \mathcal{C} so $QMQ^T \neq 0$.

The equation $QMQ^T + 2\lambda QMP^T = 0$ has no solution in λ if $QMP^T = 0$ and a single solution $\lambda = -\frac{QMQ^T}{2QMP^T}$ if $QMP^T \neq 0$. Thus ℓ meets \mathcal{C} in one point if $QMP^T \neq 0$ and two otherwise. Therefore ℓ is a tangent precisely when $QMP^T = 0$.

Now $XMP^T = 0$ is a line of $\mathbb{P}_2(\mathbb{K})$. Moreover $PMP^T = 0$ since P is on \mathcal{C} , and therefore P lies on the line $XMP^T =$

0. Hence ℓ is a tangent precisely when Q lies on $XM P^T = 0$, i.e., precisely when ℓ is the line $XM P^T = 0$. □

Example 3.15. Let \mathcal{C} be the conic in $\mathbb{P}_2(\mathbb{C})$ given by

$$x^2 + 4y^2 + 3z^2 - 2xy - 2yz - 12zx = 0.$$

Write down the matrix for \mathcal{C} . Show that \mathcal{C} is non-singular (i.e., non-degenerate) and find the equation of the tangent to \mathcal{C} at the point $(1, 2, 1)$.

Solution.

$$M = \begin{pmatrix} 1 & -1 & -6 \\ -1 & 4 & -1 \\ -6 & -1 & 3 \end{pmatrix} \text{ so } \det M = \begin{vmatrix} 1 & -1 & -6 \\ -1 & 4 & -1 \\ -6 & -1 & 3 \end{vmatrix} \\ = 1 \cdot (11) - (-1) \cdot (-9) + (-6) \cdot 25 = -148.$$

This is non-zero in \mathbb{C} , so M is non-singular and therefore \mathcal{C} is non-singular.

The tangent to $(1, 2, 1)$ is given by $XM(1, 2, 1)^T = 0$,

i.e.,

$$(x, y, z) \begin{pmatrix} 1 & -1 & -6 \\ -1 & 4 & -1 \\ -6 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} = 0.$$

This is

$$(x, y, z) \begin{pmatrix} -7 \\ 6 \\ -5 \end{pmatrix} = 0,$$

i.e., $-7x + 6y - 5z = 0$.

Theorem 3.16. *Let \mathcal{C} be a non-singular conic with matrix M . Let P be a point of $\mathbb{P}_2(\mathbb{K})$ that does not lie on \mathcal{C} . Then:*

- (a) P does not lie on the line $XM P^T = 0$.
- (b) The line $XM P^T = 0$ is not a tangent.
- (c) A point Q of \mathcal{C} lies on the line $XM P^T = 0$ if and only if P lies on the tangent to \mathcal{C} at Q .
- (d) The number of points of the line $XM P^T = 0$ lying on \mathcal{C} is equal to the number of tangents to \mathcal{C} passing through P , and this number is either 0 or 2.
- (e) If $\mathbb{K} = \mathbb{C}$, then P lies on 2 tangents to \mathcal{C} .

Proof. (a) P does not lie on \mathcal{C} , so $PM P^T \neq 0$, which means that P does not lie on the line $XM P^T = 0$.

(b) If the line $XM P^T = 0$ were a tangent, at Q say, then it would have equation $XM Q^T = 0$, with Q necessarily distinct from P (since Q is on \mathcal{C}). But this is not possible, since P and Q are distinct points, and so (by Theorem 3.12), the lines $XM P^T = 0$ and $XM Q^T = 0$ are distinct.

(c) Q lies on the line $XM P^T = 0$ precisely when $QM P^T = 0$, i.e., precisely when $PM Q^T = 0$, i.e., precisely when P lies on the line $XM Q^T = 0$. But this last line is the tangent at Q , so the statement is proved.

(d) **The first part follows from (c), given that distinct points**

of \mathcal{C} have distinct tangents (from Theorem 3.12) and

each tangent meets \mathcal{C} exactly once. Given that $XM P^T =$

0 is not a tangent, it does not meet \mathcal{C} exactly once. We

know that no line of $\mathbb{P}_2(\mathbb{K})$ contains 3 or more points

of \mathcal{C} (by Theorem 3.7), so $XM P^T = 0$ meets \mathcal{C} in 0 or 2 points.

- (e) Let ℓ be the line $XM P^T = 0$, and let Q, R be distinct points on ℓ that do not lie on \mathcal{C} (ℓ has an infinite number of points with at most 2 on \mathcal{C}). A point of ℓ on \mathcal{C} cannot be R so is $Q + \lambda R$ for some $\lambda \in \mathbb{C}$. This means that

$$\begin{aligned} 0 &= (Q + \lambda R)M(Q + \lambda R)^T = (Q + \lambda R)M(Q^T + \lambda R^T) \\ &= QMQ^T + \lambda QMR^T + \lambda RMQ^T + \lambda^2 RMR^T = QMQ^T + 2\lambda QMR^T + \lambda^2 \end{aligned}$$

Thus the points of ℓ on \mathcal{C} (if any) are given by the solutions for λ to the quadratic equation

$$(RMR^T)\lambda^2 + 2(QMR^T)\lambda + QMQ^T = 0.$$

Since $RM R^T \neq 0$, this quadratic equation has at least one solution in \mathbb{C} . Therefore ℓ meets \mathcal{C} in at least one point, and since ℓ is not a tangent it therefore meets \mathcal{C} in 2 points.

□

Example 3.17. Let \mathcal{C} be the (non-singular) conic $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}_2(3)$ and let P be the point $(1, 0, 0)$ of $\mathbb{P}_2(3)$. Show that the line given by $XMP^T = 0$ does not meet \mathcal{C} .

Solution.

The matrix M here is the identity matrix, the line $XMP^T = 0$ is just $x = 0$. It meets \mathcal{C} at (x, y, z) where $x = 0$ and $x^2 + y^2 + z^2 = 0$, so $y^2 + z^2 = 0$. In \mathbb{Z}_3 , the only possibilities for y^2 and z^2 are 0 or 1. The only way to get $y^2 + z^2 = 0$ is $y = z = 0$, but this would give $(0, 0, 0)$ which is not a point in $\mathbb{P}_2(3)$. Hence the line given by $XMP^T = 0$ does not meet \mathcal{C} .

Example 3.18. Find the equation of the non-singular conic in $\mathbb{P}_2(\mathbb{C})$ that contains the points $P = (1, 0, 0)$, $Q = (0, 1, 0)$ and $R = (0, 0, 1)$ and for which the tangents at $(1, 0, 0)$ and $(0, 1, 0)$ meet at $U = (1, 1, 1)$.

Solution.

Let the conic have equation $ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = 0$.

- $P = (1, 0, 0)$ lies on the conic so $a = 0$.
- $Q = (0, 1, 0)$ lies on the conic so $b = 0$.
- $R = (0, 0, 1)$ lies on the conic so $c = 0$.

Hence the equation of the conic reduces to $2fxy + 2gyz + 2hzx = 0$ and the matrix is $M = \begin{pmatrix} 0 & f & h \\ f & 0 & g \\ h & g & 0 \end{pmatrix}$. The tangent at P is given by $XM P^T = 0$, i.e., $fy + hz = 0$.

The tangent at Q is given by $XM Q^T = 0$, i.e., $fx + gz = 0$.

0. If U lies on both of these, then

$$f + h = 0 \text{ and } f + g = 0.$$

Therefore the conic is $2fxy - 2fyz - 2fzx = 0$, i.e.,

$xy - yz - zx = 0$. (Non-singular implies $f \neq 0$.)

3.4 A Canonical Form

As you might expect, we can choose coordinates so that the equation of a nonsingular conic takes a very simple form.

Theorem 3.19. *Let A and B be two points on a nonsingular conic. Then we can choose coordinates so that*

(i) $A = (1, 0, 0)$;

(ii) $B = (0, 0, 1)$;

(iii) the tangents to the conic at A and B meet at $C = (0, 1, 0)$;

(iv) the conic has equation $y^2 = zx$.

Proof. Let D be a third point on the conic (i.e., distinct from A and B). Choose coordinates so that $\triangle ACB$ is the triangle of reference, and D is the unit point. Let the conic have equation $ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = 0$. Then

- $A = (1, 0, 0)$ lies on the conic so $a = 0$.
- $B = (0, 0, 1)$ lies on the conic so $c = 0$.

- The tangent to A has equation $ax + fy + hz = 0$, i.e.,
 $fy + hz = 0$. Now C lies on this line if and only if
 $f = 0$, so indeed $f = 0$.
- The tangent to B has equation $hx + gy + cz = 0$, i.e.,
 $hx + gy = 0$. Now C lies on this line if and only if
 $g = 0$, so indeed $g = 0$.

This reduces the equation to $by^2 + 2hzx = 0$. However
 $D = (1, 1, 1)$ lies on the conic so $b + 2h = 0$. Hence the
equation becomes $b(y^2 - zx) = 0$, i.e., $y^2 = zx$ (note that
 $b \neq 0$ since the conic is non-singular).

□

Remark 3.20. This is a *canonical form*: $y^2 = zx$. In the case of $\mathbb{P}_2(\mathbb{R})$, $z = 0$ is the line at infinity. We can get all the points on the conic which lie in \mathbb{R}^2 by setting $z = 1$. This gives $y^2 = x$, a parabola.

Example 3.21. Let A and B be two points on a non-singular conic \mathcal{C} and suppose that the tangents at A and B meet at C . Let D be a third point of \mathcal{C} and let ℓ be a line through C distinct from AC and BC . Suppose that ℓ meets AD at F and BD at G . Show that AG meets BF in a point of \mathcal{C} .

Solution.

We can take $\triangle ACB$ as the triangle of reference, and D as the unit point, i.e., $A = (1, 0, 0)$, $B = (0, 0, 1)$, $C = (0, 1, 0)$, $D = (1, 1, 1)$. The equation of \mathcal{C} is then $y^2 = zx$.

Suppose that ℓ has equation $ax + by + cz = 0$ for some a, b, c . We know that C lies on ℓ but that A, B do not.

Thus $b = 0$ but $a, c \neq 0$, so ℓ has equation $ax + cz = 0$.

AD is the line $y = z$, which meets ℓ where $y = z$ and $x = -cz/a$, i.e., $F = (-c/a, 1, 1)$.

BD is the line $x = y$, which meets ℓ where $x = y$ and $z = -ax/c$, i.e., $G = (1, 1, -a/c)$.

AG passes through $(1, 0, 0)$ and $(1, 1, -a/c)$ so has equation $z = (-a/c)y$.

BF passes through $(0, 0, 1)$ and $(-c/a, 1, 1)$ so has equation $x = (-c/a)y$.

Hence AG and BF meet at $(-c/a, 1, -a/c)$. We observe that $1^2 = (-c/a)(-a/c)$ and so this point does indeed lie on \mathcal{C} .

Theorem 3.22. *The points on a non-singular conic in the canonical form: $y^2 = zx$ are precisely the points of the form*

$$(1, 0, 0) \text{ and } (\theta^2, \theta, 1)$$

where $\theta \in \mathbb{K}$.

Proof. Observe that all the given points lie on the conic.

Suppose that $P = (p, q, r)$ lies on the conic, so $q^2 = pr$.

If $r = 0$, then $q^2 = p \times 0$ so $q = 0$ and the point is $(p, 0, 0)$, equivalently $(1, 0, 0)$.

If $r \neq 0$, then we can write $P = (\phi, \theta, 1)$, where $\phi = p/r, \theta = q/r$. Then

$$\theta^2 = \frac{q^2}{r^2} = \frac{pr}{r^2} = \frac{p}{r} = \phi.$$

Hence $P = (\theta^2, \theta, 1)$. Therefore all points on the conic

have the given form.

□

Definition 3.23. A line meeting a non-singular conic in 2 points is called a **chord** (or sometimes a **secant line**).

Theorem 3.24. Suppose that \mathcal{C} is a non-singular conic in the canonical form $y^2 - zx = 0$.

(a) The chord joining distinct points $(\theta^2, \theta, 1)$ and $(\phi^2, \phi, 1)$ has equation

$$x - (\theta + \phi)y + \theta\phi z = 0.$$

(b) The chord joining distinct points $(\theta^2, \theta, 1)$ and $(1, 0, 0)$ has equation

$$y = \theta z.$$

(c) The tangent at the point $(\theta^2, \theta, 1)$ has equation

$$x - 2\theta y + \theta^2 z = 0.$$

The tangent at the point $(1, 0, 0)$ has equation $z = 0$.

Proof. (a) The chord has equation

$$\begin{vmatrix} x & y & z \\ \theta^2 & \theta & 1 \\ \phi^2 & \phi & 1 \end{vmatrix} = 0,$$

i.e., $x(\theta - \phi) - y(\theta^2 - \phi^2) + z(\theta^2\phi - \phi^2\theta) = 0$, i.e.,

$$(\theta - \phi)[x - y(\theta + \phi) + \theta\phi z] = 0.$$

Since $\theta \neq \phi$, we can cancel $\theta - \phi$ to get

$$x - (\theta + \phi)y + \theta\phi z = 0.$$

(b) Both points satisfy the equation, so it is the equation of the line joining them.

(c) For the sake of tidiness, note that we can write the

equation of \mathcal{C} as $2y^2 - 2zx = 0$. The matrix M of \mathcal{C} can

then be written $M = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix}$. The tangent at $(1, 0, 0)$ has equation

$$(x, y, z) \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 0, \text{ i.e., } (x, y, z) \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} = 0,$$

in other words, $z = 0$.

The tangent at $(\theta^2, \theta, 1)$ has equation

$$(x, y, z) \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} \theta^2 \\ \theta \\ 1 \end{pmatrix} = 0, \text{ i.e., } (x, y, z) \begin{pmatrix} -1 \\ 2\theta \\ -\theta^2 \end{pmatrix} = 0,$$

in other words, $-x + 2\theta y - \theta^2 z = 0$, equivalently

$$x - 2\theta y + \theta^2 z = 0.$$

□

Example 3.25. Let A, B and C be three points on a non-singular conic \mathcal{C} . Suppose that the tangent at A meets BC in P , the tangent at B meets AC in Q and the tangent at C meets AB in R . Show that P, Q, R are collinear.

Solution.

Let D be the intersection of the tangents to A and B .

Then we may take A, B, D to be the triangle of reference

with C the unit point, i.e., $A = (1, 0, 0)$, $B = (0, 0, 1)$, $D = (0, 1, 0)$, $C = (1, 1, 1)$. The equation of \mathcal{C} is then $y^2 = zx$.

The tangent at A is AD so is $z = 0$, BC is $x = y$ so $P = (1, 1, 0)$. The tangent at B is $x = 0$, AC is $y = z$ so $Q = (0, 1, 1)$. The tangent to C is given by $x - 2y + z = 0$ by Theorem 3.24, AB is $y = 0$, so $R = (1, 0, -1)$.

Observe that $(1, 0, -1) = (1, 1, 0) - (0, 1, 1)$, so R lies on PQ and hence P, Q, R are collinear.

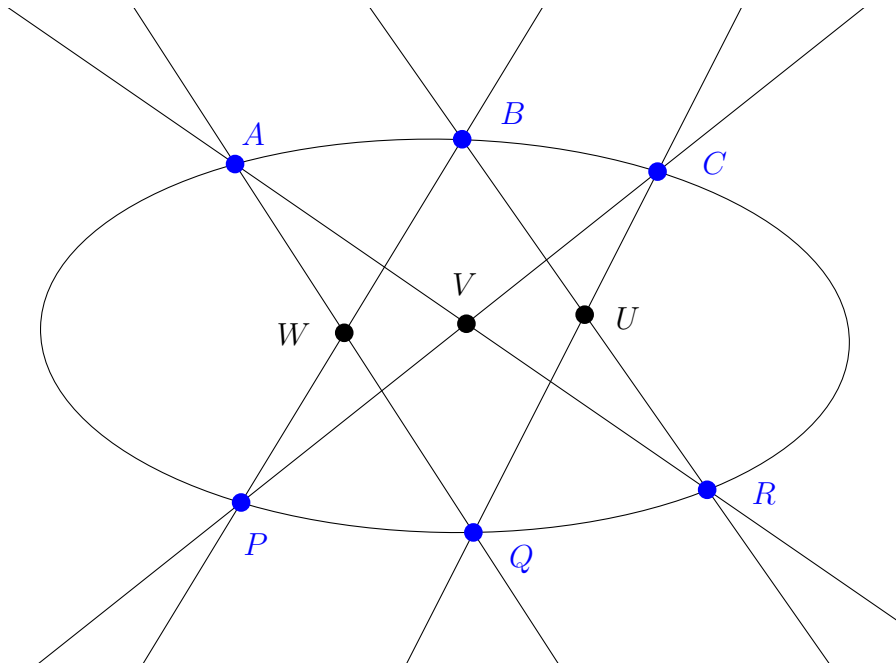
3.5 Pascal's Theorem

Theorem 3.26 (Pascal). *Let A, B, C, P, Q, R be 6 (distinct) points on a non-singular conic. Then the intersection points*

$$(i) U = BR \cap CQ; (ii) V = AR \cap CP; (iii) W = AQ \cap BP$$

are collinear.

Proof.



Choose the co-ordinates so that the equation of the conic is in the Canonical Form, with

$$A = (1, 0, 0), C = (0, 0, 1), Q = (1, 1, 1), B = (\theta^2, \theta, 1), P = (\phi^2, \phi, 1), R =$$

We use Theorem 3.24 for the equations of chords.

BR has equation $x - (\theta + \psi)y + \theta\psi z = 0$ and CQ has equation $x = y$. Therefore at U we have $x(1 - \theta - \psi) + \theta\psi z = 0$, so $U = (\theta\psi, \theta\psi, \theta + \psi - 1)$.

AR has equation $y = \psi z$ and CP has equation $x = \phi y$. Therefore $V = (\phi\psi, \psi, 1)$.

AQ has equation $y = z$ and BP has equation $x - (\theta + \phi)y + \theta\phi z = 0$. Therefore at W we have $x - (\theta + \phi - \theta\phi)z = 0$, so $W = (\theta + \phi - \theta\phi, 1, 1)$.

Now

$$\begin{aligned} (\theta-1)V + \psi W &= ((\theta-1)\phi\psi + \psi(\theta + \phi - \theta\phi), (\theta-1)\psi + \psi \cdot 1, (\theta-1) \cdot 1 + \psi) \\ &= (\psi\theta, \theta\psi, \theta + \psi - 1) = U \end{aligned}$$

so

$$U = (\theta - 1)V + \psi W.$$

Thus U lies on the line VW : U, V, W are collinear.

□

Note: It might be easier to see that $U + (1 - \theta)V = \psi W$.

Note: we could have computed

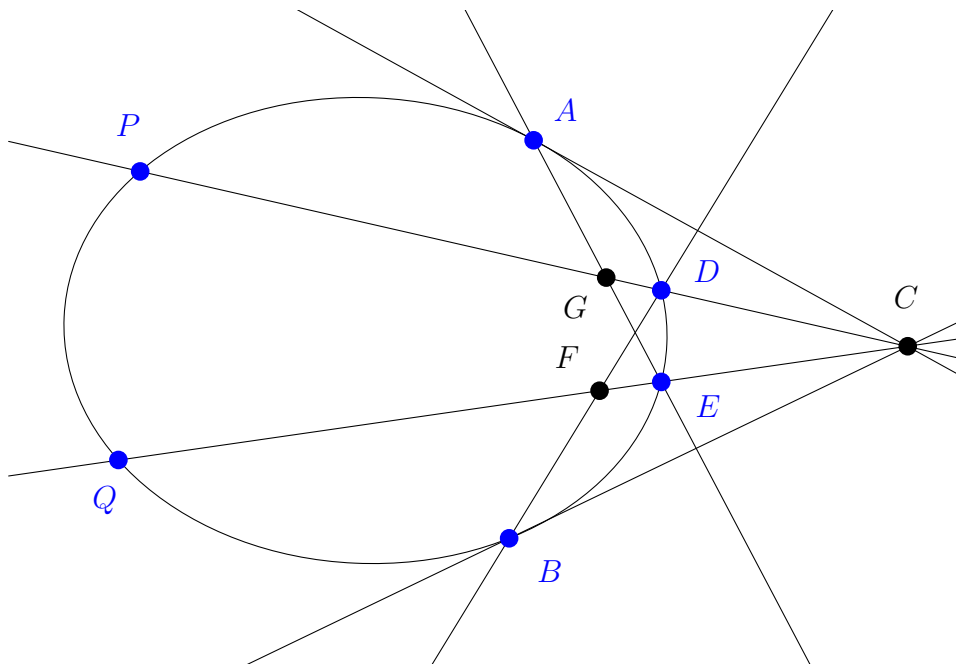
$$\begin{vmatrix} \theta\psi & \theta\psi & \theta + \psi - 1 \\ \phi\psi & \psi & 1 \\ \theta + \phi - \theta\phi & 1 & 1 \end{vmatrix}$$

$$\begin{aligned} &= \theta\psi(\psi - 1) - \theta\psi(\phi\psi - (\theta + \phi - \theta\phi)) + (\theta + \psi - 1)(\phi\psi - (\theta + \phi - \theta\phi)\psi) \\ &= \theta\psi^2 - \theta\psi - \theta\psi^2\phi + \theta^2\psi + \theta\psi\phi - \theta^2\psi\phi + \theta\phi\psi - \theta^2\psi - \theta\phi\psi \\ &\quad + \theta^2\phi\psi + \phi\psi^2 - \theta\psi^2 - \phi\psi^2 + \theta\phi\psi^2 - \phi\psi + \theta\psi + \phi\psi - \theta\phi\psi = 0. \end{aligned}$$

Remark 3.27. As we shall see soon, a conic in $\mathbb{P}_2(p)$ has $p + 1$ points. Thus a conic in $\mathbb{P}_2(3)$ has only 4 points and Pascal's Theorem cannot apply.

Example 3.28. Let \mathcal{C} be a non-singular conic (in $\mathbb{P}_2(\mathbb{C})$ or $\mathbb{P}_2(p)$ with $p \geq 5$). Let A, B, D, E be distinct points on \mathcal{C} and let C be the intersection of the tangents at A and B . Assume that C, D, E are not collinear. Let F be the intersection of DB and CE , let G be the intersection of EA and CD , let P be the intersection of CD with \mathcal{C} ($P \neq D$) and let Q be the intersection of CE with \mathcal{C} ($Q \neq E$). Prove that PQ, FG and DE are concurrent.

Solution.



We can take $A = (1, 0, 0)$, $C = (0, 1, 0)$, $B = (0, 0, 1)$ and $D = (1, 1, 1)$, so that \mathcal{C} has equation $y^2 - zx = 0$. Thus $E = (\theta^2, \theta, 1)$ for some $\theta \neq 0, 1$.

First consider P : it lies on CD so it has co-ordinates $(1, 1, 1) + \lambda(0, 1, 0)$ for some λ (clearly $P \neq C$ since C is not on \mathcal{C}). At the same time P lies on \mathcal{C} so has co-ordinates $(\phi^2, \phi, 1)$ for some ϕ (note that P cannot be $(1, 0, 0)$). The only way this can happen is if $\phi^2 = 1$, i.e., $\phi = \pm 1$. Now $\phi = 1$ would give us the point D , so ϕ must be -1 and therefore $P = (1, -1, 1)$.

Now consider Q : it lies on CE so it has co-ordinates $(\theta^2, \theta, 1) + \lambda(0, 1, 0)$ for some λ (clearly $Q \neq C$ since C is not on \mathcal{C}). At the same time Q lies on \mathcal{C} so has co-ordinates $(\phi^2, \phi, 1)$ for some ϕ (note that Q cannot be

$(1, 0, 0)$). The only way this can happen is if $\phi^2 = \theta^2$, i.e., $\phi = \pm\theta$. Now $\phi = \theta$ would give us the point E , so ϕ must be $-\theta$ and therefore $Q = (\theta^2, -\theta, 1)$.

F : the line DB is $x = y$ and CE is $x = \theta^2 z$, so $F = (\theta^2, \theta^2, 1)$.

G : the line EA is $y = \theta z$ and CD is $x = z$, so $G = (1, \theta, 1)$.

Using the equations of chords, we see that DE has equation $x - (1 + \theta)y + \theta z = 0$ and PQ has equation $x + (1 + \theta)y + \theta z = 0$. They meet where $2(1 + \theta)y = 0$. Given that $E \neq P$ (since C, D, E are not collinear), $1 + \theta \neq 0$ and so $y = 0$. Hence these lines intersect at $(-\theta, 0, 1)$. Observe that

$$(\theta^2, \theta^2, 1) - \theta(1, \theta, 1) = (1 - \theta)(-\theta, 0, 1).$$

Hence the intersection of DE and PQ lies on FG , i.e.,

DE , PQ , and FG are concurrent.

3.6 5 points determine a conic

Theorem 3.29. *Suppose we are given 5 points, no three of which are collinear. Then they lie on a unique conic.*

Proof. Let the conic have equation $ax^2 + by^2 + cz^2 + 2fxy + 2gyz + 2hzx = 0$. Choose coordinates so that the first four points, P, Q, R, U are the triangle of reference and the unit point, and the 5th point is $V = (p, q, r)$ (with, necessarily, p, q, r not all the same). In fact PQ, QR, PR, PU, QU, RU are the lines $z = 0, x = 0, y = 0, y = z, x = z, x = y$ respectively, so the requirement that V does not lie on these lines means that p, q, r are distinct and non-zero.

- $P = (1, 0, 0)$ lies on the conic so $a = 0$.

- $Q = (0, 1, 0)$ lies on the conic so $b = 0$.
- $R = (0, 0, 1)$ lies on the conic so $c = 0$.

Hence the equation of the conic reduces to $2fxy + 2gyz + 2hzx = 0$ and the matrix is $M = \begin{pmatrix} 0 & f & h \\ f & 0 & g \\ h & g & 0 \end{pmatrix}$.

□

Now use the fact that U and V lie on the conic:

- U lies on the conic, so $2f + 2g + 2h = 0$, i.e., $f + g + h = 0$.
- V lies on the conic, so $2fpq + 2gqr + 2hrp = 0$, i.e., $fpq + gqr + hrp = 0$.

Substituting $h = -(f + g)$ into the second equation gives

$$fpq + gqr - (f + g)rp = 0, \text{ i.e., } fp(q - r) + gr(q - p) = 0.$$

Then $p, r, q - r, q - p \neq 0$, so

$$g = -\frac{p(q - r)}{r(q - p)}f,$$

$$h = -f - g = \left[-\frac{r(q - p)}{r(q - p)} + \frac{p(q - r)}{r(q - p)} \right] f = \frac{q(p - r)}{r(q - p)}f.$$

The conic is then

$$2fxy - 2\frac{p(q - r)}{r(q - p)}fyz + 2\frac{q(p - r)}{r(q - p)}fzx = 0.$$

We cannot have $f = 0$ (for then $g = h = 0$) so we can simplify the equation of the conic to

$$r(q - p)xy - p(q - r)yz + q(p - r)zx = 0.$$

We have shown that there is a unique conic passing through the five given points.

3.7 Non-singular Conics in $\mathbb{P}_2(p)$

In this section we consider a non-singular conic \mathcal{C} in $\mathbb{P}_2(p)$, with p odd.

Theorem 3.30. *There are exactly $p + 1$ points on \mathcal{C} .*

Proof. If we write the equation of \mathcal{C} using the canonical form (i.e., by selecting an appropriate triangle of reference and unit point), then we know by Theorem 3.22 that the points of \mathcal{C} are precisely the points of the form

$$(1, 0, 0) \text{ and } (\theta^2, \theta, 1)$$

where $\theta \in \mathbb{K}$. There are p values for θ and so $p + 1$ points in all. □

Definition 3.31. A line of $\mathbb{P}_2(p)$ is said to be **external** to \mathcal{C} if it does not contain any points of \mathcal{C} . [Recall from Definition 3.23 that a line meeting a non-singular conic in 2 points is called a **chord**.]

Theorem 3.32. (a) *The number of tangents to \mathcal{C} is $p + 1$.*

(b) *The number of chords to \mathcal{C} is $\frac{p(p+1)}{2}$.*

(c) *The number of external lines to \mathcal{C} is $\frac{p(p-1)}{2}$.*

Proof.

(a) By Theorem 3.14, there is a unique tangent at each point of \mathcal{C} . There are $p + 1$ points on \mathcal{C} , so there are $p + 1$ tangents.

(b) Each chord meets \mathcal{C} in two points, and the line between any two points of \mathcal{C} is a chord (necessarily not passing through any other point of \mathcal{C}). There are $p + 1$ points on \mathcal{C} so there are $\binom{p + 1}{2} = \frac{p(p + 1)}{2}$ pairs of points and therefore $p(p + 1)/2$ chords.

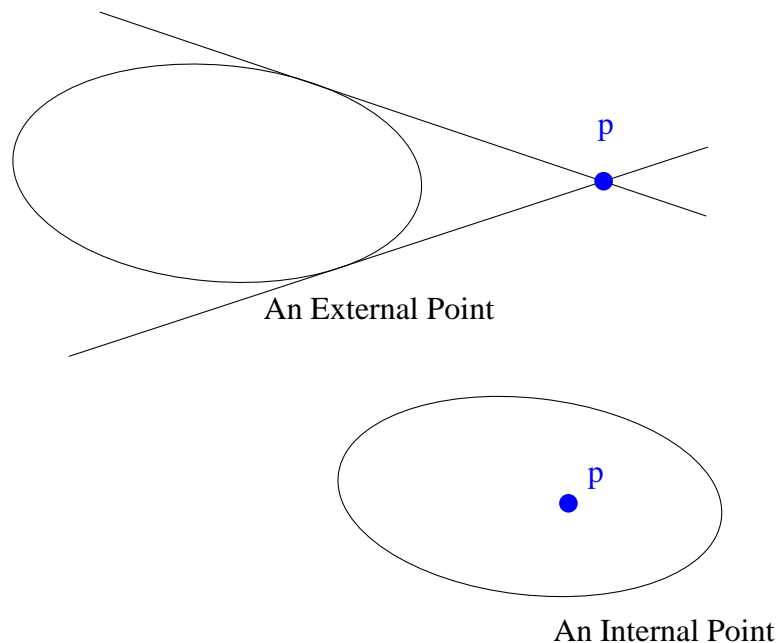
(c) The total number of lines in $\mathbb{P}_2(p)$ is $p^2 + p + 1$ (by Lemma 2.22). Each line meets \mathcal{C} in 0, 1 or 2 points. The number of external lines is the number of lines that meet \mathcal{C} in 0 points, so is

$$p^2 + p + 1 - (p + 1) - \frac{p(p + 1)}{2} = \frac{2p^2 - (p^2 + p)}{2} = \frac{p(p - 1)}{2}.$$

Recall from Theorem 3.16, given a point P of $\mathbb{P}_2(p)$ not on \mathcal{C} , the number of points of the line $XMP^T = 0$ lying on \mathcal{C} is equal to the number of tangents to \mathcal{C} passing through P , and this number is either 0 or 2.

□

Definition 3.33. A point of $\mathbb{P}_2(p)$ not on \mathcal{C} is called **external** if it lies on 2 tangents to \mathcal{C} and **internal** if it lies on no tangents to \mathcal{C} .



Theorem 3.34. Let P be a point of $\mathbb{P}_2(p)$ not on \mathcal{C} . Then the line $XMP^T = 0$ is external to \mathcal{C} if and only if P is an internal point.

Proof. The number of points of the line $XMP^T = 0$ lying on \mathcal{C} is equal to the number of tangents to \mathcal{C} passing

through P . Therefore if $XM P^T = 0$ is a chord, then the number of tangents to \mathcal{C} through C is 2, i.e., P is an external point; if $XM P^T = 0$ is an external line to \mathcal{C} , then the number of tangents to \mathcal{C} through C is 0, i.e., P is an internal point.

□

Theorem 3.35. (a) The number of external points is $\frac{p(p+1)}{2}$.

(b) The number of internal points is $\frac{p(p-1)}{2}$.

Proof. This follows immediately from Theorems 3.32 and 3.34.

□

Example 3.36. Given a non-singular conic \mathcal{C} in $\mathbb{P}_2(p)$, prove that each external line contains $(p+1)/2$ internal points and $(p+1)/2$ external points.

Solution.

Let ℓ be an external line. Each point of ℓ lies on 0 or 2 tangents to \mathcal{C} . There are $p+1$ tangents to \mathcal{C} and each necessarily meets ℓ in a point. If N is the number of external points on ℓ , then $N \times 2 = p+1$. Hence ...