# MT261 Discrete Mathematics (2006)
# Notes by Christian Elsholtz
# based on notes by David Yates

## 1 Graphs

### 1.1 Basic definitions and properties

*Definition* 1.1.1.

a) Let $V$ be a finite non-empty set of elements, called *vertices*; (singular: vertex).

b) An *edge* is an unordered pair of distinct vertices of $V$. The set of edges is denoted by $E$. $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$. (Note that not necessarily all pairs of vertices occur).

c) A graph is a pair $V$ and $E$, denoted by $G = G(V, E)$.

d) Consider a "pair" of the same element. This pair is (according to the definition above) not an edge. It is called a *loop.*

e) A *multigraph* is defined similarly except that $E$ is now a "family" consisting of finitely many edges, at least one pair not being distinct and/or there is a loop.

In this course $V$ and $E$ will always be finite; where necessary they will be denoted by $V(G)$ and $E(G)$ respectively to show their relationship to a given graph $G$. The symbol $G(V, E)$ may denote a graph or a multigraph, unless specified otherwise, but the existence of loops may cause problems. If a definition or theorem requires $G$ to be a graph this will be stated.
Some authors use different terminology. For example what was defined above to be a graph or multigraph they call a simple graph or graph respectively. The definitions in each book must be carefully checked.
A graph or multigraph is best represented pictorially, the vertices being marked by dots or small circles (see below). If the edge joining two vertices $u, v$ is in $E$, then these dots are joined in the picture by a line, usually straight. For a multigraph the lines may be duplicated. It is important to realise however that the same graph can have different pictures depending on how the dots are placed and the lines drawn.

*Example* 1.1.2.

$$V = \{a, b, c, d, e\}, \qquad E = \{\{a, b\}, \{a, d\}, \{b, e\}, \{c, d\}, \{d, e\}\}.$$

These three pictures all represent the same graph, although they look quite different. In the third picture, although the lines $\{a, d\}$ and $\{b, e\}$ appear to cross, the intersection does not represent a vertex. This is why the vertices are represented by dots or small circles. It may seem perverse to draw the picture in this way, though putting the vertices in an ordered circular pattern is not unusual, but there are many graphs where every drawing involves such "crossing points". This will be discussed later in the course.

*Definition* 1.1.3. In a graph or multigraph $G = G(V, E)$ two vertices $u, v$ are *neighbours* if $E$ contains at least one edge $e = \{u, v\}$. (In a graph: exactly one edge!)
In this case $v$ is said to be *adjacent* to $u$; $u$ and $v$ are *incident* with $e$ and are its endpoints, and $e$ *joins* $v$ to $u$ and is incident with them. Two lines are adjacent if they have at least one common endpoint.
In Chapter 1 of this course (i.e. the chapter on graph theory) $n$ and $m$ will always denote the number of vertices and edges respectively of a graph (or multigraph) $G$. Where necessary we also denote these by $n(G)$ and $m(G)$.

*Example* 1.1.4.

$$V = \{a, b, c, d, e\}, E = \{\{a, b\}, \{a, b\}, \{a, d\}, \{b, e\}, \{c, c\}, \{c, d\}, \{d, e\}\}$$

or more simply

$$E = \{ab, ab, ad, be, cc, cd, de\}.$$

This is clearly not a graph but it is a multigraph; the edge $ab$ is called a multiple edge and the edge $cc$ is a loop.

The distinction between graphs and multigraphs in this course is that the former do not have a multiple edge or loop. If they are removed from this example the resulting graph is that of Example 1.1.2, but the two objects are distinct as their families of edges are different. Basically two graphs (multigraphs) are the same if their vertices can be given the same labels (say 1 to $n$) and then the edge sets are identical; this will be discussed in more detail in section 1.4.

*Example* 1.1.5. Example (c) The Königsberg Bridge Problem

Königsberg (Kaliningrad) lies on both sides $A$ and $B$ of the river Pregel in which around 1730 there were parts $C$ and $D$ connected by seven bridges $a, b, c, d, e, f, g$ as shown in Figure 1.3 (a). The citizens attempted to take a walk which crossed each of the seven bridges exactly once. Eventually the problem was given to Euler (1736) who showed that such a walk was impossible.

Graph Theory is considered to date from this problem. Such "Eulerian walks" and similar ideas form a major part of Graph Theory and will be discussed later.

Let the land masses be the vertices of a multigraph and the bridges be the edges as shown in Figure 1.3 (b). If the walk "approaches" the vertex $A$ along the edge $a$ (say) it must "leave" along $b$ or $f$, thus using two of the edges incident with $A$. This also applies to the other three vertices; only at the start and end of the walk is an odd number of edges involved. So if a walk exists, only two of the vertices can have an odd number of incident edges, and the rest must have an even number. (If the walk must start and finish at the same vertex, all the numbers must be even.) Clearly for the Königsberg problem the condition fails, with all four vertices having an odd number of incident edges, whence an "Eulerian walk" is impossible there. For further details see: Biggs, Lloyd and Wilson, Graph Theory 1736 - 1936, OUP (1986).

It can be proved without too much difficulty that for a "connected" graph the above conditions for an "Eulerian walk" are both necessary and sufficient. Again this will be proved later, in section 1.7. The Königsberg problem produces a multigraph, but it is always possible to convert a multigraph into a graph by inserting an "extra" vertex into all but one of each set of multiple edges, and two into any loop. For Example (c) this gives the graph of Figure 1.1.3 (c). Although the walk problem is unaffected by this change the new graph is different from the original multigraph; in particular $n$ and $m$ have each increased by two.

## 1.2 Special Examples

There are several families of special graphs, most labelled by the value of $n \in \mathbb{N}$.

1. The Null Graph $N_n$ on $n$ vertices, i.e. $|V| = n$ and $E = \emptyset$, i.e. $m = 0$ with no vertices joined at all.

2. The Complete Graph $K_n$ on $n$ vertices, e.g. $V = \mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$, $\quad E = \{\{u, v\}; 0 \leq u < v \leq n - 1\}$ with each vertex joined to all of the others exactly once, so that $m(K_n) = \frac{n(n-1)}{2}$. Clearly $K_1 = N_1$.

3. The Line Graph $L_n$ on $n$ vertices, e.g. $V = \mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$, $\quad E = \{\{u, u + 1\}; 0 \leq u \leq n - 2\}$ with each vertex joined to the next one, so that $m(L_n) = n - 1$. Note that $L_1 = K_1 = N_1$ and $L_2 = K_2$.

4. The Cycle or Circuit Graph $C_n$ on $n$ vertices ($n \geq 3$), e.g. $V = \mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$, (here it is important you consider it modulo $n$). $E = \{\{u, u + 1\}; 0 \leq u \leq n - 1\}$ with each vertex joined to the next one and the last to the first (note $\{n-1, n\} = \{n-1, 0\} = \{0, n-1\}$) so that $m(C_n) = n$. Clearly $C_n$ is $L_n$ with the end vertices joined. If the vertices are placed as if they were the $n$-th roots of unity in an Argand Diagram the edges can be drawn either as the sides of the corresponding regular $n$ -gon or as the unit circle.

5. The Wheel Graph $W_k$, ($k \geq 3$), formed by adding one vertex to $C_k$ and joining it to all the other vertices of that graph. This is equivalent to including the origin in the above Argand Diagram and joining it to all the $k$-th roots of unity. Note that $n(W_k) = k + 1$ and $m(W_k) = 2k$.

   *Example* 1.2.1. Examples with $n = 5$.

6. The Petersen Graph below is named after the Danish mathematician Julius Petersen (1839-1910) who discussed its properties in 1898. It can be expressed pictorially in several ways, two of which are shown in Figure 1.2.2, and provides a useful example (or counter-example) for many interesting properties in graph theory.

*Definition* 1.2.2. A bipartite graph $G = G(V, E)$ is a graph for which $V = X \cup Y$, with $X \neq \emptyset, Y \neq \emptyset$, $X \cap Y = \emptyset$ and $\{u, v\} \in E \Longrightarrow$ either $(u \in X$ and $v \in Y)$ or $(u \in Y$ and $v \in X)$. Thus $V$ can be divided into two disjoint non - empty subsets $X, Y$ such that all the edges in $E$ join a vertex of $X$ to a vertex of $Y$ (with no multiple edges).

$K_{r,s}$ is the Complete Bipartite Graph for which $|X| = r > 0$, $|Y| = s > 0$, $\quad E = \{\{u, v\} : u \in X, v \in Y\}$, i.e. each vertex of $X$ is joined to all the vertices of $Y$ and vice versa. $K_{1,s}$ is called a Star Graph. Clearly $K_{r,s} = K_{s,r}$; usually the smaller number is written first. Also $n(K_{r,s}) = r + s$ and $m(K_{r,s}) = rs$.

*Example* 1.2.3. The white (open) dots represent the vertices of $X$ and the black (solid) dots the vertices of $Y$.

## 1.3 Adjacency and Valency

Let $G = G(V, E)$ be a graph or multigraph with $n$ vertices and $m$ edges.

*Definition* 1.3.1. i) The *adjacency list* of $G$ is a set of columns labelled by the vertices of $V$ such that the column corresponding to the vertex $v$ contains all the vertices to $v$, with multiple edges giving repeated entries.

ii) The *adjacency matrix* of $G$ is the $n \times n$ matrix with the rows and columns labelled by the vertices of $V$ in the same order for which the $uv$-entry is the number of edges joining $u$ to $v$, with the convention that loops count twice.

iii) Th *incidence matrix* of $G$ is the $n \times m$ matrix with the rows labelled by the vertices of $V$ and the columns by the edges of $E$ such that the $ve$-entry is 1, if the vertex $v$ is incident to the edge $e$, and is 0 otherwise. Again loops count twice so that if $f = \{v, v\} \in E$ then the $vf$-entry is 2.

*Example* 1.3.2. The following multigraph $G = G(V, E)$, where $V = \{a, b, c, d\}$ and $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ gives the list and matrices shown below.

Given any of these three arrays the other two can obviously be constructed, as can be a pictorial form of $G$. Clearly not every table forms a valid adjacency list, for if the column labelled $x$ contains $y$, then the column labelled $y$ must contain $x$. Moreover the adjacency matrix must be symmetrical.

From the adjacency matrix it is easy to see, whether $G$ is a graph or multigraph. There are loops, if and only if there are non-zero elements on the leading diagonal, and multiple edges if some of the other entries are greater than 1.

*Definition* 1.3.3. Given a graph $G(V, E)$. A graph $G'(V', E')$ is a *subgraph* of $G$ if $V' \subseteq V$ and $E' \subseteq E$. Note that $G'$ must be a graph in its own right so that $G'$ can only contain those edges of $E$ for which both endpoints belong to $V'$. If $G'$ contains all those edges of $E$ for which both endpoints are in $V'$, then $G'$ is said to be the subgraph of $G$, *induced* by $V'$.

*Example* 1.3.4.

*Definition* 1.3.5. Let $G = G(V, E)$ be a graph or multigraph. For each $v \in V(G)$ the valency or the degree $\rho(v)$ is the number of edges in $E(G)$ which are incident with $v$, i.e. for which $v$ is an endpoint.
Convention: a loop $(v, v)$ counts as 2 endpoints.
The nonnegative integers $\rho(v)$ are called the *valency numbers* of $G$.
A vertex $v$ is said to be *odd* or *even*, corresponding to whether $\rho(v)$ is odd or even.

**Remark**. i) Some books use $d(v)$ or $\delta(v)$ instead of $\rho(v)$.

ii) For a graph $0 \leq \rho(v) \leq n - 1$.

*Example* 1.3.6. For the multigraph $\rho(a) = 3, \rho(b) = 5, \rho(c) = 1, \rho(d) = 4, \rho(e) = 3, \rho(f) = 0$. So, $a, b, c, e$ are odd vertices, and $d, f$ are even vertices.

**Theorem 1.3.7** (Handshaking Lemma). *For every graph or multigraph $G = G(V, E)$:*

$$\sum_{v \in V} \rho(v) = 2m = 2|E|.$$

*Proof.* Each edge $e = \{u, v\}$ has two endpoints and this contributes one to $\rho(u)$ and one to $\rho(v)$, i.e. each edge contributes 2 to the sum. By the above convention this is also valid for loops.

□

**Remark**. The name arises from the fact that if in a group of people some pairs of people shakes hands (not necessarily all pairs!), then the number of hands shaken will be even, (two hands for each handshake).

**Corollary 1.3.8.** *Every graph or multigraph has an even number of odd vertices.*

The proof follows directly from the handshaking lemma, considered modulo 2.

*Definition* 1.3.9. A graph $G = G(V, E)$ is regular of valency (or degree) $r$, (also: is regular $r$-valent) if for all vertices $\rho(v) = r$.

Note that the handshaking lemma gives $r|V| = 2|E|$, (or $rn = 2m$).

*Example* 1.3.10. The circuit graph $C_n$ is regular 2-valent, $K_n$ is regular $(n-1)$-valent, $N_n$ is regular 0-valent. $W_n$ is only for $n = 3$ regular, then it is regular 3-valent (and equivalent to $K_4$).

## 1.4 Isomorphism and Planarity

*Definition* 1.4.1. Two graphs $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ are *isomorphic* if there is a bijection $f : V_1 \mapsto V_2$ such that $\{u, v\} \in E_1$ if and only if $\{f(u), f(v)\} \in E_2$. Thus $f$ maps the vertices in $V_1$ onto those of $V_2$ in such a way that the edges in $E_1$ are mapped onto those of $E_2$.

**Remark.** i) Usually it is easier to prove that two graphs are not isomorphic (since studying one vertex (the right one!) and its edges might often suffice) than to prove that two graphs are isomorphic, since here one needs to study the whole graph.

ii) For two isomorphic graphs, clearly: $|V_1| = |V_2|$ and $|E_1| = |E_2|$. Also $u$ and $f(u)$ must have the same valency. And so $G_1$ and $G_2$ have the same set of valency numbers. These conditions are necessary, but not sufficient(!), for two graphs to be isomorphic.

iii) The definition above can also be applied to multigraphs.

*Example* 1.4.2.

a) The graphs a) and b) are isomorphic. $a \mapsto \quad, b \mapsto \quad, c \mapsto \quad, d \mapsto \quad.$

The graphs of c) and d) are not isomorphic. (The valency numbers are 2222 and 2231). The multigraph in e) has the same valency numbers as the graph in d) but is not isomorphic to it.

b) Figure 1.4.2:
$K_1$ and $L_1$ are isomorphic to $N_1$.
$L_2$ and $K_{1,1}$ are isomorphic to $K_2$.
$C_3$ is isomorphic to $K_3$.
$K_{1,2}$ is isomorphic to $L_3$.
$K_{2,2}$ is isomorphic to $C_4$.
$W_3$ is isomorphic to $K_4$.
From the valency numbers it follows that no other pairs of special graphs defined in section 1.2 are isomorphic.

c) The two graphs in Figure 1.4.3 have the same valency numbers $1, 2, 2, 2, 3$ and thus the same value of $n$ and $m$ but they are not isomorphic. In the first graph the odd vertices (i.e. the vertices with odd valency) are adjacent, while they are not adjacent in the 2nd graph. (One can say, they are separated by an even vertex).

Some graphs (like $K_4$) have so far often been drawn with a crossing point, which is not a vertex.

*Definition* 1.4.3. i) $G = G(V, E)$ is a *plane* graph if $V$ is a finite subset of $\mathbb{R}^2$ and $E$ is a set of continuous curves in $\mathbb{R}^2$ which meet only at the vertices of $V$.

ii) A graph $G$ is a *planar* graph if it is isomorphic to a plane graph.

These definitions are rather awkward, we come back to these.

## 1.5 Connected Graphs

*Definition* 1.5.1. Let $G = G(V, E)$ be a graph.

i) A *walk* $W$ of length $k \in \mathbb{N}$ in $G$ is a (finite) sequence $v_0, v_1, ..., v_k$ of vertices in $V$ for which successive vertices are adjacent, so that $\{v_i, v_{i+1}\} \in E$ for $i = 0, 1, \ldots, k-1$. $v_0$ is the *initial vertex* of $W$ and $v_k$ is the *final vertex*. $W$ is a walk from $v_0$ to $v_k$, or a $v_0$ - $v_k$ walk.

ii) A *trail* in $G$ is a walk in $G$ for which no edge is repeated, in either direction.

iii) A *path* $P$ in $G$ is a walk in $G$ for which all the vertices, and hence all the edges, are distinct. If the vertices are $v_0, v_1, \ldots, v_k$, then $P$ is a path from $v_0$ to $v_k$, or a $v_0$ - $v_k$ path, where $v_0 \neq v_k$ here. Therefore $P$ is a subgraph of $G$ which is isomorphic to $L_{k+1}$.

iv) A *circuit* in $G$ is a walk $v_0, v_1, \ldots, v_k$ with $v_k = v_0$, i.e. a 'closed' walk.

v) A *cycle* $C$ of length $k$, or a $k$ - cycle, is a circuit $v_0, v_1, ..., v_k$ with $k \geq 3$ for which the vertices are distinct apart from $v_k = v_0$, so it is essentially a 'closed path'.

Thus $C$ is a subgraph of $G$ which is isomorphic to $C_k$. A cycle of length 3 is called a *triangle*.

**Remark**. Some books may use these words or others in different contexts. Sometimes a walk is described in terms of the edges or using both $V$ and $E$. This is essential if the definitions are applied to multigraphs, which can be done with care. However this section will only consider graphs unless stated otherwise. Many books allow walks and paths to have zero length ($k = 0$ ) but that will not be done here.

*Example* 1.5.2.

**Theorem 1.5.3.** *Let $G = G(V, E)$ be a graph, and suppose that $u$ and $v$ are vertices in $V$.*

*i) If $u \neq v$ there is a $u - v$ path in $G$ if and only if there is a $u - v$ walk in $G$.*

*ii) Define $u \sim v$ if either $u = v$ or there is a $u - v$ path in $G$. Then $\sim$ defines an equivalence relation on $V$, and if $V_1$ and $V_2$ are different equivalence classes under this relation, then there are no edges in $E$ which join a vertex $v_1 \in V_1$ to a vertex $v_2 \in V_2$.*

*Proof.* (i) $\Rightarrow$ is obviously true from the definitions.
For $\Leftarrow$ suppose that $u = v_0, v_1, ..., v_k = v$ is a walk $W$ from $u$ to $v$. If these vertices are all distinct, then $W$ is a path. Otherwise there is a least integer $r$ for which $v_t = v_r$ for some $t$ with $0 \leq r < t \leq k$. Let $s$ be the largest integer for which $v_s = v_r$; this $s$ exists as the walk is finite.

Then the vertices $v_0, v_1, ..., v_r, v_{s+1}$ are distinct and form a path from $u = v_0$ to $v_{s+1}$ with the adjacency of successive vertices being obtained from $W$. Repeat this process, finding the least integer $p \geq s + 1$ for which $v_q = v_p$ for some $q$ with $p < q \leq k$ etc. until all the vertices are distinct and form a path from $u$ to $v$. (This path is a subsequence of the walk W.

(ii) To prove $\sim$ is an equivalence relation we need to prove it is reflexive, symmetric and transitive. $u \sim u$ from the definition, and if $u \sim v$ with $u = v_0, v_1, \ldots, v_k = v$ being a $u - v$ path in $G$, then clearly $v = v_k, v_{k-1}, \ldots, v_0 = u$ is a $v - u$ path in $G$, whence $v \sim u$. Finally suppose that $u \sim v$ and $v \sim w$; if either $u = v, v = w$ or $u = w$ then $u \sim w$. Otherwise there is a $u - v$ path $u = v_0, v_1, \ldots, v_k = v$ and a $v - w$ path $v = w_0, w_1, ..., w_l = w$ (say), and thus $u = v_0, v_1, ..., v_k = v = w_0, w_1, ..., w_l = w$ is a walk from $u$ to $w$. Hence from (i) there is a $u - w$ path and $u \sim w$, so that $\sim$ is an equivalence relation. Clearly any edge from $v_1 \in V_1$ to $v_2 \in V_2$ would be a path of length 1 and thus give $v_1 \sim v_2$, contradicting the definition of equivalence classes and their disjointness.

□

*Definition* 1.5.4. A graph $G$ is said to be *connected* if for every pair of distinct vertices $u$ and $v$ there is a $u - v$ path in $G$; otherwise $G$ is *disconnected.* In the first case there is only one equivalence class under $\sim$ but in the second there must be at least two.

*Example* 1.5.5. (b) The graphs $K_n, L_n, C_n, W_k, K_{r,s}$ defined in section 1.2 are all connected as is $N_1$, but the graphs $N_n$ are disconnected if $n \geq 2$. So is the graph shown in Figure 1.5.2.

*Definition* 1.5.6. For connected graphs $G = G(V, E)$,

i) the distance $d(u, v)$ between distinct vertices $u$ and $v \in V$ is the length of the shortest $u - v$ path in $G$; $d(v, v)$ is defined to be 0.

ii) the diameter $d(G)$ of a connected graph $G$ is the largest distance between two vertices in $G$.

iii) the girth $g(G)$ of $G$ is the length of the shortest cycle in $G$.

**Remark**. Two isomorphic graphs must clearly have the same diameters and girths.

*Example* 1.5.7. i) For $K_n, d(u, v) = 0$ or 1 and so $d(K_n) = 1$ and $g(K_n) = 3$ if $n \geq 3$.

ii) For $L_n$ with $n \geq 2, d(u, v) = |u - v|, d(L_n) = n - 1$ while $g(L_n)$ is not defined.

iii) For $C_n$ with $n \geq 3, d(u,v) = \min\left(|u-v|, n-|u-v|\right), d(C_n) = [n/2]$ and $g(C_n) = n$.

iv) For $W_k$ with $k \geq 4, d(u,v) = 0, 1$ or $2$, $d(W_k) = 2$ and $g(W_k) = 3$.

v) For the Petersen Graph, by inspection $d(u,v) = 0, 1$ or $2$, the diameter is 2 and the girth is 5.

vi) For $K_{r,s}$ with $2 \leq r \leq s, d(u,v) = 0, 1$ or $2$, $d(K_{r,s}) = 2$ and $g(K_{r,s}) = 4$ (see the Theorem below).

*Definition* 1.5.8. For a general graph $G = G(V,E)$ the equivalence classes $V_j$ under $\sim$ induce another relation on $E$ with the edge $e = \{u,v\} \in E$ belonging to $E_j$ if and only if $u, v \in V_j$. (This statement is valid from Theorem 1.5.3 (ii)). Thus $G_j = G_j(V_j, E_j)$ is the subgraph of $G = G(V,E)$ induced by $V_j$. These subgraphs $G_j$ are called the *components* of $G$. Each is a connected graph from its definition and the number of them is denoted by $\omega(G)$. For each $u \in V_j \subseteq V, G(u) = G_j$ is the component of $u$ in $G$. It contains all the vertices $v \in V$ for which there is a $u - v$ path in $G$. If $u$ is the only vertex in $G(u)$ then its valency is 0 and it is said to be an *isolated* vertex of $G$. Clearly every vertex of $N_n$ is isolated. A connected graph $G$ has only one component which is equal to $G(u)$ for every $u \in V$.

**Theorem 1.5.9.** *A graph $G$ is bipartite if and only if each cycle has an even length.*

*Proof.* Using the notation of section 1.2, if $v_0, v_1, \ldots, v_k$ is a cycle in $G$ suppose without loss of generality that $v_0 \in X$. Then $v_1 \in Y, v_2 \in X$, and generally $v_{2i} \in X, v_{2i+1} \in Y$ for every $i \in \mathbb{N}_0$ since all the edges of $E$ join a vertex of $X$ to one of $Y$. Therefore if $v_k = v_0 \in X$ , $k$ must be even.
Conversely suppose that $G$ has no cycles of odd length. Let $u_1$ be a given vertex of the component $G_1$ of $G$ and put $v$ into $X_1$ if the distance $d(u_1, v)$ between the vertices $u_1$ and $v$ in $G_1$ is even and into $Y_1$ if it is odd. Suppose that $x$ and $y$ both belong to $X_1$ but that there is an edge $e = \{x, y\} \in E_1$. Let $P(x)$ and $P(y)$ be paths of shortest distance from $u_1$ to $x$ and $y$ respectively. Neither of these can contain $e$ without violating the parity condition. But if the paths last separate at $w$ then the parts of these paths from $u_1$ to $w$ must have the same length otherwise they would not be the 'shortest'. Thus the parts from $w$ to $x$ and $y$ must have the same parity, whence the path from $x$ to $w$ and from there to $y$ is of even length. As this path together with $e$ would form a cycle of odd length, no such edge $e \in E_1$ can exist. Similarly if both $x$ and $y$ are in $Y_1$; so $G_1$ is a bipartite graph. The process can be repeated for the other components $G_j$ of $G$, with the choice of each of the 'given' vertices $u_j$ determining which part belongs to $X_j$ and which to $Y_j$. Thus $G = G(X \cup Y, E)$ is a bipartite graph with $X = \cup X_j$ and $Y = \cup Y_j$ since from Theorem 1.5.3 (ii) there are no edges joining the vertices which are in different components.
Note: If $G$ is connected there is essentially only one choice for $X$ and $Y$; otherwise there may be several depending on the choice of the $u_j \in V_j$. □

*Definition* 1.5.10. For a connected graph $G = G(V, E)$, a *disconnecting set of edges* is a subset of $E(G)$ such that removing them ’disconnects’ $G$. A *cutset* is a minimal disconnecting set, i.e. one for which no proper subset is a disconnecting set. An *isthmus* is a single edge which forms a cutset. Therefore $e = \{u, v\} \in E$ is an isthmus in $G$ if and only if the subgraph $G^* = G^*(V, E \setminus \{e\})$ of $G$ is disconnected, which leaves $u$ and $v$ belonging to different components of $G^*$ (see below).

*Example* 1.5.11. For the graph in Figure 1.5.3, $\{3, 4, 5\}$ forms a disconnecting set, $\{4, 5\}$ is a cutset and 7 is an isthmus.

*Example* 1.5.12. If $n \geq 3$ the cutsets of $C_n$ must contain exactly 2 edges while those of $K_n$ must contain at least $n - 1$ edges. For many of the special examples of section 1.2 the ’smallest’ cutsets are those which isolate just one of the vertices.

**Theorem 1.5.13.** *Let $e = \{u, v\}$ be an edge of a connected graph $G = G(V, E)$ and put $G^* = G^*(V, E \setminus \{e\})$.*

*i) Removing e from E cannot give a graph $G^*$ with more than two components, and there are exactly two components if and only if e is an isthmus of G.*

*ii) Any two distinct vertices $u, v$ of a cycle $C$ in $G$ can be connected by two distinct paths in $G$ which are disjoint apart from their endpoints.*

*iii) An edge $e = \{u, v\} \in E$ belongs to a cycle $C$ in $G$ if and only if it is not an isthmus of $G$.*

*Proof.* i) Assume $G^*$ consists of at least 3 components, then one would need at least two edges to join $G^*$ to a connected graph

ii) A cycle in $G$ can be traversed 'clockwise' or 'anticlockwise'. Formally if $C$ is $v_0, v_1, \ldots, v_k = v_0$, and $u = v_i, v = v_j$ where $i < j$ (see Figure 1.5.5), then one path is $v_i, v_{i+1}, \ldots, v_j$ with increasing indices and the other is $v_i, v_{i-1}, ..., v_0, v_{k-1}, \ldots, v_j$ with decreasing indices. These paths are clearly disjoint apart from their endpoints $u$ and $v$.

iii) If $e = \{v_i, v_{i+1}\}$ is an edge of the cycle $C$ of (ii) (see Figure 1.5.5 again), then removing it still leaves $G^*$ connected, for from (ii) there is a path from $v_i$ to $v_{i+1}$ round the rest of the cycle, whence $G^*(v_i) = G^*(v_{i+1})$ from Theorem 1.5.3 (i) and $G^*$ has only one component from (i). Thus $e$ cannot be an isthmus of $G$ from the same result.

Conversely, if $e = \{u, v\} \in E$ is not an isthmus of $G$, the graph $G^*$ is still connected, and there is a path $v_0, v_1, \ldots, v_{k-1}$ (say) from $v$ to $u$ in $G^*$ (see Figure 1.5.6). Clearly $v_0, v_1, \ldots, v_{k-1}, v_0$ is a cycle in $G$, the last edge being $e$ which thus belongs to a cycle in $G$.

Note: Although they are obviously closely related, $G$ and $G^*$ are different graphs. If $G$ is 'disconnected' by the removal of $e$ the remaining graphs are subgraphs of $G$ and components of $G^*$. □

## 1.6 Trees

*Definition* 1.6.1. A *tree* is a connected graph which has no cycles, and a *forest* is a graph which has no cycles, i.e. one for which every component is a tree. Clearly from Theorem 1.5.13 (iii), a graph is a tree if and only if it is connected and every edge is an isthmus.

Clearly every line graph $L_n$ is a tree with $n$ vertices and $n-1$ edges. The tree of Figure 1.6.1(a), which is $L_4$, is not isomorphic to that of (b) though both have four vertices and three edges. The three trees of (e) are isomorphic to that of (d), each having six vertices and five edges. All these trees satisfy the following theorem.

**Theorem 1.6.2.** *A tree $T$ with $n$ vertices has exactly $m = n-1$ edges.*

*Proof.* Use induction on $n$, observing first that the result is obviously true for both $n=1$ and $n=2$ as shown by the following diagrams. Let $T = T(V,E)$ be a tree with $n$ vertices and suppose that the theorem is true for all trees having fewer than $n$ vertices. From the above statement every $e \in E$ is an isthmus, so as in Theorem 1.5.13 (i) removing it from $T$ leaves a graph $T^* = T^*(V, E \setminus \{e\})$ with exactly two components, $T_1$ and $T_2$ (say). Both of these must be trees since they are connected and if either contained a cycle $C$, then $C$ would also be a cycle in $T$. If $T_1, T_2$ have $n_1, n_2$ vertices and $m_1, m_2$ edges respectively, then $n_1$ and $n_2$ are both less than $n$ and $n_1 + n_2 = n$. Hence from the induction hypothesis, $m_1 = n_1 - 1$ and $m_2 = n_2 - 1$ so that $T^*$ has $m_1 + m_2 = n_1 + n_2 - 2 = n - 2$ edges. Thus replacing $e$ the number of edges of $T$ is $m_1 + m_2 + 1 = n - 1$. □

**Corollary 1.6.3.** *A connected graph $G$ with $n$ vertices must have at least $n-1$ edges.*

*Proof.* If $C$ is a cycle in $G$ then from Theorem 1.5.13 (iii) none of its edges is an isthmus and so any one edge of $C$ can be removed from $G$ without 'disconnecting' it. This deletion of single edges can be repeated so long as there are cycles, and since $E$ is finite the process stops when the final connected graph produced has no cycles. But this final graph is a tree with the same set of $n$ vertices as $G$ and exactly $n-1$ edges from Theorem 1.6.2, whence $G$ must have had at least $n-1$ edges. □

**Corollary 1.6.4.** *A graph $G$ with $n$ vertices and $\omega$ components has at least $n-\omega$ edges, with equality if $G$ is a forest.*

*Proof.* If each component $G_j$ of $G \quad (j = 1, 2, \ldots, \omega)$ has $n_j$ vertices and $m_j$ edges, then from Corollary 1.6.3 $m_j \geq n_j - 1$, whence $\sum_{j=1}^{\omega} m_j \geq \sum_{j=1}^{\omega}(n_j - 1) = n - \omega$. If each $G_j$ is a tree the inequality becomes an equality, so that a forest with $n$ vertices and $\omega$ components has $n-\omega$ edges. (See Remarks (3) below.) □

There are several alternative ways of defining a tree, all equally valid as proved in the following theorem.

**Theorem 1.6.5.** *Let $G = G(V, E)$ be a graph with $n$ vertices. Then the following statements are equivalent:*

*i) $G$ is a tree;*

*ii) $G$ contains no cycles and has exactly $n-1$ edges;*

*iii) $G$ is connected and has exactly $n-1$ edges;*

*iv) for any two distinct vertices $u, v$ of $G$ there is exactly one $u-v$ path;*

*v) $G$ contains no cycles, but the addition of any new edge between non - adjacent vertices creates exactly one cycle.*

*Proof.* If $n = 1$, then all the statements are satisfied (trivially) so assume that $n \geq 2$. For each part of the proof only the 'current statement' may be assumed.

i) $\longrightarrow$ ii) By definition $G$ contains no cycles; that it has exactly $n-1$ edges is proved in Theorem 1.6.2.

ii) $\Longrightarrow$ iii) Suppose that $G$ is not connected. Then each of its components $G_1, G_2, \ldots, G_\omega$, $(\omega \geq 2)$ is connected and contains no cycles and is thus a tree. So if $G_j$ has $n_j$ vertices, then from Theorem 1.6.2 $G_j$ has $n_j - 1$ edges. But since $n_1 + n_2 + \cdots + n_\omega = n$, there are only $n-\omega$ edges in $G$, which is a contradiction of (ii) as $\omega \geq 2$, so $G$ must be connected.

iii) $\Longrightarrow$ i) If any edge $e$ is removed from $G$ then the resulting graph $G^*$ has only $n-2$ edges, whence it is disconnected from Corollary 1.6.3. Therefore every edge of $G$ is an isthmus and so from Theorem 1.5.13 (iii) $G$ has no cycles and is thus a tree.

i) $\Longrightarrow$ iv) Since $G$ is connected, for any two distinct vertices $u, v$ there is at least one path from $u$ to $v$. Suppose that there are two distinct $u-v$ paths $P_1, P_2$ in $G$. Starting from $u$ assume that these paths have the vertices $u = u_0, u_1, \ldots, u_k = x$ in common but that the next vertices $w_1, w_2$ of $P_1, P_2$ respectively are different. Let $y$ be the first vertex after $x$ which is common to $P_1$ and $P_2$; there must be such a vertex since the paths coincide at $v$. Then the two sections of the paths from $x$ to $y$ together form a cycle when one is taken in the 'reverse' order, contradicting the definition of a tree, whence the result.

iv) $\Longrightarrow$ v) $G$ cannot contain a cycle, for if it did contain a cycle $C$, then from Theorem 1.5.13 (ii) there would be two paths connecting any two distinct vertices of $C$. Since any two non - adjacent vertices $u, v$ are connected by a path in $G$, the addition of the edge $e = \{u, v\}$ forms a cycle. But if $e$ completes two cycles $C_1, C_2$, then the parts of $C_1, C_2$ not containing $e$ form two different paths from $u$ to $v$ in $G$, which contradicts (iv).

v) $\Longrightarrow$ i) From the hypothesis $G$ contains no cycles. If $u, v$ are non - adjacent vertices of $G$, adding the edge $e = \{u, v\}$ creates a cycle. But from Theorem (ii) there is a $u - v$ path in $G$ which does not include $e$. Since there is clearly a path joining adjacent vertices, $G$ is connected and is therefore a tree.

□

**Remark.**

1. The last two parts of the proof are still valid if $n = 2$, when the tree has no non - adjacent vertices.
2. The first three parts show that any two of the statements : $G$ is connected, $G$ has no cycles, $m = n - 1$, define a tree.
3. It follows from this theorem that the statements of Theorem 1.6.2 and its Corollaries are both necessary and sufficient. Thus a connected graph is a tree if and only if $m = n-1$, and a graph with $n$ vertices and $\omega$ components has $n - \omega$ edges if and only if it is a forest.

*Definition* 1.6.6. Suppose that $G = G(V, E)$ is a connected graph. A subgraph $G_1(V_1, E_1)$ of $G$ is a *spanning tree* if it is a tree which spans $G$, meaning that $V = V_1$. Thus $G_1 = T(V, E_1)$. Here $|E_1| = n - 1$.

Every connected graph has a spanning tree. It can be constructed from $G$ as in the proof of Corollary 1.6.3, by deleting edges that belong to a cycle. Note that a graph can have many distinct spanning trees.

**Theorem 1.6.7.** *Let $T = T(V, K)$ and $S = S(V, L)$ be two different spanning trees of a connected graph $G = G(V, E)$. There is an edge $e$ of $T$ which is not in $S$, i.e. $e \in K \backslash L$, and there is an edge $f$ of $S$ which is not in $T$ such that the graph $Y = Y(V, L \cup \{e\} \backslash \{f\}$ is also as spanning tree of $G$.*

*Proof.* Since $T$ and $S$ are distinct and since the set of vertices is the same, the set of edges must be distinct. Since $|K| = |L|$ for each edge $e \in K \backslash L$ there must be an edge $f \in L \backslash K$ (and vice versa).
By Theorem 1.6.5 *i)* $\Longrightarrow$ *v)* the addition of $e$ to $S$ creates a cycle, actually exactly one cycle. Since $T$ does not contain any cycles, the new graph $X = X(V, L \cup \{e\})$ must contain at least one edge $f$ on the cycle which is not in $T$. Since $e \in T$ but $f \notin T$, we have $f \neq e$. So, $f \in L$. Now let $Y$ be the graph obtained from $X$ by removing $f$; $Y = Y(V, L \cup \{e\} \backslash \{f\})$. $Y$ contains $n = |V|$ vertices, $|L| + 1 - 1 = |L| = n - 1$ edges and no cycles, since the only cycle has been broken by removing $f$. By Theorem 1.6.5 *ii)* $\Longrightarrow$ *i)* $Y$ is a spanning tree of $G$.

Figure 1.6.3

□

**Corollary 1.6.8.** *Every edge $e \in E$ belongs to a spanning tree of $G$.*

*Proof.* Start with any spanning tree $S = (V, L)$. If $e \notin L$, then define $X = X(V, L \cup \{e\})$ and find (by the previous Theorem) $f$ so that $Y = Y(V, L \cup \{e\} \backslash \{f\})$ is a spanning tree containing $e$. □

**Remark.** i) There is a dual statement, where a given edge $e$ of $S$ is removed. By repeating this, step by step, one can obtain a spanning tree $T$ which does not have any edge in common with $S$.

ii) Spanning trees have important applications. A typical application would be if vertices represent cities and edges the roads between them. The edges carry a value (for example the cost to build this road) and the task is to find a spanning tree with minimal sum of these values, representing a road network connecting all cities but with minimum building costs.

## 1.7 Eulerian Trails and Hamiltonian Paths

*Definition* 1.7.1. i) Let $G = G(V, E)$ denote a graph or multigraph. A walk in $G$ is Eulerian if it includes every edge of $E$ exactly once (so that it is a trail). An Eulerian circuit is an Eulerian trail which is also a circuit (i.e. which is a closed trail).

ii) A graph or multigraph is said to be Eulerian, if it has an Eulerian circuit and is said to be semi-Eulerian if it has an Eulerian trail but is not Eulerian.

These names come from the generalisation of the Königsberg bridge problem, at the beginning of the course.

*Example* 1.7.2. Figure 1.7.1.

Observe that a graph or multigraph $G$ can only be Eulerian/semi Eulerian if it is connected, apart from components which only consist of isolated vertices. For this reason we can assume without loss of generality that $G$ is connected.

**Theorem 1.7.3.** *Let $G = G(V, E)$ be a connected graph. Then $G$ is Eulerian if and only if every vertex is even (i.e. has an even valency or degree).*

*Proof.* $\Longrightarrow$ For every Eulerian circuit of $G$ the consecutive edges $\{u, v\}, \{v, w\}$ contribute 2 to the value of $\rho(v)$. This occurs every time $v$ is a vertex in the walk (through a different pair of edges each time). Since $G$ is connected, the circuit goes along all edges and meets all vertices. For each vertex $v \in V$: for each incoming edge there is an outgoing edge, along the circuit (all distinct), so $\rho(v)$ must be even.
$\Longleftarrow$ To prove the other direction we first present an algorithm and then prove that this algorithm constructively gives the Eulerian circuit.
**Algorithm (due to Hierholzer 1873):**
Given a finite connected graph $G$ with $\rho(v)$ is even, for all $v \in V$.
1) Start at an arbitrary edge $v_0$. Want to construct a circuit. Choose any trail $v_0, v_1, v_2 \ldots v_i$, as long as this is possible. One ends at $v_i = v_0$ (to be proved below). So we have found a circuit $C_0$.
If the circuit $C_0$ is Eulerian, then STOP.
2) Otherwise there is an edge $w$ not yet used in $C_0$. Starting at $w$, construct a circuit $C_1'$ on the edges of $G$ avoiding those already used in $C_0$, so work on $G_1 = G_1(V, E\backslash C_0)$. (Compare step 1).
To get one circuit $C_1$, start at $v_0$ and go along $C_0$ until one reaches $w$, then go along $C_1'$, which returns to $w$, continue along $C_0$.
If the circuit $C_0$ is Eulerian, then STOP, otherwise iterate step 2, constructing circuits $C_2, C_3, \ldots$.
After finitely many steps one reaches an Eulerian circuit, (to be proved below).

Proof of the correctness of the algorithm.
(It is convenient to separate the algorithm and its proof),

Step 1 does indeed give a circuit: Continue on any trail as long as this is possible. If it is not possible to continue at $v_i$, then $v_i = v_0$. Otherwise $\rho(v_i)$ were odd.
In the same way, the trails constructed in step 2 are circuits.
We now must prove that we can stop after finitely many steps, reaching an Eulerian circuit.
Since $G$ is finite one only needs finitely many steps, so the question is if the final circuit $C_i$ is Eulerian. Otherwise there must be an edge $e$ that is not on the circuits $C_i$. Moreover all the vertices on the circuit $C_i$ are only incident with edges that are used in $C_i$ (otherwise go to step 2)! But then there cannot be any trail from any point on $C_i$ to the edge $e$. This contradicts the hypothesis that $G$ is connected, (where one can go from any vertex to all other vertices). □

*Example* 1.7.4. In Figure 1.7.2. we start (for example) with $v_0 = a$, and get a circuit $C_0 = (abha)$. Now all edges incident to $a$ have been used. Get another circuit $C_1' = (bcdfchgb)$ (so no new edges incident to $b$) and so $C_1 = (abcdfchgbha)$ and $C_2' = (defgd)$ and so $C_2 = (abcdefgdfchgbha)$.

An alternative algorithm is due to Fleury:
**Fleury's algorithm:** 1) Start at any vertex $v_0$.
2) Traverse any edge $e_1 = \{v_0, v_1\}$, but only choose an isthmus if there is no other choice.
3) Delete $e$ and also $v_i$ if it is now isolated.
4) Repeat steps 2 and 3 for $v_1$, ...
5) Stop, when there are no more edges remaining that can be traversed
In 2), isthmus refers to the subgraph of $G$ after deleting edges and vertices (in step 3).
The resulting walk $v_0, v_1, v_2, \ldots, v_k$ (say) will be an Eulerian circuit of $G$ with $v_0 = v_k$.

*Example* 1.7.5. Figure 1.7.3. Starting at $v_0$, choose $e_1$ going to $v_1$, delete $e_1$. The edge $e_5$ is *now* an isthmus, so avoid it. So walk along $e_2$, $e_3$ and $e_4$ (there is no choice!) and delete these edges, and also the isolated vertices.) Now one has to choose $e_5, e_6, e_7$ completing the Eulerian circuit.

**Corollary 1.7.6.** *A connected graph $G$ is semi-Eulerian if and only if it has exactly two odd vertices.*

*Proof.* $\Longleftarrow$ If there is an Eulerian trail which is *not* an Eulerian circuit, then from the proof of Theorem 1.7.3 (part $\Longrightarrow$) every vertex is even except possibly for the initial vertex $v_0$ and the final vertex $v_k \neq v_0$ of the trail. By the Handshaking Lemma the degree of the initial and final vertex must both be even, or both be odd. Since there is no Eulerian circuit ($G$ is semi Eulerian), by Theorem 1.7.3 (part $\Longleftarrow$) these vertices must both be odd.
$\Longrightarrow$ Suppose that $u$ and $v$ are the only odd vertices. Define a new graph $G' = G'(V \cup \{x\}, E \cup \{\{x,u\},\{x,v\}\})$. All vertices of $G'$ are even, and so by Theorem 1.7.3 there is an Eulerian circuit starting at $x$ and ending at $x$: $(x, u = v_0, \ldots, v_k = v, x)$. Then $(v_0, \ldots, v_k)$ is an Eulerian trail of $G$. See figure 1.7.4.

□

**Remark**. If one works with multigraphs, then one adds an additional vertex on the multiple edges or loops. These vertices have even degree. In this way one can transform the multigraph $G$ to a graph $G'$, where the number of odd vertices remains the same, and one then applies the results above.
Adding such additional vertices on edges is called *subdivision of a graph.*

*Definition* 1.7.7. i) Let $G = G(V,E)$ be a connected graph. A path in $G$ is *Hamiltonian* if it passes through each vertex $v \in V$ exactly once. So, if the path is $v_0, v_1, \ldots, v_k$, then $v_i \neq v_j$ for $i \neq j$ and $V = \{v_0, v_1, \ldots, v_k\}$.

ii) A cycle in $G = G(V,E)$ is Hamiltonian, if it has a Hamiltonian path $v_0, v_1, \ldots, v_k$ with $v_0 = v_k$.

iii) G is Hamiltonian if it has a Hamiltonian cycle. $G$ is semi-Hamiltonian if it has a Hamiltonian path, but not a Hamiltonian cycle.

**Remark**. Clearly a disconnected graph cannot have a Hamiltonian path. Also, from the definition, multiple edges or loops cannot be part of the walk so that we can restrict (without loss of generality) to connected graphs.
The name comes from Sir William Rowan Hamilton who was interested in the edge graph of the dodecahedron (which is Hamiltonian). He posed as a puzzle to find a cycle meeting each vertex once.

*Example* 1.7.8. $C_n, K_n, W_n$ are Hamiltonian. $K_{3,3}$ is Hamiltonian, $K_{2,3}$ is semi-Hamiltonian.

In contrast to Theorem 1.7.3 there is no known necessary and sufficient condition for a graph to be Hamiltonian. Still, Hamiltonian graphs have many applications, in particular in a variant called the Travelling salesman problem where the edges carry a weight (say the distance between the vertices which are thought of as cities), and the question is about a tour passing through all cities exactly once with the minimum sum of the weight of the edges. This is (for large graphs) a very difficult problem, both in theory and practice.

**Theorem 1.7.9** (O. Ore, 1960)**.** *Let $G = G(V, E)$ be a graph with $n \geq 3$ vertices and suppose that $\rho(u) + \rho(v) \geq n$ for every pair of non-adjacent vertices $u$ and $v$. Then $G$ is a connected graph and is Hamiltonian.*

[We do not prove this Theorem. We do not use this result later on.]

**Theorem 1.7.10** (G.A. Dirac, 1952)**.** *Let $G = G(V, E)$ be a graph with $n \geq 3$ vertices. If for all $v \in V : \rho(v) \geq \frac{n}{2}$ holds, then $G$ is Hamiltonian.*

*Proof.* Define a graph $G'$ by adding $k$ new vertices to $V$ and joining these to all vertices in $V$. If $k = n$, then $G'$ is certainly Hamiltonian. Let $k_0$ be the minimum number so that $G'$ becomes Hamiltonian. Certainly $0 \leq k_0 \leq n$ and we will prove that $k_0 > 0$ leads to a contradiction. This then implies that $G$ itself is already Hamiltonian.
Assume that $k_0 > 0$. Let $K = (a, x, b, \ldots a)$ be a Hamiltonian cycle of $G'$, where $a, b$ are already in $G$ but $x$ is a new vertex. $a$ and $b$ are not adjacent, since otherwise $x$ is not necessary for the cycle to be Hamiltonian. Note that a vertex $b'$ adjacent to $b$ cannot be a direct successor of a vertex $a'$ which is adjacent to $a$. Otherwise replace the cycle $K = (a, x, b, \ldots, a', b')$ by $K = (a, a', \ldots b, b', \ldots a)$ and again $x$ is omitted.
Let $A$ be the set of neighbours of $a$, (i.e. the set of all vertices adjacent to $a$). Let $B$ be the set of neighbours of $b$ and $F$ be the set of vertices of $G'$ that are directly behind a vertex of $A$, in the cycle $K$. $B \cap F = \emptyset$ (note that also $a$ and $b$ are not adjacent. Then $|B| \geq \frac{n}{2} + k_0, |F| \geq |A| \geq \frac{n}{2} + k_0$. The inclusion and exclusion principle, which we study in more detail later, generally states: $|B \cup F| = |B| + |F| - |B \cap F|$. Here, this simplifies to $|B \cup F| = |B| + |F| \geq n + 2k_0$. This is a contradiction since $G'$ only contains $n + k_0$ vertices.

□

The hypotheses above are sufficient for guaranteeing the existence of a Hamiltonian cycle. The graphs satisfying these hypotheses are relatively dense, i.e. have very many edges. But the hypotheses are not necessary conditions. This means there can be graphs which are Hamiltonian, but where these hypotheses are not satisfied. For example the cycle $C_n$ or the wheel $W_n$.

## 1.8 Planarity and Euler's Formula

Plane and planar graphs were defined in section 1.4.
In this section we study ways to draw graphs.

*Definition* 1.8.1. i) A *continuous* curve in the Euclidean plane $\mathbb{R}^2$ is a set of points $\{(f(t), g(t)) : t \in [a, b]\}$, where $[a, b]$ is a finite closed real interval and where $f : [a, b] \to \mathbb{R}$ and $g : [a, b] \to \mathbb{R}$ are continuous functions.

ii) A *smooth* curve is a continuous curve, where in addition $f'$ and $g'$ are also continuous.

iii) A *Jordan* curve is a smooth curve in the Euclidean plane which does not intersect (i.e. $(f(x_1), g(x_1)) \neq (f(x_2), g(x_2))$, if $x_1 \neq x_2$).

Jordan's curve theorem says that a closed Jordan curve divides the plane $\mathbb{R}^2$ into two parts (interior and exterior). This is actually very difficult to prove.

*Definition* 1.8.2. A graph is plane if $V \subset R^2$ and the edges are Jordan curves which meet (intersect) only at their endpoints, the vertices. A graph is planar if it isomorphic to a plane graph.

*Example* 1.8.3. $K_4, K_{2,3}$.

*Definition* 1.8.4. Given a graph with its drawing. Assume that edges meet vertices only at their endpoints. A point where edges of $E$ cross (intersect) but which is not a vertex is called a crossing point. The crossing number of $G$, $cr(G)$ is the smallest integer so that the graph $G$ can be drawn with $cr(G)$ crossings. (For planar graphs: $cr(G) = 0$).

*Definition* 1.8.5. A planar graph divides $\mathbb{R}^2$ into regions, called faces. One of the regions is unbounded, the others are bounded. (But it may be depend on the drawing which region is unbounded.)

**Theorem 1.8.6.** *Let $G$ be a planar connected graph. Let $n = |V|, m = |E|$ and let $f$ be the number of faces. Then $n - m + f = 2$.*

*Proof.* Proof by induction on $m$. Let $m = 0$, then $n = f = 1$ so that the formula is correct. (Also, if $m = 1$, it is correct).
Now assume that the formula has been proved for all planar connected graphs with $m-1$ edges. Let $G$ be a planar connected graph with $m$ edges. If $G$ is a tree, then the formula is correct since $m = n - 1$ and $f = 1$. So assume that $G$ is not a tree and therefore it contains a cycle. Define a new graph $G'$ by removing an edge $e$ from the cycle. $G'$ has $m - 1$ edges and so the formula is valid for $G'$ (induction hypothesis). All planar diagrams of $G$ come from planar diagrams of $G'$ by adding this one edge $e$. Adding the edge $e$ to come from $G'$ back to $G$ divides one face into two parts. (This actually makes use of the difficult Jordan's curve theorem). So, in the expression $n - m + f = 2$ (which is valid for $G'$ in the form $n - m' + f' = 2$) one increases the number of edges and faces by one ($m = m' + 1$) and ($f = f' + 1$) so that the formula is valid for $G$.

□

**Corollary 1.8.7.** *For a planar graph with $k$ components the formula is:*

$$n - m + f = k + 1.$$

*Proof.* Apply the theorem to each component. □

**Theorem 1.8.8.** *Let $G$ be a planar graph with $n$ vertices and $m \geq 2$ edges. Then*

$$m \leq 3n - 6.$$

*Proof.* The proof uses a technique called double counting. Count the same thing twice and get information out of it. The object we count is: how often is an edge part of the boundary of a face.
Given a diagram of a planar graph with $n$ vertices, $m \geq 3$ edges and $f$ faces $F_1, \ldots, F_f$. We define an $m \times f$ matrix $A = (a_{i,j})$ as follows:

$$a_i = \begin{cases} 1 & \text{if the edge } e_i \text{ is part of the boundary of } F_j \\ 0 & \text{otherwise.} \end{cases}$$

An edge is part of the boundary of at most two faces, (here: one face is actually possible). So, each row contains at most two entries of 1. So, the number of ones in the matrix is at most $2m$. On the other side, each face is bounded by at least 3 edges (here we need $m \geq 3$). So, each column contains at least 3 entries 1. There are at least $3f$ ones in the matrix. So $3f \leq 2m$. Replacing $f$ by $m - n + 2$ gives $m \leq 3n - 6$. For $m = 2$ there is nothing to prove. And for unconnected graphs one adds up the inequalities for the individual components.

□

The same proof (with 3 replaced by 4 for the minimum number of edges around a face) also shows:

**Theorem 1.8.9.** *Let $G$ be a planar triangle-free graph with $n$ vertices and $m \geq 2$ edges. (Triangle-free means: the shortest cycle has length at least 4.). Then*

$$m \leq 2n - 4.$$

**Corollary 1.8.10.** *A finite planar graph $G$ has a vertex $v$ of degree $\rho(v) \leq 5$.*

*Proof.* Assume all vertices have degree $\rho(v) \geq 6$. Then, by the Handshaking Lemma:

$$2m = \sum_{v} \rho(v) \geq 6n,$$

contradicting Theorem 1.8.8.

□

# 2 Methods of Counting

## 2.1 Sets and cardinal numbers

### SETS

*Definition* 2.1.1. In this chapter $\mathbb{N}$ will denote the (infinite) set of natural numbers,
$\mathbb{N}_0$ the set of natural numbers including 0, namely $\{0, 1, 2, 3, \}$,
$\mathbb{Z}$ is the set of all integers,
$\mathbb{Q}$ the set of rational numbers,
$\mathbb{R}$ the set of real numbers and
$\mathbb{C}$ the set of complex numbers.
$\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ denote the positive integers, rationals and reals respectively.
$\emptyset$ or $\{\}$ is the empty set with no elements.
Here $k, m, n$ denote natural numbers $\geq 1$.
Let $M_n$ denote the set of integers $\{1, 2, 3, \ldots, n\}$. Although this is clearly related to the ring $\mathbb{Z}_n$ there are advantages in using a different symbol; the latter has addition and multiplication modulo $n$ included.

### FUNCTIONS

*Definition* 2.1.2. A function $f$ from a set $A$ into a set $B$ associates with *each* element $a \in A$ a *unique* element $b \in B$ which is usually denoted by $f(a)$. A is called the domain of $f$, $B$ is its codomain, and the subset $f(A) = \{f(a); a \in A\}$ of $B$ is its range. But in general there may be several elements $a$ associated with each $b$, or none at all. $f$ maps $a$ onto $b$, and $A$ into $B$ written $A \to B$. If for each $b \in f(A)$ there is only one $a \in A$ associated with $b$ then $f$ is said to be an injection $(1-1)$; in this case $f(a_1) = f(a_2)$ if and only if $a_1 = a_2$. If $f(A) = B$, i.e. every $b \in B$ is associated with at least one $a \in A$, then $f$ is a surjection (onto). Both these definitions depend on the sets $A$ and $B$ as well as on the function $f$. A function g which is both an injection and a surjection is called a bijection from $A$ onto $B$, sometimes written $A \leftrightarrow B$.
In this case each $b \in B$ is associated with exactly one $a \in A$ and so $g$ has an inverse function $g^{-1}$ from $B$ onto $A$ defined by $g^{-1}(b) = a$. Note that $f$ has an inverse function if and only if it is a bijection; otherwise its 'inverse' is essentially a relation (see below).

## CARDINAL NUMBERS for FINITE SETS

*Definition* 2.1.3. If $A$ is a finite set (see below) define its cardinal number $|A|$ to be $n$ if there is a bijection $g$ from A onto $M_n$.

This defines a method of labelling the elements of $A$, namely $a_i$ where $g(a_i) = i$. The empty set has cardinal number 0. If $A = \{a, b, c, \ldots\}$, $|A|$ is often written $\#\{a, b, c, \ldots\}$.

**Theorem 2.1.4.** *If $k, l$ are natural numbers with $k < l$ there is no injection from $M_l$ into $M_k$.*

*Proof.* Suppose that $k$ is the least positive integer for which an injection $f$ from $M_l$ into $M_k$ exists for some $l > k$. Then $k > 1$ for otherwise all the $l \geq 2$ elements of $M_l$ map onto 1. Now if there is no element of $M_{l-1}$ which maps onto $k$ then restricting $f$ to that set contradicts the 'least' as the range is a subset of $M_{k-1}$. But if $a \in M_{l-1}$ maps onto $k$, then $f$ must map $l$ onto some $b \in M_{k-1}$ since $f$ is an injection. Hence the function $g$ defined by $g(a) = b, g(c) = f(c)$ if $c \in M_{l-1}$ but $c \neq a$, is an injection from $M_{l-1}$ into $M_{k-1}$, again a contradiction of the 'least'. Thus for every $k \in \mathbb{N}$ no such injection can exist. □

**Remark**. This is the Pigeonhole Principle which can be stated in many forms. For example if $l$ letters are put into $k$ pigeonholes or boxes, and $l > k$ at least one hole has more than one letter in it. But there is no way of knowing how many holes have two or more letters, or which they are, or how many letters are in each hole.

**Corollary 2.1.5.** *i) The cardinal number of a finite set $A$ is well-defined, for if $|A| = m = n$, there is a bijection $M_m \leftrightarrow A \leftrightarrow M_n$ whence $m = n$ from the theorem. It follows that $|A| = |B|$ if and only if there is a bijection from $A$ onto $B$.*

*ii) If $k < l$ there is no surjection $h$ from $M_k$ onto $M_l$.*

*Proof.* i) If $|A| = m = n$, there is a bijection $M_m \leftrightarrow A \leftrightarrow M_n$ whence $m = n$ from the theorem. It follows that $|A| = |B|$ if and only if there is a bijection from $A$ onto $B$.

ii) If there was, defining $b = \min\{x \in M_k; h(x) = a\}$ for each $a \in M_l$ would make $a \longrightarrow b$ an injection from $M_l$ into $M_k$. Hence by the Theorem above $l = |f(A)| \leq |A| = k$ for all functions $f$.

□

**THE ALGEBRA OF CARDINAL NUMBERS** If $A, B$ are disjoint finite sets, i.e. $A \cap B = \emptyset$, then $|A \cup B| = |A| + |B|$, for if $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_k\}$, where $b_j \neq a_i$, then the function $a_i \mapsto i$, $b_j \mapsto n + j$ is a bijection of $A \cup B$ onto $M_{n+k}$. In general if the finite sets $S_r$ are mutually disjoint, then $|\cup_r S_r| = \sum_r |S_r|$. For any finite sets $A$ and $B$ the sets $A \cap B = \{x \in A; x \in B\}$

and $A \setminus B = \{x \in A; x \notin B\}$ are disjoint (the law of the excluded middle) with union $A$, and so $|A| = |A \cap B| + |A \setminus B|$. Similarly, $|B| = |A \cap B| + |B \setminus A|$. Since $A \cup B$ is the union of the disjoint sets $A$ and $B \setminus A$, $|A \cup B| = |A \cap B| + |A \setminus B| + |B \setminus A| = |A| + |B| - |A \cap B|$. This will be generalized later in this section to give the Inclusion-Exclusion Principle.

Consider the set of ordered pairs from $A$ and $B$, namely $A \times B = \{(a, b); a \in A, b \in B\}$. If as above $A = \{a_1, a_2, \dots, a_n\}$ and $B = \{b_1, b_2, \dots, b_k\}$, define $A_s = \{(a, b_s); a \in A\}$. Then the $k$ sets $A_s$ are mutually disjoint with union $A \times B$ and for all $s$: $|A_s| = |A| = n$, whence $|A \times B| = nk = |A||B|$. Again this can be generalized for any finite number of finite sets $S_r$ to $|\prod_r S_r| = \prod_r |S_r|$. Finally consider the set $S$ of all functions from $A$ into $B$; let $|S| = q(n, k)$. Then the functions in $S$ for which $f(a_n) = b_s$ are distinct from those for which $f(a_n) = b_t$, i.e. the sets $T_r = \{(f \in S); f(a_n) = b_r\}$ are disjoint with union $S$. But $|T_r| = q(n-1, k)$ and so $q(n, k) = |S| = kq(n-1, k)$, for all $n$. As $q(1, k) = k$, $q(n, k) = k^n = |B|^{|A|}$ by induction. $q(n, 0) = 0, q(0, k) = 1$ can be justified by careful logic.

*Example* 2.1.6. For each subset $X$ of $A$ define $f_X(a) = 1$ if $a \in X$, $f_X(a) = 0$ if $a \notin A \setminus X$, the Characteristic Function of $X$. Clearly each $X$ defines a unique function of $A$ into $\{0, 1\}$ and conversely each such function gives a unique subset of $A$. Thus $A$ has $2^{|A|}$ subsets; $\{X \subseteq A\} = \mathcal{P}(A)$ is called the Power Set of $A$.

## RELATIONS

*Definition* 2.1.7. A relation on a set $A$ is defined as a subset $R$ of $A \times A$ with $a$ being related to $b$, often written $a \sim b$ or $aRb$ if $(a, b) \in R$. An *equivalence relation* on $A$ is a relation on $A$ for which the following laws apply:

i) $a \sim a$, for all $a \in A$, the reflexive law;

ii) If $a \sim b$, then also $b \sim a$, the symmetric law;

iii) If $a \sim b$ and $b \sim c$, then $a \sim c$, the transitive law, where $a, b, c$ are any elements of $A$. Such a relation divides $A$ into disjoint equivalence classes $C_a = \{x \in A; x \sim a\}$ each of which contains related elements. Hence $|A| = |\cup C_a| = \sum_a |C_a|$ but it is important that only one label $a$ be chosen for each class (i.e. a system of representatives of the classes). Note that unlike the examples $A_s$ and $T_r$ above, the classes $C_a$ may have different cardinal numbers.

*Example* 2.1.8. If $n \geq 2$ is an integer, let us define a relation $\equiv$ on $\mathbb{Z}$ by: $a \equiv b$ if and only if $n \mid (a-b)$. This is an equivalence relation and the $n$ equivalence classes are used to define the ring $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

**CARDINAL NUMBERS FOR GENERAL SETS** (assuming the standard axioms)

A set $A$ is infinite if there is a bijection from $A$ onto a proper subset $A^* \subset A$.

*Example* 2.1.9. The set of positive integers can be bijectively mapped to the set of positive even integers. $f(n) = 2n$.

It is not too difficult to prove that a set is not infinite if and only if it has a cardinal number $n$ ($\Leftarrow$ is Theorem 2.1.4). The definition of the cardinal number of a general set is based on the statement that $|A| = |B|$ if and only if there is a bijection from $A$ onto $B$. But most of its algebraic properties are now defined by using the results proved in the previous section. For example, define $|A|$ to be $\leq |B|$ if there is a injection of $A$ into $B$; then the Schröder-Bernstein Theorem proves that $|A| \leq |B|$ and $|B| \leq |A|$ implies that $|A| = |B|$. The inequality $|f(A)| \leq |A|$ is still true. Finally Cantor's diagonal argument proves that $|A| < 2^{|A|} = |\mathcal{P}(A)|$ for every set $A$.

### Applications of the pigeonhole principle

*Example* 2.1.10. At a meeting of a set $S$ of $n$ people, some of them shake hands with some of the other people. Show that there are two people that shake the same number of hands.

For each $x \in S$ let $f(x)$ denote the number of hands shaken by person $x$. $0 \leq x \leq n-1$. In this form one cannot apply the pigeonhole principle. But one observes: whenever at least one person shakes all $n-1$ hands, then there is no person shaking 0 hands. Conversely, if there is a person with $f(x) = 0$, then there is no person with $f(x) = n-1$. So the range of the values of $f$ is actually: $[0, n-2]$ or $[1, n-1]$ (both with $n-1$ elements). By the pigeonhole principle, there cannot be an injection from the set $S$ of $n$ elements into the sets of $n-1$ elements above. This problem is equivalent to a problem on sheet 3: in a finite graph there are two vertices with the same valency.

*Example* 2.1.11. Let $\alpha$ be an irrational number. Define $\{t\alpha\} = t\alpha - [t\alpha]$ to be the fractional part, i.e. $\{ta\} \in [0,1)$. The pigeonhole principle can be used to prove that irrational numbers can be approximated by rational numbers. Study the sequence $\{t\alpha\}$ with $1 \leq t \leq n$ in the $n$ intervals $[\frac{k}{n}, \frac{k+1}{n})$. Either there is one member of the sequence in each interval or there is an interval with two members of the sequence. In the first case $0 < t\alpha - [t\alpha] < \frac{1}{n}$ holds for some $t$. In the second case, if $x\alpha$ and $y\alpha$ are in the same interval, then $0 < (x-y)\alpha - ([x\alpha] - [y\alpha]) < \frac{1}{n}$. In both cases there are integers $p$ and $q$ so that $|q\alpha - p| < \frac{1}{n}$. So, $|\alpha - \frac{p}{q}| < \frac{1}{qn} \leq \frac{1}{q^2}$. For example $\frac{22}{7}$ is such an approximation for $\pi$.

*Example* 2.1.12. Let $n \geq 3$ be an integer and suppose that the integer $t$ satisfies $t^2 \equiv -1 \bmod n$. (Example: $12^2 = 144 \equiv -1 \bmod 29$, since $29 \times 5 = 145$.) Let $(u, v)$ be pairs of integers with $0 \leq u \leq \sqrt{n}$ and $0 \leq v \leq \sqrt{n}$. Since $([\sqrt{n}] + 1)^2 > n$, by the pigeonhole principle there are two pairs $(u_1, v_1), (u_2, v_2)$ with $u_1 - tv_1 \equiv u_2 - tv_2 \bmod n$. So, $(u_1 - u_2) \equiv t(v_1 - v_2) \bmod n$. Let $x = u_1 - u_2, y = v_1 - v_2$, i.e. $x \equiv ty \bmod n$ and observe that $|x| \leq \sqrt{n}$ and $|y| \leq \sqrt{n}$. Actually, if $n$ is not a square, even $|y| < \sqrt{n}$. Therefore, $0 < x^2 + y^2 < 2n$ and $x^2 + y^2 \equiv (ty)^2 + y^2 \equiv 0 \bmod n$, and so $n \mid x^2 + y^2$. In other words $x^2 + y^2 = n$.
Note: if $n$ is a prime of the form $4k + 1$, then such a $t$ exists, actually one can take $t = (\frac{n-1}{2})! \bmod n$. Example: $(\frac{29-1}{2})! = 14! = 87178291200 = 12 \bmod 29$ and then the by the discussion above the prime can be written as a sum of two squares, (example: $29 = 2^2 + 5^2$). If $n$ is a prime of the form $4k + 3$, then no such $t$ exists, and modulo 4 one can see that there is no way of writing an integer $4k + 3$ as a sum of two squares.

**THE INCLUSION-EXCLUSION PRINCIPLE** This generalizes the statement $|A \cup B| = |A| + |B| - |A \cap B|$ given earlier.

**Theorem 2.1.13.** *Let $X$ be a finite set and let $A_1, \ldots, A_n$ be a collection of subsets of $X$. For $x \in X$ let $m(x)$ denote the number of subsets $A_i$ to which $x$ belongs.*

*i)*

$$|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| - \ldots + \ldots + (-1)^{n-1} |\cap_{i=1}^n A_i|.$$

*ii) The number of $x \in X$ for which $m(x) = m$ is*

$$\sum_{\substack{T \subseteq M_n \\ m \leq |T| \leq n}} (-1)^{(|T|-m)} \binom{|T|}{m} |A_T|, \text{ where } A_T = \cap_{i \in T} A_i.$$

*Proof.* i) Consider an element $x \in X$ for which $m(x) = s$. The proof compares the contribution made by th element $x$ to both sides of the equation. If $s = 0$, then

$x$ is in none of the sets and it contributes 0 to both sides. Otherwise $s \geq 1$ and $x$ contributes 1 to the LHS. For this fixed $x$ assume it belongs to precisely the sets $A_{t_1}, \ldots, A_{t_s}$, where $1 \leq t_1 < t_2 < \ldots < t_s \leq n$. Then $x$ contributes 1 to each of the $s$ terms $A_{t_i}$ in the first sum on the RHS, so it contributes $s$. It also contributes -1 to each of the $\binom{s}{2}$ terms $A_{t_i} \cap A_{t_j}, (1 \leq i < j \leq n)$, so altogether $-\binom{s}{2}$. It contributes $\binom{s}{3}$ to the triple intersections, and so on. The total contribution is:

$$s - \binom{s}{2} + \binom{s}{3} - \ldots + (-1)^{s-1}\binom{s}{s} = 1 - (1-1)^s = 1.$$

This holds for every $x \in X$, so the theorem follows.
The proof of part ii) is similar in spirit but more complicated in the analysis of the binomial coefficients.

□

**Corollary 2.1.14.** *The number of elements of $X$ which belong to none of the $A_i$, i.e. $m(x) = 0$ is*

$$|X| - \sum_{i=1}^{n} |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^n |\cap_{i=1}^n A_i| = \sum_{T \subseteq M_n} (-1)^{|T|} |A_T|, \text{ where } A_T = \cap_{i \in T} A_i.$$

*Proof.* This number is $|X \setminus \cup_{i=1}^n A_i| = |X| - |\cup_{i=1}^n A_i|$. □

*Example* 2.1.15. Of 30 third year students, 10 take MT361, 14 take MT362 and 12 take MT365; 4 students are taking both MT361 and MT362, 3 are taking MT361 and MT365, 3 are taking MT362 and MT365, while 1 is taking all three units. How many of this set of students are taking none of the three units and how many are taking precisely one?

Let $X$ be the set of 30 students. $A_i$ those taking MT361, MT362, MT365 for $i = 1, 2, 3$ respectively. The inclusion-exclusion principle part i) gives

$$30 - (10 + 14 + 12) + (4 + 3 + 3) - 1 = 3$$

students take none of the three units. Part ii) shows that: taking

$$T = \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\} :$$

$$1 \times (10 + 14 + 12) - 2 \times (4 + 3 + 3) + 3 \times 1 = 1 \times 36 - 2 \times 10 + 3 \times 1 = 19$$

are taking precisely one unit (or $4+8+7 = 19$ from the Venn-diagram). Similarly, $1 \times 10 - 3 \times 1 = 7$ (or $3 + 2 + 2 = 7$) are taking precisely two units.

*Example* 2.1.16. Let $X = M_n$ where the integer $n \geq 2$ has prime factors $p_1, p_2, \dots, p_k$. For each $i = 1, \dots, k$ let $A_i$ be the set of multiples of $p_i$ in $M_n$ so that $|A_i| = \frac{n}{p_i}$. Clearly, if $i < j$, $A_i \cap A_j$ is the set of multiples of $p_ip_j$ in $M_n$ so that $|A_i \cap A_j| = \frac{n}{p_ip_j}$ etc. Therefore, from the corollary the number of integers $a$ in $M_n$ which are coprime to $n$, i.e. $\gcd(a, n) = 1$, is

$$n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_ip_j} - \ldots + \ldots = n\left(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_ip_j} - \ldots\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),$$

which is Euler's function $\varphi(n)$.
If for example $n = 30$, then there are 8 coprime integers. These are $1, 3, 7, 11, 13, 17, 19, 23, 29$, and the formula gives $30(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - (\frac{1}{5}) = 30\,\frac{1}{2}\,\frac{2}{3}\,\frac{4}{5} = 8$.

*Example* 2.1.17. Using the inclusion-exclusion principle count the primes $p \leq 40$.
$n \leq 40$ is prime, if $n = 2, n = 3, n = 5$ or $n$ is not divisible by $n = 2, 3, 5$ but $n \neq 1$.
$A_2 = \{2, 4, 6, \dots, 40\}, |A_2| = 20$.
$A_3 = \{3, 6, 9, \dots, 39\}, |A_3| = 13$.
$|A_5| = 8, |A_6| = 6, |A_{10}| = 4, |A_{15}| = 2, |A_{30}| = 1$.

$$40 - (20 + 13 + 8) + (6 + 4 + 2) - (1) + 3 - 1 = 40 - 41 + 12 - 1 + 3 - 1 = 12.$$

For comparison, the 12 primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.

**DERANGEMENTS**

The permutations of $M_n = \{1, 2, \ldots, n\}$ form a group $S_n$ of order $n!$. A derangement of $M_n$ is a permutation in $S_n$ which maps no element onto itself. For each $i = 1, \ldots, n$ define a subset $A_i$ of $S_n$ by $A_i = \{\alpha \in S_n; \alpha(i) = i\}$. Then, $|A_I| = (n-1)!$ for each $i$. $A_i \cap A_j = \{\beta \in S_n; \beta(i) = i, \beta(j) = j\}$ giving $|A_i \cap A_j| = (n-2)!$, etc. Since a derangement belongs to none of the $A_i$, the number of derangements of $M_n$ is, with $X = S_n$:

$$\begin{aligned} D_n &= n! - n(n-1)! + \binom{n}{2}(n-2)! - \ldots + (-1)^n \times 1 \\ &= n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^n \frac{1}{n!}\right) \quad \sim \quad \frac{n!}{e}. \end{aligned}$$

In fact, $D_n$ is the "closest" integer to $\frac{n!}{e}$, since the difference between $D_n$ and $\frac{n!}{e}$ is $< \frac{1}{n+1}$.

*Example* 2.1.18. When $n = 4$, the derangements are those elements of $S_4$ whose cycle decompositions contains no cycles of length 1, i.e. those of types [4] or [22]. There are 6 of the first type, namely $(1234), (1243), (1324), (1342), (1423), (1432)$. And there are 3 of the second type, namely $(12)(34), (13)(24), (14)(23)$. Therefore $D_4 = 9$, which is close to $\frac{24}{e} = 8.8291\ldots$.

*Example* 2.1.19. If two full packs of playing cards (of 52 cards each) are turned over simultaneously, the probability of no matching pairs is $\frac{D_{52}}{52!}$ which differs from $\frac{1}{e} = 0.3678\ldots$ by less than $\frac{1}{53!} \approx 2.29 \times 10^{-70}$.

## 2.2 Partitions

*Definition* 2.2.1. If $n \in \mathbb{N}$ a *partition of $n$ into $r$ parts* is a sum of the form $a_1+a_2+\ldots+a_r = n$ where the terms $a_i \in \mathbb{N}$ and satisfy $a_1 \geq a_2 \geq \ldots \geq a_r > 0$. Let $p(n,k)$ be the number of partitions of $n$ with at most $k$ non - zero terms (i.e. $r \leq k$) and $p(n)$ the total number of partitions of $n$, so that $p(n) = p(n,n) = p(n,m)$ for all $m \geq n$.

**Remark**. The simplest way of writing the above partition is as a 'descending string' of numbers $a_1\, a_2\, \ldots\, a_r$ with spaces but no + signs and no commas. The number of terms uniquely gives $r$ and their sum is $n$.

Some small values of the partition functions:

$$p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, p(4,2) = 3, p(5,3) = 5.$$

since for example for 4 has the following 5 partitions.

$$4, 3\,1, 2\,2, 2\,1\,1, 1\,1\,1\,1$$

$$p(n,1) = 1, p(n,2) = 1 + \left[\frac{n}{2}\right], p(n,n-1) = p(n) - 1$$

and $p(n,m) = p(n)$, for $m \geq n$,

$$p(n,0) = 0, p(0) = p(0,k) = 1.$$

**Recurrence relations** If $a_1\, a_2\, \ldots a_k$ is a partition of $n \in \mathbb{N}$ with exactly $r = k$ non zero terms, then $a_1 - 1\ a_2 - 1\ \ldots a_k - 1$ is a partition of $n - k$ with at most $k$ non-zero terms. Hence $p(n,k) - p(n,k-1) = p(n-k,k)$ since the correspondence of those two partitions is a bijection. This is valid if $1 \leq k \leq n$, Adding this over $k$ gives

$$p(n) = p(n,n) - p(n,0) = \sum_{k=1}^{n} p(n-k,k).$$

*Example* 2.2.2.

$$p(7,3) = p(7,2) + p(4,3) = 1 + \left[\frac{7}{2}\right] + p(4,2) + p(1,3) = 1 + 3 + 3 + 1 = 8.$$

$$p(6) = p(5,1)+p(4,2)+p(3,3)+p(2,4)+p(1,5)+p(0,6) = 1+3+p(3)+p(2)+p(1)+1 = 11.$$

**Ferrers diagrams**

Write the partition $\lambda$ of $n$ which has terms $a_1\,a_2\,\ldots\,a_r$ as a sequence of $r$ rows of dots with $a_i$ dots in the $i$-th row. This array is the *Ferrers diagram* of $\lambda$. The columns of such a partition define another partition $\lambda^*$ of $n$, called the *conjugate* of $\lambda$. Clearly $(\lambda^*)^* = \lambda$. $\lambda$ is self conjugate if $\lambda^* = \lambda$.

*Example* 2.2.3. For the partition 4 2 2 1 1 of 10 the conjugate partition is 5 3 1 1.

**Theorem 2.2.4** (Euler, Sylvester)**.** *i) If $\lambda$ has $r$ non-zero terms, then $r$ is the maximum value of the terms of $\lambda^*$. Hence $p(n,k)$ is also the number of partitions for which all the terms are $a_i \leq k$.*

*ii) The number of self conjugate partitions of $n$ is equal to the number of partitions with distinct odd terms.*

*iii) The number of partitions of $n$ with distinct terms is equal to the number of partitions which have odd terms.*

*Example* 2.2.5. The partitions of 9 with distinct terms are $9, 8\,1, 7\,2, 6\,3, 6\,2\,1, 5\,4, 5\,3\,1$ and $4\,3\,2$. These correspond to the partitions with odd terms, namely

$$9, 111111111, 711, 333, 33111, 51111, 531, 3111111.$$

Only 9 and 531 belong to both types, i.e. have odd distinct terms. They correspond to the self conjugate partitions 51111 and 333 respectively.

*Proof of the Theorem.* i) The number $r$ of rows in the Ferrers diagram for $\lambda$ is also the length of the longest column and thus the value of the maximum term for $\lambda^*$. $p(n, k)$ counts all those partitions of $n$ with $r \leq k$. $\lambda$ with $\leq k$ terms, or $\lambda^*$ with al terms $\leq k$.

ii) For a self conjugate partition the Ferrers diagram is symmetric about the diagonal. (compare the partition 4 4 3 2 of 13). Combining the $i$-th row and $i$-th term to a term, gives a partition of $n$ of odd terms only. The process can be reversed: all partition of odd terms can be drawn as a symmetric diagram and hence lead to a self conjugate partition.

(In the example: 7 5 1).

iii) We give a bijection between the partitions with distinct terms and the partitions with odd terms.

- If a partition of $n$ has distinct terms, each $a_i$ can be uniquely written in the form $a_i = 2^{u_i} v_i$, where $v_i$ is odd. Now collect all terms with the same $v_i$: $a_{i_1}, \ldots, a_{i_t}$ all have the same $v_{i_j} = v_i$. Put $w_i = \sum_{i=1}^{t} 2^{u_{i_j}}$. Then $\lambda$ corresponds to the partition $\mu$ of $n$ which has $w_i$ many copies of $v_i$, for each of the odd numbers $v_i$.
- Conversely, given $\mu$ each $w_i$ has a unique binary expansion $\sum_{j=1}^{t} 2^{u_{i_j}}$ and the set $2^{u_{i_j}} v_i$ gives a partition $\lambda$ of $n$ of distinct terms. Since the correspondence between $\lambda$ and $\mu$ is bijective, the theorem follows.

Example: Let $33 = 12 + 8 + 6 + 4 + 3$ be a partition of distinct terms. Order these terms according to the odd number $v_i$. $12 = 4 \times 3, 6 = 2 \times 3, 3 = 1 \times 3$. $8 = 8 \times 1, 4 = 4 \times 1$.
So $w_3 = 4 + 2 + 1 = 7 = 111_2$ (in binary).
and $w_1 = 8 + 4 = 12 = 1100_2$. So the partition above induces the partition of 7 copies of 3 and 12 copies of 1, which is a partition of odd terms only.

Conversely, given the partition of 7 copies of 3, and 12 copies of 1. Write $7 = 111_2$ and $12 = 1100_2$ in binary. Finally, $2^2 \times 3 = 12, 2^1 \times 3 = 6, 2^0 \times 3 = 3$ and $2^3 \times 1 = 8, 2^2 \times 1 = 4$ gives the partition of distinct integers.

□

**Generating functions**

Suppose that a partition $\lambda$ of $n$ contains $s_1$ copies of 1, $s_2$ copies of 2 etc. up to $s_k$ copies of $k$.

We observe that the additive partition $s_1 \times 1 + s_2 \times 2 + \ldots + s_k \times k = n$ can be rewritten as follows:

$$x^{s_1 1} x^{s_2 2} \ldots x^{s_k k} = x^n.$$

Further recall the geometric series:

$$\frac{1}{1-x^t} = 1 + x^t + x^{2t} + x^{3t} + \ldots.$$

Now the coefficients $c_n$ of the function

$$P_k(x) = \prod_{t=1}^{k} \frac{1}{1-x^t} = \prod_{t=1}^{k}(1 + x^t + x^{2t} + x^{3t} + \ldots) = \sum_{n=0}^{\infty} c_n x^n$$

are the number of ways to write $n$ as a sum of $\leq k$ integers, i.e. the number of ways to write is a sum of integers $\leq k$. (by Theorem 2.2.4 i). This number is: $c_n = p(n,k)$. If $k$ tends to infinity this gives:

$$P(x) = \prod_{t=1}^{\infty} \frac{1}{1-x^t} = \prod_{t=1}^{\infty}(1 + x^t + x^{2t} + x^{3t} + \ldots) = \sum_{n=0}^{\infty} p(n)x^n,$$

since here the coefficient is the number of ways to write $n$ as a sum of smaller integers.

These functions are called generating functions, because their coefficients generate the object we are interested in. This is a rather algebraic approach. One does not care too much about convergence. However, the geometric series is convergent if and only if $|x| < 1$.

*Example* 2.2.6.

$$\begin{aligned} & \frac{1}{1-x}\,\frac{1}{1-x^2}\,\frac{1}{1-x^3} \\ = \; & (1 + x + x^2 + x^3 + x^4 + x^5 + \ldots)(1 + x^2 + x^4 + x^6 + \ldots)(1 + x^3 + x^6 + \ldots) \\ = \; & 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + \ldots. \end{aligned}$$

Here the coefficients count the number of ways to write $n$ as a sum of ones, twos and threes.

$$\begin{aligned}
&\prod_{t=1}^{\infty}\frac{1}{1-x^t} = \frac{1}{1-x}\,\frac{1}{1-x^2}\,\frac{1}{1-x^3}\,\frac{1}{1-x^4}\,\frac{1}{1-x^5}\cdots \\
= \;& (1+x+x^2+x^3+x^4+x^5+\ldots)(1+x^2+x^4+\ldots)(1+x^3+x^6+\ldots)\times \\
& \times(1+x^4+\ldots)(1+x^5+\ldots)\ldots \\
= \;& 1+x+2x^2+3x^3+5x^4+7x^5+\ldots.
\end{aligned}$$

Here the coefficients count the number of partitions of $n$.

**Remark**. Many important but difficult results have been proved about partitions.

i) Euler proved:

$$p(n) = p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)\ldots$$

where $p(n-i)$ occurs, if $i$ can be written as $\frac{1}{2}l(3l\pm 1)$, (for an integer $l$) and the sign is $(-1)^{l+1}$. So, $l=1$ gives $i=1$ and 2. $l=2$ gives $i=5$ and 7 etc.

ii) Hardy and Ramanujan proved that

$$p(n) \sim \frac{\exp(\pi\sqrt{\frac{2n}{3}})}{4\sqrt{3}n}.$$

For comparison: $p(1000000) \approx 1.471685 \times 10^{1107}$, whereas the approximation gives $1.4723 \times 10^{1107}$. Better approximations, and even exact formulae, are known.

## 2.3 Partitions of finite sets

*Definition* 2.3.1. A partition of $M_n$ is a division of it into disjoint non-empty subsets. The number of these partitions with exactly $r$ non-empty subsets is denoted by $S(n,r)$, which is called *Stirling number of the second kind.*

| $n\backslash r$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 0 | 0 | 0 | 0 |
| 3 | 1 | 3 | 1 | 0 | 0 | 0 |
| 4 | 1 | 7 | 6 | 1 | 0 | 0 |
| 5 | 1 | 15 | 25 | 10 | 1 | 0 |
| 6 | 1 | 31 | 90 | 65 | 15 | 1 |

Let us state some elementary properties about these numbers:

i) The number of surjections from $M_n$ onto $M_r$ is $S(n,r)r!$.

ii) $S(n,1)=1, S(n,2)=2^{n-1}-1$ (count the number of pairs of complementary nonempty subsets).

iii) $S(n,n)=1, S(n,n-1)=\binom{n}{2}=\frac{n(n-1)}{2}$, i.e. the number of ways to choose a 2-element subset of an $n$-element set.

iv) Define $S(0,0)=1, S(n,0)$ and $S(n,r)=0$, if $r>n$.

**Theorem 2.3.2.** *i) For every $n,r\in\mathbb{N}: S(n+1,r)=S(n,r-1)+rS(n,r)$.*

*ii) For every $n\in\mathbb{N}: x^n=\sum_{r=1}^{n} S(n,r)x(x-1)\dots(x-r+1)$.*

*iii) For every $n,r,k\in\mathbb{N}: k^n=\sum_{r=1}^{n} S(n,r)r!\binom{k}{r}=\sum_{r=1}^{k} S(n,r)r!\binom{k}{r}$.*

*Proof.* i) For each partition of $M_{n+1}$ into $r$ subsets, the element $n+1$ either forms its own set or it belongs to a subset containing other elements. In the first case, there are $S(n, r-1)$ partitions. In the second case, each of the $S(n,r)$ partitions of $M_n$ into $r$ sets allows $r$ possibilities to allocate the element $n+1$ to any of the $r$ sets.

ii) We use induction. As an abbreviation we introduce the following notation:

$$(x)_r = x(x-1)\dots(x-r+1).$$

For $n=1$:

$$x^1 = S(1,1)(x)_1 = x.$$

Assume (as induction hypothesis) that $x^n = \sum_{r=1}^n S(n,r)(x)_r$. Then

$$x^{n+1} = x^n \times x = \sum_{r=1}^{n}(x)_r((x-r)+r)S(n,r).$$

Since $(x)_r\,(x-r) = (x)_{r+1}$ we have

$$\begin{aligned} x^{n+1} &= \sum_{r=1}^{n} S(n,r)(x)_{r+1} + \sum_{r=1}^{n} rS(n,r)(x)_r \\ &= \sum_{r=1}^{n+1} \left(S(n,r-1) + r(S(n,r)\right)(x)_r \\ &\phantom{=} \text{ here we used: } S(n,0) = S(n,n+1) = 0. \\ &= \sum_{r=1}^{n+1} S(n+1,r)(x)_r, \end{aligned}$$

which proves the claim.

iii) Follows from ii) with $x = k : k(k-1)\dots(k-r+1) = r!\binom{k}{r}$, and as $S(n,r) = 0$ if $r > n$ and $\binom{k}{r} = 0$, if $k < r$.

□

**Remark.** i) As kind of converse to part ii) of the Theorem: There are uniquely defined constants $s(n,r)$ such that

$$x(x-1)\dots(x-r+1) = \sum_{r=1}^{n}(-1)^{n-r}s(n,r)x^r.$$

These are the Stirling numbers of the first kind. (We do not use them in the lecture otherwise).

ii) A generating function for $\frac{S(n,r)}{n!}$ is $\frac{1}{r!}(e^x-1)^r$. Example: For $k=r$:

$$\frac{1}{3!}(e^x-1)^3 = \frac{x^3}{6}+\frac{x^4}{4}+\frac{5x^5}{24}+\frac{x^6}{8}+\dots.$$

Multiplying $x^i$ by $i!$ gives the coefficients in the third column of the table: $1, 6, 25, 90, \dots$.

**Multinomial Coefficients**

These are a useful generalization of the binomial coefficients.

*Definition* 2.3.3. Let $n=\sum_{i=1}^t n_i$. Let us define the multinomial coefficient

$$\binom{n}{n_1,n_2,\dots,n_t} := \frac{n!}{n_1!n_2!\dots n_t!}.$$

Observe that the binomial coefficient $\binom{n}{n_1}$ corresponds in this notation to $\binom{n}{n_1,n-n_1}$.

**Theorem 2.3.4.** *i) The number of partitions of $M_n$ into $t$ disjoint subsets of size $n_i \in \mathbb{N}_0$ (i.e. $\sum_{i=1}^t n_i = n$) is $\binom{n}{n_1,n_2,\dots,n_t}$.*

*ii) The coefficient of $\prod_{i=1}^t x_i^{n_i}$ in the expansion of $(x_1+x_2+\dots+x_t)^n$ is $\binom{n}{n_1,n_2,\dots,n_t}$.*

*iii) The number of permutations of $n$ balls of which $n_i$ have colour $i$ (and are indistinguishable otherwise) is $\binom{n}{n_1,n_2,\dots,n_t}$.*

*Proof.* i) There are $\binom{n}{n_1}$ choices for the elements of $X_1$, then $\binom{n-n_1}{n_2}$ choices for $X_2$, etc., up to $\binom{n_t}{n_t}$ choices for $X_t$. Multiplying these together gives the claim:

$$\binom{n}{n_1} = \frac{n!}{n_1!(n-n_1)!}, \qquad \binom{n}{n_1}\binom{n-n_1}{n_2} = \frac{n!}{n_1!n_2!(n-n_1-n_2)!}$$

etc.

ii) When multiplying the brackets, and counts how often $\prod_{i=1}^n x_i^{n_i}$ occurs, one actually partitions the $n$ elements into parts. As in part i). There is a bijection between the partitions and the products $\prod_{i=1}^n x_i^{n_i}$. So the result follows.

iii) If for a given permutation the balls of colour $i$ have the positions $i_1, i_2, \dots, i_{n_i}$, put these numbers into the set $X_i$. There is a bijection between the permutations and the partitions counted in i) into parts $X_1$ of size $n_1$.

□

*Example* 2.3.5. i) For $n = 4, t = 3$: $\binom{4}{3,1,0} = 4$ counts the partitions of the type $\{a, b, c\}, \{d\}, \emptyset$. (There are 4 choices for $d$, then everything else is fixed). $\binom{4}{2,1,1} = 12$ counts the partitions of the type $\{a, b\}, \{c\}, \{d\}$. (There are 4 choices for $d$, then three for $c$, then everything else is fixed. Or: there are $\binom{4}{2} = 6$ choices for $\{a, b\}$, then 2 for $c$. Note: the order of $a, b$ does not matter. But order of $c$ and $d$ does.

ii)

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

$$(x+y+z)^3 = x^3+y^3+z^3+3x^2y+3x^2z+3y^2z+3xy^2+3xz^2+3yz^2+6xyz.$$

Note that

$$\binom{3}{3,0,0} = 1, \binom{3}{2,1,0} = 3, \binom{3}{1,1,1} = 6.$$

The sum of the coefficients in the second example is $3^3 = 27$.

iii) How many ways are there to arrange the letters $ASSESS$ to give different "words". (Assume that various copies of the letter $S$ are identical. Also do not care whether the rearranged "words" have any meaning.) There are 6 letters, 4 of them the same, and then two single letters $A, E$:

$$\binom{6}{4,1,1} = \frac{6!}{4!1!1!} = 30.$$

For $ASSETS$ it is:

$$\binom{6}{3,1,1,1} = \frac{6!}{3!1!1!1!} = 120.$$

# 3 Finite mathematical structures

## 3.1 Latin squares

### Finite fields

For each $n \geq 2$ the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, with usual addition and multiplication modulo $n$ is a ring. The zero element is 0, and the multiplicative identity is 1. When $n$ is composite, say $n = ab$, there are zero divisors, i.e. nonzero factors whose product is zero: $ab = 0$. So, for composite $n$, $(\mathbb{Z}_n < +, \cdot)$ is not an integral domain. The elements of $\mathbb{Z}_n$ which are coprime to $n$, i.e. $\gcd(a, n) = 1$, are invertible, i.e. there is a $b \in \mathbb{Z}_n$ with $ab = 1$.
Define $\mathbb{Z}_n^*$ to be the set of invertible elements of $\mathbb{Z}_n$, so that $|\mathbb{Z}_n^*| = \varphi(n)$ (Euler's $\varphi$ function). In $n = p$ is prime, all the elements, except for 0, are invertible: i.e. there $\mathbb{Z}_p$ is a finite field. (In a field all elements, but zero, have an inverse). $|\mathbb{Z}_p^*| = p - 1$.
In general, for every prime power $p^k$ there is an essentially unique finite field of $p^k$ elements, often called: GF$(p^k)$ (GF for Galois field) or $\mathbb{F}_{p^k}$. Note that for $k > 1$ this field is NOT the same as $\mathbb{Z}_{p^k}$, as here $pp^{k-1} = 0$, so that $p$ is a zero divisor, which implies that $p$ is not invertible. GF$(p^k)$ is actually a $k$-dimensional vector space over $\mathbb{Z}_p$.
The $p^k - 1$ non-zero elements $\alpha$ have the following properties:
adding them $p$ times: $\alpha + \alpha + \ldots + \alpha = p\alpha = 0$.
They form a multiplicative cyclic group, which means there is a generating element $\theta$, such that each non-zero element can be written as $\alpha = \theta^i$, for some exponent $i \in \{0, 1, \ldots, p^k - 2\}$.
The set of invertible elements (i.e the non-zero elements) is also called $\mathbb{F}_{p^k}^*$.

**Latin Squares**

*Definition* 3.1.1. Let $S = \{s_1 \ldots, s_n\}$ be a set of $n$ symbols. A Latin square of order $n$ is an $n \times n$-array in which each symbol $s_i inS$ occurs exactly once in each row, and exactly once in each column.

Historically, one used letters for these $n$ symbols, (Latin alphabet), which explains the name Latin squares. Today one prefers the integers from 0 to $n-1$:

*Definition* 3.1.2. A Latin square is in standard form if its symbols are $0, 1, \ldots, n-1$ and the first row is $0, 1, \ldots, n-1$. Moreover, the Latin square is in canonical form if the first column is also $0, 1 \ldots, n-1$.

*Example* 3.1.3.

It is always possible to transform any Latin square by a change of rows and columns into standard and even canonical form. Each canonical form corresponds to $(n-1)!$ many Latin squares in standard forms, and each in standard form corresponds to $n!$ in general form. (So altogether each canonical form corresponds to $n!(n-1)!$ Latin squares.
The number of Latin squares of a given order is very large. We concentrate on a few simple methods to construct Latin squares.
The number of latin squares of size 1 is: 1
The number of latin squares of size 2 is: 2
The number of latin squares of size 3 is: 12
The number of latin squares of size 4 is: 576
The number of latin squares of size 5 is: 161280
The number of latin squares of size 6 is: 812851200

We number the rows and columns also from 0 to $n-1$. The $i, j$-entry is the entry in row $i$ and column $j$.

**Construction of Type 1:**
For any $n \geq 2$, let $a$ be an invertible element in $\mathbb{Z}_n$, (i.e. $\gcd(a, n) = 1$). Define an $n \times n$ array $L(a)$ using the symbols of $\mathbb{Z}_n$ by taking the $i, j$-entry to be $ai+j \bmod n$.
Claim: $L(a)$ is a Latin square.
Suppose there is twice the same entry in row $i$:

$$ai + j_1 \equiv ai + j_2 \bmod n \Rightarrow j_1 = j_2.$$

Or suppose there is twice the same entry in column $j$:

$$ai_1 + j = ai_2 + j \bmod n \Rightarrow i_1 = i_2,$$

since $a$ is invertible.
So, the number of Latin squares of this type in standard form is $\varphi(n)$.

*Example* 3.1.4.

$$L(1) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 2 & 3 & 0 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 0 & 1 & 2 \\ \hline \end{array} \qquad L(3) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 3 & 0 & 1 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 1 & 2 & 3 & 0 \\ \hline \end{array}$$

Note: Clearly $L(1)$ is in canonical form. Moreover it is the addition table for $\mathbb{Z}_n$, the $i,j$-entry being $i + j$.

**Construction of Type II**

A similar construction, which can be applied to any finite field $\mathrm{GF}(p^k) = \mathbb{F}_{p^k}$. Label the rows and columns by $\{0, 1, \theta, \theta^2 \ \ldots, \theta^{p^k-2}\}$ (see above). Each non-zero element $\alpha$ defines an array $M(\alpha)$ for which the $i,j$-entry is $\alpha i + j$ (as an element of $\mathbb{F}_{p^k}$). The proof that this defines a Latin square is the same as above. $M(1)$ is the addition table of the field. If the elements of the field in the order above are replaced by the symbols $0, \ldots, n-1$ of $\mathbb{Z}_n$, then $M(1)$ is in canonical form, and $M(\alpha)$ is in standard form for every $\alpha$.

*Example* 3.1.5. $p^k = 2^2 = 4$. $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$. Moreover $\theta^3 = 1$, which implies via $0 = \theta^3 - 1 = (\theta - 1)(\theta^2 + \theta + 1)$ that $\theta^2 = \theta + 1$. (Note that one works modulo 2, so $+1 = -1$.

$$M(1) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & \theta & \theta^2 \\ \hline 1 & 0 & \theta^2 & \theta \\ \hline \theta & \theta^2 & 0 & 1 \\ \hline \theta^2 & \theta & 1 & 0 \\ \hline \end{array} \qquad M(\theta) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & \theta & \theta^2 \\ \hline \theta & \theta^2 & 0 & 1 \\ \hline \theta^2 & \theta & 1 & 0 \\ \hline 1 & 0 & \theta^2 & \theta \\ \hline \end{array} \qquad M(\theta^2) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & \theta & \theta^2 \\ \hline \theta^2 & \theta & 1 & 0 \\ \hline 1 & 0 & \theta^2 & \theta \\ \hline \theta & \theta^2 & 0 & 1 \\ \hline \end{array}$$

$$M(1) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array} \qquad M(\theta) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline \end{array} \qquad M(\theta^2) = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline \end{array}$$

The addition and multiplication tables of the finite field with 4 elements are as follows:

| $+$ | $0$ | $1$ | $\theta$ | $\theta^2$ |
|---|---|---|---|---|
| $0$ | | | | |
| $1$ | | | | |
| $\theta$ | | | | |
| $\theta^2$ | | | | |

| $\cdot$ | $0$ | $1$ | $\theta$ | $\theta^2$ |
|---|---|---|---|---|
| $0$ | | | | |
| $1$ | | | | |
| $\theta$ | | | | |
| $\theta^2$ | | | | |

Recall that $\theta^2 = \theta + 1$.

*Definition* 3.1.6. i) A Latin square is diagonal, if both of the diagonals contain all $n$ different symbols exactly once each.

ii) Two Latin square $A, B$ of order $n$ are orthogonal, if all $n^2$ ordered pairs $(a_{ij}, b_{ij})$ are all different. (This means: all ordered pairs of symbols occur exactly once).

iii) A Latin square is self-orthogonal, if it is orthogonal to its transpose. (The transpose is clearly also a Latin square).

*Example* 3.1.7. **diagonal**: $n = 4$. $M(\theta), M(\theta^2)$, but not $M(1), L(1), L(3)$.
**orthogonal**: $L(1), L(2)$, when $n = 2$. $M(1), M(\theta), M(\theta^2)$, but not $L(1), L(3)$, for $n = 4$. For $n = 5$: $L(1), L(2), L(3), L(4)$ are **mutually orthogonal**, which means that any pair of squares are orthogonal.
**self-orthogonal**: $M(\theta), M(\theta^2)$ for $n = 4$.

**Theorem 3.1.8.** *There are at most $n-1$ Latin squares of order $n$ which are mutually orthogonal.*

*Proof.* Assume w.l.o.g. they are in standardform. For the entry $a_{1,0}$ there are at most $n-1$ symbols available, since 0 is not possible. □

*Definition* 3.1.9. A Magic square of order $n$ is an $n \times n$ array of the integers $1, 2, \ldots, n^2$ in some order, such that the sum of the entries in each row, column and diagonal is the same, and thus equals $n(\frac{n^2+1}{2})$.

*Example* 3.1.10.

| | | | |
|---|---|---|---|
| 1 | 8 | 13 | 12 |
| 14 | 11 | 2 | 7 |
| 4 | 5 | 16 | 9 |
| 15 | 10 | 3 | 6 |

Note that also "broken" diagonals sum up to 34. This property is called pandiagonal.

**Theorem 3.1.11.** *i) For any $n \geq 2$: $L(a)$ and $L(b)$ are orthogonal if and only if $a-b$ is invertible in $\mathbb{Z}_n$. If $n = p^k$ the Latin squares $M(\alpha)$ and $M(\beta)$ are orthogonal if and only if $\alpha \neq \beta$. If $n = p$ is prime, then $L(1), \ldots, L(p-1)$ is a maximal set of mutually orthogonal Latin squares. If $n = p^k$, then the $M(\alpha)$ form a maximal set of $p^k - 1$ mutually orthogonal Latin squares.*

*ii) For any $n \geq 2$: $L(a)$ is diagonal if and only if $a^2 - 1$ is coprime to $n$, and in that case $L(a)$ is also self-orthogonal.*
*If $n = p^k$, then $M(\alpha)$ is diagonal and self-orthogonal except when $\alpha = \pm 1$ in $\mathbb{F}_{p^k}$.*

*iii) If $A, B$ are orthogonal diagonal Latin squares of order $n$ with $ij$ - entries $a_{ij}, b_{ij} \in \mathbb{Z}_n$ respectively, then the $n \times n$ array $C$ whose $ij$ - entry is $c_{ij} = na_{ij} + b_{ij} + 1$ is a Magic square of order $n$.*

*Proof.* i) Two of the ordered pairs $(a_{ij}, b_{ij})$, $(a_{uv}, b_{uv})$ from $L(a)$ and $L(b)$ are equal if and only if $ai + j \equiv au + v$ and $bi + j \equiv bu + v \bmod n$, i.e. $j - v \equiv a(u - i) \equiv b(u - i)$, giving $(a - b)(u - i) \not\equiv 0 \bmod n$. So as in the proof that $L(a)$ is a Latin square, if $a - b$ is invertible, then $u \equiv i$ and so $u = i$ and $v = j$. Conversely if $a - b$ is not invertible there is an element $c \in \mathbb{Z}_n \backslash \{0\}$ such that $(a - b)c \equiv 0 \bmod n$ and then the entries at position $(0, 0)$ and $(c, -ac)$ both give the ordered pair $(0, 0)$. The same proof applies to the case when $n = p^k$ and the Latin squares are $M(\alpha)$ and $M(\beta)$, for in the field $\mathbb{F}_{p^k}$ $\alpha - \beta$ is invertible whenever $\alpha \neq \beta$. This explains why there are sets of $n - 1$ mutually orthogonal Latin squares whenever $n$ is a prime or a prime power, given by the $L(a)$ or $M(\alpha)$ corresponding to the invertible elements $a$ or $\alpha$ of the fields $Z_p$ or $F_{p^k}$ respectively.

- The entries on the leading diagonal of $L(a)$ are of the form $ai + i \equiv (a + 1)i \bmod n$, and those on the other long diagonal are congruent to $ai - i - 1 \equiv (a - 1)i - 1 \mod n$ since $j = n - 1 - i$ for these entries. Hence the elements on each diagonal are all distinct if and only if $a + 1$ and $a - 1$ are both invertible in $Z_n$, i.e. their product $a^2 - 1$ is coprime to $n$. The $ij$-entry of $L(a)^T$,the transpose of $L(a)$, is $aj + i$ and therefore as in (i) the entries at positions $i, j$ and $u, v$ are equal if and only if $ai + j \equiv au + v$ and $aj + i \equiv av + u \bmod n$. Multiplying the first congruence by $a$ and subtracting the second gives $(a^2 - 1)(i - u) \equiv 0 \bmod n$. So, if $a^2 - 1$ is coprime to $n$, then $u \equiv i \bmod n$ and hence $u = i$ and $v = j$ as required.

  Since one of any three consecutive integers is divisible by 3 and at least one is even, $a$ and $a^2 - 1 = (a + 1)(a - 1)$ can only both be coprime to $n$ if $n$ is coprime to 6. When $n$ is an odd prime $\geq 5$ : $a - 1$ and $a + 1$ are invertible unless $a = 1$ or $a = n - 1$ respectively and so there are at least two Latin squares $L(a)$ which are diagonal and self - orthogonal in this case. The comments about the situation when $n$ is a prime also apply to the case when $n = p^k$ and the Latin squares are the $M(\alpha)$, for then the diagonal elements are multiples of $\alpha \pm 1$ and these elements of $F_{p^k}$ are invertible except when $\alpha = \mp 1$ respectively. For $n = 4$ both $M(\theta)$ and $M(\theta^2)$ are diagonal and self - orthogonal. So, $n$ being coprime to 6 is a sufficient but not a necessary condition on $n$ for such squares to exist.

iii) Since $a_{ij}, b_{ij} \in Z_n$, these entries are respectively the unique quotient and remainder when $c_{ij} - 1$ is divided by $n$ and as the pairs $(a_{ij}, b_{ij})$ are distinct so are the $c_{ij}$. Moreover $1 \leq c_{ij} \leq n(n - 1) + n = n^2$, whence the $c_{ij}$ are the numbers $1, 2, 3, \dots, n^2$ in some order. From the definition of a Latin square the sum of the entries in each row and column is $(n + 1)[n\frac{n-1}{2}] + n = n\frac{n^2+1}{2}$, and the same applies to both of the long diagonals, whence $C$ is a Magic square of order $n$.

□

From the statements in the proofs of (i) and (ii) the above construction shows that a Magic square of order $n$ exists for all integers $n$ coprime to 6 and for every prime power $p^k$ with $k \geq 2$. A slight modification of the Theorem part (iii) proves that a Magic square exists for every odd order, for the condition that the Latin squares $A, B$ are diagonal can be dropped so long as the sum of the diagonal elements is $\frac{n(n-1)}{2}$.

A simple construction for Latin squares of odd size is as follows: Go $n$ steps in the same direction, here one to the right and one to the top. Reduce modulo $n$, ie. if you leave the grid to the top reenter at the bottom, if you leave to the right, reenter at the left. then make one move, here one to the bottom and place the next $n$ symbols etc.

| | | | | |
|---|---|---|---|---|
| 1 | 8 | 15 | 17 | 24 |
| 7 | 14 | 16 | 23 | 5 |
| 13 | 20 | 22 | 4 | 6 |
| 19 | 21 | 3 | 10 | 12 |
| 25 | 2 | 9 | 11 | 18 |

The following Latin square is famous because it appears in Albrecht Dürer's picture Melancholia from 1514. Not only the diagonals add up to 34, not only the broken diagonals, but even more, whenever one adds an entry and the centrally symmetric entry, the sum is 17.

| | | | |
|---|---|---|---|
| 16 | 3 | 2 | 13 |
| 5 | 10 | 11 | 8 |
| 9 | 6 | 7 | 12 |
| 4 | 15 | 14 | 1 |

**Remark**. Euler posed a problem involving six officers of different ranks from different regiments which is equivalent to finding a pair of orthogonal Latin squares of order 6. Tarry proved in 1900 that there is no solution. It had been conjectured that there wouldn't be pairs of Latin square of size $10, 14, n \equiv 2 \bmod 4$, but this has been disproved using a long computer search. However, it is not known whether there are 3 mutually orthogonal Latin squares of order 10. This is out of the range of today's computers.

Another open problem: are there 11 mutually orthogonal Latin squares of order 12? It is conjectured that the answer is no.

## 3.2 Block Designs

*Definition* 3.2.1. A Block Design $D$ consists of a set $S$ with $v$ elements and a collection of $b$ distinct subsets $B_i$ of $S$ called blocks, each containing $k$ elements. This design has the additional property that there are integers $t$ and $\lambda$ such that every subset $T$ of $S$ with $t$ elements is contained in exactly $\lambda$ of the blocks $B_i$. $D$ is called a $t - (v, k, \lambda)$ design.

Clearly from the definitions $t \leq k \leq v$ and $\lambda \leq b \leq \binom{v}{k}$. We assume that $t \geq 1, \lambda \geq 1$ and $1 < k < v$ (which avoids very special cases only). It can be proved that every $t$ - design is also a $(t-1)$ - design (see the book by Biggs), but finding examples with $t \geq 3$ is not easy. Since the case $t = 1$ is rather trivial this course will concentrate on the case when $t = 2$. This is sometimes called a Balanced Incomplete Block Design (BIBD), 'balanced' from the existence of $\lambda$ and 'incomplete' since $k < v$.

**Theorem 3.2.2.** *Suppose that $D$ is a $2 - (v, k, \lambda)$ design with $1 < k < v$. Then*

*i)* $\lambda v(v-1) = bk(k-1)$*;*

*ii) each $x \in S$ belongs to exactly $r$ of the blocks where $\lambda(v-1) = r(k-1)$;*

*iii)* $vr = bk$*.*

*Proof.* Here we use again the technique of double counting that was for example used for Euler's upper bound on the number of edges of a plana graph. The same object is counted twice.

i) Count all the pairs of sets $B_i, \{x, y\}$ where $x, y \in B_i$. The number of $\{x, y\}$ is $\frac{v(v-1)}{2}$ and each belongs to $\lambda$ of the $B_i$, giving $\lambda\frac{v(v-1)}{2}$ pairs in total. But each of the $b$ sets $B_i$ contains $\frac{k(k-1)}{2}$ subsets with two elements, so the number of pairs is also $b\frac{k(k-1)}{2}$, whence the result.

Another way to express this: Define a matrix $A$ with $b$ rows and $\binom{v}{2}$ columns. Whenever a pair of points $(x, y)$ lies on the block $i$, the entry of $a_{i,(x,y)}$ is 1, and 0 otherwise. Each column contains $\lambda$ ones. Each row contains $\binom{k}{2}$ ones. So $\lambda\binom{v}{2} = b\binom{k}{2}$.

ii) Suppose that a given $x \in S$ belongs to exactly $r(x)$ of the blocks $B_i$. For this $x$ count the number of pairs $B_i, y$ where $x, y \in B_i$ but $y \neq x$. As in (i) each of the $v - 1$ choices for $y$ gives a pair $\{x, y\}$ which belongs to $\lambda$ of the $B_i$, while each of the $r(x)$ sets $B_i$ containing $x$ has $k-1$ choices for $y$. Therefore $\lambda(v-1) = r(x)(k-1)$, and as $v, k$ and $\lambda$ are fixed and $k \neq 1$, $r(x)$ must have the same value $r$ for every $x \in S$, whence the formula.

iii) Counting the pairs $B_i, x$ where $x \in B_i$, each of the $v$ elements $x$ belongs to $r$ blocks $B_i$ while each of the $b$ blocks $B_i$ contains $k$ elements $x$, whence $vr = bk$.

□

**Remark**. (a) From (i) and (ii) of the Theorem, $b$ and $r$ are uniquely defined by the values of $v, k$ and $\lambda$, with $\lambda < r < b$ when $1 < k < v$. Despite this dependence a 2 - design is often called a $(b, v, r, k, \lambda)$ design, with all five parameters being included. In general $\lambda \leq k \leq r \leq v \leq b$; see the Theorem below, part (iii).
(b) Even if $b, v, r, k, \lambda$ satisfy the conditions of the last Theorem there may be no block designs with these parameters; see Theorem 3.2.5.

*Definition* 3.2.3. An *incidence matrix* of a $2-(v,k,\lambda)$ design D is a $b \times v$ matrix $A = (a_{ij})$ where for each $x_j \in S, a_{ij} = 1$ if $x_j \in B_i$ and $a_{ij} = 0$ otherwise. Since neither $S$ nor the $B_i$ have a 'natural' ordering, the matrix $A$ is not uniquely defined by $D$ unless or until such orderings are imposed. A $2-(v,k,\lambda)$ design is *symmetric* if $b = v$, and therefore $r = k$ from Theorem 3.2.2 (iii) ; many of the more interesting and useful designs such as that of Example (i) below have this property. Although an incidence matrix of a symmetric design must be a square matrix it does need not to be a symmetric matrix.

*Example* 3.2.4. i) Let $S = M_7$ and define the blocks $B_i, (i = 1, 2, \ldots, 7)$ to be $B_1 = \{1,2,4\}, B_2 = \{2,3,5\}, B_3 = \{3,4,6\}, B_4 = \{4,5,7\}, B_5 = \{5,6,1\}, B_6 = \{6,7,2\}$ and $B_7 = \{7,1,3\}$. These form a symmetric $2-(7,3,1)$ design with $b = v = 7$ and $r = k = 3$. The incidence matrix $A_1$ with the block order given above is:

$$A_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Although it is not symmetric, reversing the row order gives a symmetric matrix.

ii) For every $v \geq 3$ there is a $2-(v,2,1)$ design for which the blocks are all the 2 - element subsets of the set $S$. Thus $b = \frac{v(v-1)}{2}, r = (v-1)$ and the design is not symmetric when $v \geq 4$. One incidence matrix $A_2$ when $v = 4$ is as follows, (but there are many more).

$$A_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

iii) Consider the $3 \times 3$ array $C$ shown below. Let $S = M_9$ and define the blocks by taking the three rows, $\{1,2,3\}, \{4,5,6\}, \{7,8,9\}$ the three columns, $\{1,4,7\}, \{2,5,8\}, \{3,6,9\}$ the two 'long' diagonals and the four 'broken' diagonals: $\{1,5,9\}, \{2,6,7\}, \{3,4,8\}$ and $\{1,6,8\}, \{2,4,9\}, \{3,5,7\}$. These form a $2-(9,3,1)$ design with $b = 12$ and $r = 4$.

$$C = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

**Remark**. Examples i) and ii) are special cases of two general classes of designs which arise from finite geometries as described in the next section.

**Theorem 3.2.5.** *Let $A$ be an incidence matrix of a $2-(v,k,\lambda)$ design $D$ with parameters $b, v, r, k, \lambda$. Then*

*i) $A^T A = (r-\lambda)I_v + \lambda J_v$ where $I_v$ is the $v \times v$ identity matrix and $J_v$ is the $v \times v$ matrix for which all the entries are 1, i.e. the leading diagonal entries of $A^T A$ are $r$ and the rest are $\lambda$.*

*So the matrix of size 3 looks like*

$$\begin{pmatrix} r & \lambda & \lambda \\ \lambda & r & \lambda \\ \lambda & \lambda & r \end{pmatrix}.$$

*ii) $det(A^T A) = kr(r-\lambda)^{v-1}$.*

*iii) Fisher's Theorem (1940) If $1 < k < v$ is assumed (as usual) then $v \leq b$.*

*iv) If the design is symmetric with $1 < k < v$, then $A^T$ commutes with $A$ and $|B_s \cap B_t| = \lambda$ if $s \neq t$. If in addition $v$ is even then $k - \lambda$ must be the square of an integer.*

*Proof.* i) Since the $ij$-entry of $A^T$ is $a_{ji}$ the $st$-entry of $A^TA$ is $\sum a_{si}a_{it}$. If $s \neq t$ this sum over $i$ counts the number of blocks $B_i$ containing both $x_s$ and $x_t$ and is therefore equal to $\lambda$. If $s = t$ it counts the number of $B_i$ containing $x_s$ which from Theorem 3.2.2 (ii) is $r$ for each $s$. Therefore the leading diagonal entries of $A^TA$ are $r$ and the rest are $\lambda$, as stated.

ii) Adding or subtracting rows and columns of a matrix to others does not change its determinant. When the first row of $A^TA$ is subtracted from the rest the resulting matrix is diagonal apart from the first row and column. Then adding the other columns to the first gives a triangular matrix with $r+(v-1)\lambda$ as the first diagonal entry and $(r-\lambda)$ for the rest. The determinant of $A^TA$ is the product of these entries and since the first entry is $kr$ from Theorem 3.2.2 (ii) the result follows.

iii) Assuming that $1 < k < v$ so that $\lambda < r$ from Theorem 3.2.2 (ii) $A^TA$ is a $v \times v$ matrix with a non - zero determinant whence from matrix theory $v =$ rank $(A^TA) \leq$ rank $A \leq$ (Number of rows of $A$)$= b$.

iv) If the design is symmetric so that $b = v$ and $r = k$, then from the definition of a design the $v \times v$ matrix $A$ satisfies $AJ_v = kJ_v$, $J_vA = rJ_v = kJ_v$. Also $A^TA = (k-\lambda)I_v + \lambda J_v$ from (i) whence $A(A^TA) = (k-\lambda)A + \lambda A = (A^TA)A$. But from (ii), assuming that $1 < k < v$ again, **rank** $A = v$ and $A$ is invertible whence $AA^T = (AA^TA)A^{-1} = (A^TA)AA^{-1} = A^TA$ as required. This result implies that if $s \neq t$ the $st$ - entry $a_{sj}a_{jt}$ of $AA^T$, which counts the number of elements $x_j$ belonging to both $B_s$ and $B_t$, is also $\lambda$. (The diagonal elements of $AA^T$ are $k = |B_s| = r$.) Finally $(\det A)^2 = \det(A^TA) = k^2(k-\lambda)^{v-1}$, so if $v$ is even and $v-1$ is odd, then from the unique factorization of integers $k - \lambda$ must be the square of an integer.

□

Note: Part (iii) and the last result of (iv) exclude several sets of parameters which satisfy Theorem 3.2.2.

## 3.3 The construction of block designs

### Difference Sets

*Definition* 3.3.1. A subset $C$ consisting of $k$ elements of $\mathbb{Z}_v$ where $v \geq 3$ and $1 < k < v$ is a *difference set* in $\mathbb{Z}_v$ if every non - zero element $d$ of $Z_v$ occurs exactly $\lambda$ times as a difference $x - y$ where $x, y \in C$. Counting the pairs $\{x, y\}$ gives $\lambda(v-1) = k(k-1)$ as in Theorem 3.2.2 (ii), so that $\lambda < k < v$. Since $\mathbb{Z}_v$ is an additive cyclic group $C$ is called a *cyclic difference set.* If $\lambda = 1$ it is called a *perfect difference set.*

Every difference set $C$ generates a symmetric $2 - (v, k, \lambda)$ design $D$ on $S = \mathbb{Z}_v$ by defining the blocks $B_i$ to be the sets $C + i = \{c + i; c \in C\}$ for each $i \in \mathbb{Z}_v$. Clearly each block, being a 'shift' of $C$, is also a difference set. If $a, b \in \mathbb{Z}_v$ and $a - b = d = x - y$ where $x, y \in C$ then $a, b \in B_i$ where $i = a - x = b - y$. Hence $a, b$ belong to $\lambda$ of the blocks $B_i$ as required, each corresponding to one pair $x, y \in C$.

**Remark**. Difference sets can also be defined in other finite Abelian groups.

*Example* 3.3.2. i) Suppose that $p = 4s + 3, (s \in \mathbb{N})$ is a prime number and let $C$ be the set of quadratic residues in $\mathbb{Z}_p$, i.e. the elements of the form $a^2($ mod $p)$ where $1 \leq a \leq 2s + 1$. Then $C$ is a difference set in $\mathbb{Z}_p$ which gives a $2 - (4s + 3, 2s + 1, s)$ design. $s = 1$ gives the $2 - (7, 3, 1)$ design of section 3.2 with $C = \{1, 2, 4\}$ giving the blocks listed there. The next example $s = 2$ gives a $2 - (11, 5, 2)$ design with $C = \{1, 3, 4, 5, 9\}$. and the third with $s = 4$

gives the example on $v = 19$ points, on the problem sheet.

ii) The perfect difference set $\{0, 1, 3, 9\}$ in $\mathbb{Z}_{13}$ forms a $2 - (13, 4, 1)$ design and the perfect difference set $\{0, 1, 4, 14, 16\}$ in $\mathbb{Z}_{21}$ forms a $2 - (21, 5, 1)$ design. These are related to the designs below.

iii) $\{0, 1, 2, 4, 5, 8, 10\}$ is a difference set in $\mathbb{Z}_{15}$ which gives a $2 - (15, 7, 3)$ design (see below).

**Projective Planes**

The $n$ - dimensional Euclidean geometry $\mathbb{R}^n$, $(n \geq 2)$ has $n$ real coordinates. An $n$ - dimensional projective geometry over the field $\mathbb{K}$ uses $n + 1$ coordinates from $\mathbb{K}$ but assumes that the points $(x, y, z, \ldots, w)$ and $(cx, cy, cz, \ldots, cw)$ are the same for every $c \neq 0$ in $\mathbb{K}$. The point $(0, 0, \ldots, 0)$ is excluded. If $n \geq 2$ and $|\mathbb{K}| = q$ is finite, and thus a prime power from field theory, this geometry is denoted by $PG[n, q]$. When $n = 2$ giving a projective plane the points $(x, y, z)$ have three coordinates from $\mathbb{K}$ and a line is defined by a single linear equation between them. If $|K| = q$ there are $q^2 + q + 1$ points and $q^2 + q + 1$ lines. Each line contains $q + 1$ points and each point lies on $q + 1$ lines. Every pair of distinct points lies on a single line and every pair of distinct lines meets in a unique point. This gives a symmetric 2 - design with the points as $S$ and the lines forming the blocks (strictly the points on them) so that the parameters are $v = q^2 + q + 1, k = q + 1$ and $\lambda = 1$.

*Example* 3.3.3. Again the example of section 3.2 is equivalent to the 'smallest' projective geometry $PG[2, 2]$ which gives the Seven Point Geometry, also called Fanoplane. Define the points to be $A = (1, 0, 0), B = (0, 1, 0), C = (0, 0, 1), D = (1, 1, 0), E = (0, 1, 1), F = (1, 1, 1), G = (1, 0, 1)$ over $\mathbb{Z}_2$. Then the lines are $ABD(z = 0), BEC(x = 0), CDF(x = y), DEG(x + y + z = 0), EFA(y = z), FGB(x = z), GAC(y = 0)$. If the letters are replaced by their 'numerical' values these lines correspond exactly to the blocks given in the previous Examples i). Similarly $PG[2, 3]$ and $PG[2, 4]$ (for which $\mathbb{K}$ is $\mathbb{F}_4$) are 13 and 21 point projective geometries corresponding to the difference sets of Example ii) above.

**Remark**. i) The geometry $PG[n, q]$ also defines a symmetric 2 - design with the elements of $S$ being the points and the $n - 1$ dimensional subspaces forming the blocks. The case $n = 3$ produces a design with $v = q^3 + q^2 + q + 1, k = q^2 + q + 1, \lambda = q + 1$ which for $q = 2$ gives the $2 - (15, 7, 3)$ design of Example iii) above.

ii) It can be proved that every projective plane (or geometry) on $v$ points corresponds to a difference set in $\mathbb{Z}_v$. These are called Singer difference sets, after J. Singer who investigated them in 1930.

**Affine Planes** Every projective plane geometry $PG[2, q]$ has a so - called 'line at infinity' given by the equation $z = 0$. If this line and the points on it are removed the resulting points $(x, y, 1)$ and lines form the affine geometry $AG[2, q]$. This gives a 2 - design with $b = q^2 + q, v = q^2, r = q + 1, k = q$ and $\lambda = 1$ where $S = \mathbb{K}^2$ and the blocks are the lines as before. If the last coordinate $z = 1$ is omitted $AG[2, q]$ corresponds to the 2 - dimensional vector space over the field $\mathbb{K}$, which is used to define the field $GF[p^2]$ when $\mathbb{K} = \mathbb{Z}_p$.

**Remark**. If the above process is reversed by adding a 'line at infinity' $z = 0$ then the corresponding projective geometry is 'recovered'. Also for each $n, q$ there is an affine geometry $AG[n, q]$ related to $PG[n, q]$.