SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Permutation groups and some applications on Graph Theory

av

Joel Åhfeldt

2020 - No K9

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Permutation groups and some applications on Graph Theory

Joel Åhfeldt

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Paul Vaderlind

2020

Contents

1 Introduction

This work is based on projects from the book N.L Biggs, A.T White- Permutation groups and combinatorial structures. It will cover project 4.1 which is about the full automorphism groups of graphs as well as some of 4.2 which is about strongly regular graphs. chapther 1-5 will cover necessary theory with the two projects being solved in chapter 6 and 7 respectively.

2 Permutations

This work will make heavy use of permutations and permutation groups so the first chapter is dedicated towards them. We start with a definition,

Definition 2.1: A permutation is a bijection $\alpha : X \to X$ from a set X to itself.

Thus a permutation is map that rearranges a set as you can see in the following example:

Example 2.2: Let $A = \{1, 2, 3\}$, the function f defined by $f(1) = 2$, $f(2) = 1$ and $f(3) = 3$ is bijection since it maps the set to itself.

We can describe a permutation in several different ways. A easy one is by a permutation scheme were a element is mapped to the on below it, so the permutation from example 2.2 would be represented as:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

A much more compact way of describing a permutation is by using *cycle notation*. In cycle notation we use *cycles* to describe a permutation. The cycle $(a_1, a_2, ..., a_n)$ denotes the permutation that maps a_1 to a_2, a_2 to a_3 and so on with a_n mapping back to a_1 completing the cycle. Any permutation thus consists of one or more cycles. A cycle is categorised by its length, and a cycle of length n is called a n-cycle. With cycle notation the permutation in example 2.3 would be written as (12)(3). This indicates that 1 is mapped to 2 and that 2 is mapped back to 1, completing a cycle. While 3 is mapped to itself. Thus this permutation consists of a 2-cycle and a 1-cycle. Often 1-cycles will be left out without any loss of information if the permuted set is clear from the context. Thus we can only write (12) to describe the given permutation.

Example 2.3: Let α be a permutation that maps the elements 1, 2, 3, 4, 5, 6 to 3, 2, 4, 1, 6, 5 respectively.

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$$

To write α in cycle notation we start by looking at a number and to where its mapped, and then continuing with the number until we finish a cycle. We see that 1 is mapped to 3, 3 is mapped to 4 and 4 is mapped back to 1, so we have a cycle (134). We continue with 2 which is mapped to itself creating a 1-cycle. Finally we see that 5 is mapped to 6 and 6 is mapped back to 5 creating the cycle (56). So we have $\alpha = (134)(56)$.

Cycle notation is however not unique, a permutation can be described in many different ways using cycle notation as we will see in the following section.

2.1 Composition of permutations

This section will aim to cover the composition of permutations.

Let X be a set and α and β be two permutations of this set. The composition $\gamma = \beta\alpha$ is the permutation we get by first permuting by α and then by β. So if for example is the permutation from example 2.3, and β is the permutation:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{pmatrix}$$

Or written in cycle notation we can write this as $\beta = (256)$. The composition $\beta\alpha$ would then be computed by:

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix},$$

where the middle row is the result after α and the final row is the result after the composition $\beta\alpha$. In cycle notation we would write this as $\beta\alpha = (134)(25)$, with (6) being left out as it is an 1-cycle.

3 Groups

This section will cover permutation groups as well as groups in general, establishing some important definitions and theorems. We start with the definition of a group.

Definition 3.1: A group is and ordered pair $(G, *)$ where G is a set and * is a binary operation on G satisfying the following axioms:

1. $(a * b) * c = a * (b * c)$ for all a,b,c∈G.
2. There exists an element e in G, called the identity of G such that for all g∈G we have $e * g = g * e = g$.
3. For each a in G there is an element a^{-1} in G such that $a*a^{-1} = a^{-1}*a = e$

Just like a set can have subsets, a group can also have subgroups, the definition of a subgroup is as follows:

Defintion 3.2: We say that $(H, *)$ is a subgroup of a group $(G, *)$ if H is a subset of G and if $(H, *)$ also forms a group.

Most often the operation * will be clear from the context and so we will refer to a group $(G, *)$ with subgroup $(H, *)$ as just G with a subgroup H and omit the operation.

When talking about groups we would like to have some notion of their sizes, some groups are larger than others. For this we use the term *order*, which is the number of elements in the groups underlying set.

Defintion 3.3: Let $(G, *)$ be a group, then the order of the group, denoted $|G|$, is the cardinality of G.

Some very important theorem regarding groups are the Sylows theorems, in this work we will make use of the first of the theorems. First we need the following definition.

Definition 3.3 Let G be a group and let p be a prime. If G is a group of order $p^a m$ where p does not divide m, then a subgroup of order p^a, if such a subgroup exists, is called a Sylow p-subgroup of G. The set of Sylow p-subgroups of G is denoted by $Syl_p(G)$ (and the number of Sylow p-subgroups of G is denoted by $n_p(G)$).

Now, what the first sylow theorem actually says, is that it asserts the existence of the sylow subgroups.

Sylow theorem 1 Let G be a group of order $p^a m$, where p is a prime that does not divide m. Then Sylow p-subgroups exist, i.e $Syl_p(G) \neq \emptyset$.

Proof: See for example Abstract Algebra, D. Dummit, R. Foot.

With the notion of order we can compare the sizes of groups, we would also like to compare their structures. This can be done by maps between them, specifically we want maps that preserves a groups structure. We call these maps *homomorphisms.*

Definition 3.4: Given two groups $(G, *)$ and $(H, \circ)$ a map h from G to H is a homomorphism if $h(a * b) = h(a) \circ h(b)$ for all $a, b \in G$.

Thus, it does not matter if we first calculate a*b and then apply the homomorphism to the result, or instead apply the homomorphism to a and b first and then calculate $h(a) \circ h(b)$. In both cases we will get the same result. Intuively when we have a homomorphism from a group G to a group H, we can think of it as the group structure of G exists inside the structure of H. If a homomorphism is bijective we call it an *isomorphism* and say that the two groups are *isomorphic*. Then not only does the structure of G exist in the structure of H but also the other way around, meaning that the groups share the same structure. Isomorphic groups are thus essentially the same, they behave in the exact same way and only differ, possibly, in their notation.

Definition 3.5: Let h be a homomorphism from a group G to another group H. The set $\{g \in G | h(g) = 1\}$, where 1 is the identity element of H, is called the kernel of h and denoted by Ker(h).

The kernel is thus the set of all elements that gets mapped to the identity. The kernel will in fact be a subgroup.

Proposition 3.6 Let h be a homomorphism from the group $(G, *)$ to $(H, \circ)$. Then Ker(h) forms a subgroup of $(G, *)$

Proof: Let G,H be as in the proposition and e be the identiy of G and 1 the identity of H. The kernel is a subset of G, it remains to show that it forms a group. The identity element e must belong to Ker(h) since it has to be mapped to the identity 1 of H: $h(g) = h(e * g) = h(e) \circ h(g)$. To show that every element in Ker(h) has an inverse, suppose that $g \in Ker(h)$. Then $1 = h(gg^{-1}) = h(g) * h(g^{-1}) = 1 * h(g^{-1})$ so g^{-1} must be in the kernel as well. Lastly, associativity follows from the associativity of G. Thus Ker(h) is a group, completing the proof. □

Defintition 3.7: Let G be a group and H a subgroup, the set $gH = \{gh | h \in H\}$ is called a *left coset* of H in G.

Proposition 3.8: Let G be a group and H any subgroup. The set of left cosets of H partition G.

Proof: First we show that $G = \bigcup_{g \in G} gH$. Since H is a subgroup $e \in H$ and $g * 1 \in gH$ for all g. To show that all the cosets are dissjoint, suppose that $gH \cap jH \neq \emptyset$. Let x be any element contained in the intersection. Then $x = gh = jh'$ for some $h, h' \in H$. Multiplying the equality $gh = jh'$ by h^{-1} from the right gives $g = jh_1$ where $h_1 = h'h^{-1} \in H$. For any element gh of gH we get $gh = j(h_1 h) \in jH$. Thus $gH \subseteq jH$, in the same way we can show that $jH \subseteq gH$, so jH=gH. Thus all cosets are dissjoint and the cosets partion G. □.

Proposition 3.8 gives motivation for the following definition of the index of a subgroup:

Definition 3.9 Let G be a group and H a subgroup of G. The number of left cosets of H in G is called the index of H in G and is denoted $|G : H|$.

3.1 Permutation Groups

We shall see that the set of all permutations of a set X form a group under composition.

Example 3.1.1: The set of all permutations of a set X form a group under composition, defined by $\alpha\beta(x) = \alpha(\beta(x))$. This group is called Sym(X). We show that Sym(x) does indeed satisfy the definition of a group.

1. Composition of permutations are associative as we have already shown.
2. Let e be the identity permutation of the set X, i.e it maps every element to itself.
3. Let α be any permutation on a set X, and let $^{-1}$ be the permutation that reverses α such that $\alpha^{-1}(\alpha(x)) = x$. Then $\alpha * \alpha^{-1} = e$.

Since Sym(X) consists of all permutations of X, we have that $|Sym(X)| = |X|!$ is the order of $Sym(X)$.

Definition 3.1.2 If G is a subgroup of Sym(X) we say that the pair (G,X) is a permutation group of *degree* $|X|$.

3.2 Group actions

This section will introduce group actions and several related definitions. Group action are a very important concept and tool in group theory, which in short consists of letting groups *act* on sets.

Definition 3.2.1 If G is a group and X is a set, then a function

$$\phi : G \times X \to X, (g, x) \to \phi(g, x)$$

is a *left group action* if it satisfies the following two conditions:

$$i)\forall x \in X, \phi(e, x) = x$$

$$ii)\forall g, h \in G, \forall x \in X, \phi(gh, x) = \phi(g, \phi(h, x))$$

where e denotes the identity element of G.

Group actions are closely related to permutations and permutation groups. If we fix g for ϕ, we get a map from X to X. This map is in fact a permutation of X.

Proposition 3.2.2 For each $g \in G$, the map ϕ_g from X to X defined by $\phi_g(x) = \phi(g, x)$ is a permutation of X.

Proof: To show that ϕ_g is a permutation of X is to show that it is a bijective map, we do this by showing that ϕ_g has a 2-sided inverse. Since G is a group g will have an inverse g^{-1}, then ϕ_g^{-1} will be a 2-sided inverse of ϕ_g:

$$\phi_g(\phi_g^{-1}(x)) = \phi(g, \phi(g^{-1}, x)) = \phi(gg^{-1}, x) = \phi(e, x) = x$$

$$\phi_g^{-1}(\phi_g(x)) = \phi(g^{-1}, \phi(g, x)) = \phi(g^{-1}g, x) = \phi(e, x) = x$$

Thus ϕ_g is a permutation of X for each $g \in G$ $\square$.

Due to G being a group, we see that each ϕ_g acts as a permutation. Similarliy we can see that the set of all ϕ_g forms a group under composition, this group will in fact be homomorphic to a permutation group, as summarised by the following proposition.

Proposition 3.2.3 The set of maps ϕ_g from X to X for all $g \in G$ from a left group action forms a group Φ under composition that is isomorphic to a permutation group of degree $|X|$.

Proof: First we prove that this does indeed form a group, and afterwards we show that the group is isomorphic to a permutation group of degree $|X|$. We have already showed that every element ϕ_g has an inverse ϕ_g^{-1}, it remains to show that it has an identity and that the composition is associative. Let e be the identity element of the group G, then ϕ_e will be the identity element of Φ.

$$\phi_g(\phi_e(x)) = \phi(g, \phi(e, x)) = \phi(ge, x) = \phi(g, x)$$

$$\phi_e(\phi_g(x)) = \phi(e, \phi(g, x)) = \phi(eg, x) = \phi(g, x)$$

Similarly we can show that the composition is associative, we here use $\circ$ to denote composition.

$$((\phi_g \circ \phi_h) \circ \phi_j)(x) = \phi((g * h) * j, x)$$

$$(\phi_g \circ \phi_h(\circ \phi_j))(x) = (g * (h * j), x)$$

Where * is the operation of the group G, associativity then follows from the associativity of G. We have then shown that Φ is a group.

To show that Φ is isomorphic to a permutation group of degree $|X|$, we start by defining a homomorphism from Φ to S_X by sending ϕ_g to its corresponding permutation. The image of this map is then isomorphic to $|Phi|$ and is also a permutation group of rank $|X|$. $\square$.

Definition 3.2.4: Let G be a group acting on a non empty set X. The set $\{g \in G | \phi(g, x) = x\}$ is called the stabilizer of x and will be denoted G_x

Definition 3.2.5: Let G be a group acting on the nonempty set X. The set

$\{\phi(g,x)|g \in G\}$ is called the orbit of x, which contains all the elements that x can be mapped to by the group action.

On any given group action we can see that a element only belongs to a single orbit and that the orbits form a equivalence relation on the underlying set of the group action. To see this we first note that an element x is always in its own orbit, since $\phi(e,x) = x$. If x is in the orbit of y, then there exists a $g \in G$ such that $\phi(g,x) = y$. Then

$$x = \phi(g^{-1}g, x) = \phi(g^{-1}, \phi(g,x)) = \phi(g^{-1}, y),$$

so y is also in the orbit of X. Lastly if x is the orbit of y, and y is in the orbit of z, then there exists $g, h \in G$ such that $\phi(g,x) = y$ and $\phi(h,y) = x$. Thus we see that

$$\phi(hg, x) = \phi(g, \phi(h,x) = \phi(g,y) = z$$

so x is also in the orbit of z. This shows that belonging to the same orbit is a equivalence relation.

Definition 3.2.6: A group action is transitive if it only has one orbit.

Since we have seen the connection between permutation groups and group actions the notions of orbits and stabilzers makes sense for Permutation groups as well. We say that for a permutation group (G,X), the orbit of an element $x \in X$ is the set $\{gx|g \in G\}$, that is all elements x can be permuted to. We similarliy say that a permutation group is transitive if it only has one orbit.

Definition 3.2.7: Let (G,X) be a transitive permutation group, and suppose R is an equivalence relation on X. R is said to be G-admissible if $(x,y) \in R$ implies $(gx, gy) \in R$ for all $g \in G$.

The universal relation $X \times X$ and the equality relation, $(x,y) \in R$ iff $x = y$, are always G-admissible. We say that these relations are trivial. Note that the orbit relation here will always be G-admissable as it is in fact the Universal relation since G is transitive.

Definition 3.2.8: The transitive permutation group (G,X) is primitive if there are no non trivial G-admissible equivalence relations R on X.

Last for this section is a definition that we will see is more important later in section 5.

Definition 3.2.9: Let (G,X) be a transitive permutation group, then the *rank* of (G,X) is the number of orbits of G_x on X.

4 Graphs

This section will aim to quickly cover some basic definitions and results for graphs. We start with the definition of an undirected graph or digraph for sort.

Definition 4.1: An undirected graph consists of a finite nonempty vertex set V, and an edge set $E \subseteq V \times V$. The egde set is symmetric, if $(a, b) \in E$ then $(b, a) \in E$, and both (a, b) and (b, a) represent the same edge.

In a directed graph, or digraph for sort, the edge set does not have to be symmetric and (a, b) is different from (b, a). The former represents an edge from a to b while the latter represents and edge from b to a.

Definition 4.2: A walk in a graph from a vertex a to a vertex b is a series of vertices $a = v_1, v_2, ..., v_r = b$ such that $(a, v_2), (v_2, v_3), ..., (v_{r-1}, b)$ are all edges.

Definition 4.3: Let (V,E) be an undirected graph. For every vertex $v \in V$ the degree of v, denoted deg(v), is the number of edges from the vertex v.

When looking at groups acting on graphs we will mostly be interested in regular graphs, which are graphs where all vertices are of the same degree. Even more interesting are strongly regular graphs which will be covered in the next section.

5 Groups and Graphs together

In this section we aim to connect permutation groups and graphs with each other, in particular we aim to develop methods to use graphs to study permutation groups and vice versa.

As mentioned previously the rank of a transitive group is the number of orbits of the stabilizer G_x on X. The following lemma gives us another way of calculating the rank of a transitive permutation group (G,X) by letting G act on the Cartesian product $X \times X$.

Proposition 5.1 Let (G,X) be a transitive permutation group and suppose that G has r orbits on $X \times X$. Then r is the rank of (G, X).

We will denote the orbits by $D_0, D_1, ..., D_{r-1}$, with D_0 denoting the diagonal orbit containing all elements on the form (x,x) for $x \in X$ and will remain the convention for this work. This orbit will always exist as G is presumed to be transitive.

Proof of 5.1: Suppose that G has r orbits, $D_0, D_1, ..., D_{r-1}$ on $X \times X$. Fix $x \in X$ and let $D_i(x) = \{y \in X | (x, y) \in D_i\}$. Then if $y \in D_i(x)$ then $(x, y) \in D_i$. Since all D_i are orbits of G any $g \in G_X$ will send all elements of $D_i(x)$ to $D_i(x)$. Since $D_i(x)$ for $i = 0, 1, ...r - 1$ is a partition of X, they will correspond to the orbits of G_x on X. Thus G_x has r orbits and the rank of G is r. □

We also note that each of the orbits D_i defines a relation R_i on X by $(x, y) \in R$ if and only if $(x, y) \in D_i$. For example D_0 always defines the identity relation on X. These relations can be represented as a graph by letting each element of X represent a vertex, where there is an edge from x to y if $(x, y) \in D_i$ for $i \neq 0$. This gives a digraph representing the relation, for any orbit D we denote the corresponding graph by $\Gamma(D)$. Thus for D_0 the graph will just consist of loops from each vertex to itself.

Example 5.2 Consider S_n, $n \geq 2$, acting on $\{1, ..., n\} \times \{1, ..., n\}$. One orbit will be the diagonal orbit D_0. Consider an element (x,y) with $x, y \in \{1, ..., n\}$ and $x \neq y$, then (x,y) does not belong to D_0. For any pair (x', y') of the same form as (x, y) the permutation $(xx')(yy') \in S_n$ takes (x,y) to (x',y') so they belong to the same orbit. Thus there are only two orbits and S_n is of rank 2.

We will now see that we can study properties of the permutation group by studying properties of these digraphs.

Theorem 5.3 Let (G,X) be a transitive permutation group. (G,X) is primitive iff the digraph $\Gamma(D)$ is connected for each orbit $D \neq D_0$ on $X \times X$.

Proof: Suppose first that (G,X) is primitive and let D be any orbit except D_0. Define the relation R by $(x, y) \in R$ iff x and y may be joined by a walk in $\Gamma(D)$, R is then an equivalence relation. If $x = v_0, v_1, ..., v_r = y$ are vertices of a walk joining x and y that means that $(x, v_0), (v_0, v_1), ..., (v_r, y) \in D$. Since D is an orbit of G on $X \times X$ we also have that $(gx, gv_0), (gv_0, gv_1), ..., (gv_r, gy) \in D$, so $gx = gv_0, gv_1, ..., gv_r = gy$ is a walk joining gx and gy. This shows that R is G-admissible. Since G acted primitively R is trivial and since $D \neq D_0$ R must be the universal relation $R = X \times X$ so $\Gamma(D)$ is connected. This shows that $\Gamma(D)$ $(D \neq 0)$ is connected if (G, X) is primitive.

Now instead suppose that (G, x) is not primitive and R is a non-trivial G-admissible equivalence relation on X. Since R is non trivial and thus not the equality relation we can choose distinct points a,b such that $(a, b) \in R$. Now (a, b) will be in some orbit $D(\neq D_0)$ of G on $X \times X$. R is G-admissible so since R contains one element from D it will also contain the entire orbit. Since by assumption R is not the universal relation we can choose c,d such that $(c, d) \notin D$. Suppose $\Gamma(D)$ is connected, then there is a walk $c = v_0, v_1, ..., v_r = d$ and so $(c, v_1), (v_1, v_2), ..., (v_{r-1}, d) \in D$ and thus also $(c, v_1), (v_1, v_2), ..., (v_{r-1}, d) \in R$. However, R is an equivalence relation so it follows that $(c, d) \in R$ which is a contradiction so $\Gamma(D)$ has to be disconnected. □

6 Some graphs and their automorphism groups

In this section we begin by introducing automorphism groups of graphs and continue to explore the automorphism groups of some particular graphs. We start with the definition of an automorphism and automorphism group.

Definition 6.1 An automorphism of a graph is a permutation α of the vertices such that if (a,b) is an edge then $\alpha a, \alpha b$ will also be an edge.

Definition 6.2 The automorphism group of a graph G, also called the full automorphism group, is the group consisting of all automorphisms of the graph and is denoted $Aut(G)$

A group of autmorphisms of graph G is thus not the same as a graphs automorphism group. The former need not contain all automorphisms of the graph and is a subgroup of the $Aut(G)$

Definition 6.3 A graph is vertex transitive if it admits a group of automorphisms acting transitively on the vertices.

For a graph to be vertex transitive it must most definitely be regular, since an automorphism can only map vertices to vertices of the same degree. Being regular is however only a necessary condition but not a sufficient one.

The following two theorems shows a connection between the automorphism group of a vertex transitive graph and the associated graph of a transitive permutation group.

Theorem 6.4 Let (G,X) be a transitive permutation group and D a symmetric orbit of G on $X \times X$. Then the associated graph $\Gamma(D)$ admits G as a group of automorphisms.

Proof: Let $\{x, y\}$ be any edge of $\Gamma(D)$. Then $(x, y) \in D$ and since D is an orbit $(gx, gy) \in D$ for all $g \in G$. Thus $\{gx, gy\}$ is an edge in $\Gamma(D)$ for all $g \in G$ which shows that G acts as a group of automorphisms on $\Gamma(D)$. □

Theorem 6.5 Let $\Gamma = (V, E)$ be a vetex transitive graph and suppose that G is a group of automorphisms of Γ acting transitively on the vertex set V. Then there is a family $\mathcal{D}$ of orbits such that

$$\{u, v\} \in E \Leftrightarrow (u, v) \in D$$

for some $D \in \mathcal{D}$.

Proof Suppose that $\Gamma = (V, E)$ is vertex transitive graph and that G is a group of automorphisms acting transitively on the vertex set V. We start by defining a family $\mathcal{D}$. Let a orbit D be in the family $\mathcal{D}$ if there exists an edge

$\{x, y\}$ such that $(x, y) \in D$. This guarantees that $\{u, v\} \in E \rightarrow (u, v) \in D$ for some $D \in \mathcal{D}$. To show the other implication note that if $(u, v) \in D \in \mathcal{D}$ there is some edge $\{x, y\}$ such that $(x, y) \in D$. Since D is an orbit there exists a g such that $gx = u$ and $gy = v$. G is an automorphism so thus $\{u, v\}$ must be an edge, showing the left implication. □

6.1 Tools for estimating an automorphism group

This section develop some tools for estimating an upper bound for the order of the automorphism group of a graph. This will be used in the subsequent sections to find the the automorphism group of the graphs O_k and $K_{n,n}$.

Let $\Gamma = (V, E)$ be a vertex transitive graph and suppose that x, y are vertices such that $\{x, y\}$ is an edge. Let G be a group of automorphisms of Γ acting transitively on the vertex set V and on the set of ordered pairs of adjacent vertices. Define

$$L_x = \{g \in G_x | g \textit{ fixes each vertex adjacent to } x\}$$

$$L_{xy} = L_x \cap L_y$$

Lemma 6.1.1 Let k denote the valency of Γ, then $|G_x : L_x| \leq k!$.

Proof: Fix a vertex x in Γ, we denote its k adjacent vertices by $1, 2, ..., k$. Define a homomorphism from G_x to a permutation group P of degree k by how g permutes the vertices $1, 2, ..., k$. The kernel of this homomorphism are all elements that gets mapped to identity permutation. These are the elements of G_x that fixes all adjacent vertices of x, so the kernel of this homomorphism is L_x. There are a maximum of $k!$ different permutations of k elements. So we can conclude $|G_x : L_x| \leq k!$.

Proposition 6.1.2 If x and y are adjacent vertices and $L_{xy} = e$, then $|G_x| \leq k!(k-1)!$.

Proof: Fix x,y such that they are adjacent vertices. We want to proceed in a similar fashion as in the previous lemma to show that $|L_x : L_{xy}| \leq (k-1)!$. Define a homomorphism from L_x to permutation group P of degree k-1 by how it permutes the k-1 vertices of y except x. The kernel of this homomorphism is all elements of G that fixes all k-1 vertices, this amounts exactly to L_{xy}. Since there are at most $(k-1)!$ different permutations we get that $|L_x : L_{xy}| \leq (k-1)!$. Now if $L_{xy} = 1$ we get that $|L_x| \leq (k-1)!$ and then by Lemma 6.1.1 we get that $|G_x| \leq k!|L_x| \leq k!(k-1)!$ which is what we wanted to show.

6.2 The complete bipartite graph $\mathbf{K}_{n,n}$

We now have the results we need to start looking at the automorphism group of the complete bipartite graph. The graph consits of a vertex set that is the disjoint union of to sets $V = A \cup B$ and with the edge set $E = \{\{a,b\}|a \in A, b \in B\}$. By using proposition 6.1.2 we can find a upper bound for the full automorphism group $|\text{Aut}(K_{n,n})|$.

Proposition 6.2.1 $|\text{Aut}(K_{n,n})| \leq 2(n!)^2$

Proof: Suppose G is a group of automorphisms of $\text{Aut}(K_{n,n})$. Let $V = A \cup B$ and x and y be adjacent vertices. Since x and y are adjacent they belong to different sets of the union, suppose without loss of generality that $x \in A$ and $y \in B$. Then x is adjacent to every element of B and y is adjacent to every element of A, thus $L_{x,y} = e$ since it fixes every vertex. By proposition 6.1.2 then $|G_x| \leq n!(n-1)!$. From proposition ?.? we have $|Gx||G_x| = |G|$, since there is only one orbit, it is the size of the whole vertex set $|Gx| = 2n$. Putting it together we get $|G| \leq 2(n!)^2$ which is what we wanted to show $\square$.

If we can find a group of automorphisms of $K_{n,n}$ of order $2(n!)^2$, then by proposition 6.2.1 that has to be $\text{Aut}(K_n, n)$. Let $A = \{a_1, a_2, ..., a_n\}$ and $B = \{b_1, b_2, ..., b_n\}$ be the two dissjoint vertex sets of $K_{n,n}$. Consider the set of permutations consisting of Sym(A), Sym(B) and the permutation that swaps A and B by sending a_i to b_i for $i = 1, 2, ..., n$ as well as any composition of those. Here we consider the permutations of Sym(A) and Sym(B) as permutations of the whole vertex set by letting the the permutations of Sym(A) fix all vertices in B and the permutations of Sym(B) fix all vertices in A. The order of this set is exactly $2(n!)^2$, since Sym(A) gives n! permutatons of A, Sym(B) gives n! independent permutations of B and for a total of $(n!)^2$ permutations. Finally, for any permutations we can also swap A, B which gives the total of $2(n!)^2$. We call this set Ψ, if we can show that all of the elements of Ψ are a group of automorphisms of $K_{n,n}$ under composition, then that means that $\Psi = \text{Aut}(K_{n_n})$.

Lemma 6.2.2 Ψ is a set of automorphisms of $K_{n,n}$.

Proof: Since all vertices of A have edges to the exact same edges, namely all vertices in B, any permutation of just vertices in A will be an automorphism. Thus Sym(A) is a set of automorphisms, similarly Sym(B) is also a set of automorphisms. The permutation swapping A and B is also an automorphism since any edge (a_i, b_j) will be mapped to (b_i, a_j) which is again an edge. Finally, a composition of automorphims will again be an automorphism, thus Ψ is a set of automorphisms. $\square$

Lemma 6.2.3 Ψ forms a group under composition.

Proof: As we know already, composition is associative. We have to show that there exists an identity element and that every element has an inverse. The identity element from either Sym(A) and Sym(B) are here the same element, it fixes all elements and is thus the identity permutation. Every element of Sym(A) and Sym(B) has an inverse and the permutation swapping A and B is its own inverse. If α is a permutation of Ψ then it is a composition of permutations, say $p_1, p_2...p_n$, that all have inverses in Ψ. Then $p_n^{-1}...p_2^{-1}, p_1^{-1}$ belongs to Ψ and is the inverse of α. This shows that Ψ forms a group under composition. $\square$

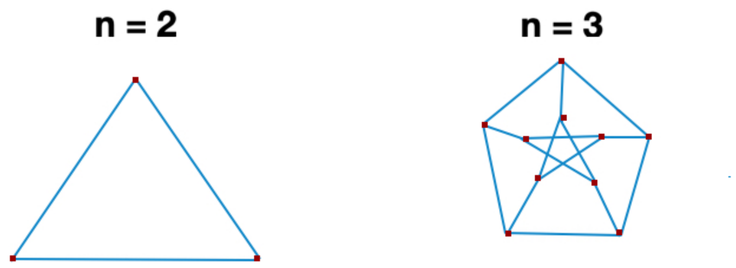
With the above reasoning together with lemma 6.2.2 and 6.2.3 we can finally reach the following proposition:

Proposition 6.2.4 Ψ is the full automorphism group of $K_{n,n}$.

6.3 The odd Graph O_k

We will now take a look at another a specific type of graph, called the odd graph, which we will denote by O_k. The odd Graph O_k is defined as follows (for $k \geq 2$). The vertice set V, is the set of (k-1)-subsets of a fixed (2k-1)-set, and the edge set E, is the set of pairs $\{v, w\}$ for $v, w \in V$ such that v and w are disjoint sets.

Example:(pictures of O_2 and O_3)



Proposition 6.3.1 The odd graph O_k has $\binom{2k-1}{k-1}$ vertices and $\frac{k\binom{2k-1}{k-1}}{2}$ edges.

Proof: The number of vertices follows straight from the definition of O_k, there is a vertex for every k-1 subset of the 2k-1 set, which gives $\binom{2k-1}{k-1}$ vertices. Every vertex has an edge to all vertices it shares no element with. Since the vertex consists of k-1 elements there are k elements remaining. Removing any one of these elements will give arise to a disjoint k-1 subset, thus every vertex has k edges. This gives a total of $k\binom{2k-1}{k-1}/2$ edges. $\square$

Trying to find a group of automorphisms of O_k we can see that S_{2k-1} acts as a group of automorphisms by permuting the underlying (2k-1)-set as shown in the following lemma:

Lemma 6.3.2: S_{2k-1} acts as a group of automorphisms on O_k and is transitive on the vertices and on ordered pair of adjacent vertices.

Proof: We let S_{2k-1} act on the vertices by permuting the fixed (2k-1)-set. If $\alpha \in S_{2k-1}$ and $\{v, w\} \in E$, since v and w are disjoint and α is a bijection, αv and αw will also be disjoint so $\{\alpha w, \alpha v\} \in E$, which shows that S_{2k-1} acts as a group of automorphisms. It is clear that it is transitive on vertices since S_{2k-1} can permute any (k-1)-subset to any other (k-1)-subset. Let $(a, b)\rangle$ and (c, d) be two ordered pairs of adjacent vertices, then a and b are disjoint and together contain 2k-2 distinct elements, the same is true for c and d. Consider a permutation that bijectively maps a to c, b to d and the one element not in $a \cup b$ to the one element not in $c \cup d$, such a permutation exists and is an elements of S_{2k-1} which shows that S_{2k-1} acts transitively on ordered pairs of adjacent vertices. $\square$

What is the rank of this automorphism group? From propsition 5.1 we know that the rank of the group (S_{2k-1}, X) is equal to the number of orbits of S_{2k-1} on $X \times X$. We already showed that S_{2k-1} is transitive on ordered pairs of adjacent vertices, thus all pairs of k-1 subsets of $S_{2k-1} \times S_{2k-1}$ which have no elements in common are contained in the same orbit. It is also clear that this orbit contains no other elements, since if a pair of subsets share some elements it can only be mapped to a pair of subset sharing the same number of elements. Thus ordered pairs of subsets sharing no elements will constitute one orbit.

Similarly we can show that S_{2k-1} is transitive on ordered pairs of subsets sharing n elements with $0 \leq n \leq k-1$. Let $\langle a, b\rangle$ and $\langle c, d\rangle$ be two ordered pairs of subsets with each pair having n elements in common. Then there exists a bijection α that maps the n shared elements from a, b to the n shared elements of c, d and that maps the remaining k-1-n elements of a to the remaining elements of c and the same from b to d. This shows that S_{2k-1} is indeed transitive on ordered pairs of subsets sharing n elements with $0 \leq n \leq k-1$. With the same argument as when n=0 we can show that for each n there is a unique orbit. Thus there are k orbits which gives us the following proposition

Proposition 6.3.3 (S_{2k-1}, O_k) is a permutation group of rank k.

It can now be interesting to ask ourselves if S_{2k-1} is the full automorpishm group of O_k or not. We will come back to this question but first we will study the structure of the graph O_k some more with the following lemma:

Lemma 6.3.4 If a,b,c,d are distinct vertices of O_k such that $\{a, b\}, \{b, c\}$ and $\{c, d\}$ are edges. Then a,b,c,d determine a unique pair of vertices $e \neq c$ and $f \neq b$ such that $\{d, e\}, \{e, f\}$ and $\{f, a\}$ are edges.

Proof:

a,b,c,d are vertices of O_k, so they are all (k-1)-subsets of a set with 2k-1 elements with $a \cap b = \emptyset$, $b \cap c = \emptyset$ and $c \cap d = \emptyset$. Thus $a \cup b$ consists of 2k-2 different elements. We denote the elements of a by $1, 2, ...k-1$ and the elements of b by $k, k+1, .., 2k-2$. Now we know that c is disjoint with b, so c contains k-1 elements of the k elements $1, 2, ..., k-1, 2k-1$. Since c is also distinct from a, the one element it does not contain has to be in a, otherwise a=c. Since the names of the elements of a is arbitrary, let the element that is in a but not in c be 1. Thus c consists of the elements $2, 3, .., k-1, 2k-1$. For d, we have the possibilities of k-1 elements from the k elements $1, k, k+1..., 2k-2$.. The one element of these not in d has to be an element of b, so we choose one of the elements of $k, k+1, .., 2k-2$ to remove, and again since the naming was arbitrary, we can say that this is the element k. We can thus, without any loss of generality denote the vertices by $a = \{1, 2, ...k-1\}, b = \{k, k+1, .., 2k-2\}, c = \{2, 3, .., k-1, 2k-1\}$ and $d = \{1, k+1, k+2, ..., 2k-2\}$. We now want to show that the new vertices, e and f are uniquely determined. Since $\{d, e\}$ and $\{f, a\}$ are edges, e and f are restricted to k-1 of the k elements $2, 3, ..., k, 2k-1$ and $k, k+1, ..., 2k-1$ respectively. We also have that $e \neq c$ and $f \neq b$. So for e we have to remove one of the elements in $c = \{2, 3, .., k-1, 2k-1\}$ from $2, 3, ..., k, 2k-1$, and for f we have to remove one of the elements in $b = \{k, k+1, .., 2k-2\}$ from $k, k+1, ..., 2k-1$, thus we have $k \in e$ and $2k-1 \in f$. The final remaining criterion is that $\{e, f\}$ is an edge, i.e disjoint sets. So $k \notin f$ and $2k-1 \notin e$, which then gives the only possibilities $e = \{2, 3, ..., k\}$ and $f = \{k+1, k+2, ..., 2k-1\}$, so e and f are uniquely determined. □

While not immediately useful, the proof of lemma 6.2.2 gives us more insight into the structure of the odd graph O_k. Suppose that G is the full group of automorphisms of O_k. If $\alpha \in L_a$ then α only permutes the elements 1,2,...,k-1 of a and fixes everything else. Similarly if $\alpha \in L_b$ then α only permutes the elements $k, k+1, ..., 2k-2$ and fixes everything else. Thus, if $\alpha \in L_{a,b}$ then α fixes everything not in a and not in b. Since a and b are disjoint sets, we get that α fixes everything so $\alpha = e$. We summarize this result in the follwoing lemma:

Lemma 6.3.5 Let G be the full automorphism group of O_k If x and y are adjacent vertices then $L_{x,y}$=e

Using Lemma 6.2.5 we are now ready to return to question of whether or not S_{2k-1} is the full automorphism group of O_k and show that this is indeed the case.

Proposition 6.3.6 S_{2k-1} is the full automorphism group of O_k.

Proof: Suppose G is the full automorphism group of O_k. From 6.2.5 and 6.1.2 we get that that $|G_x| \leq k!(k-1)!$. Since G is transitive we have that

$|Gx| = \binom{2k-1}{k-1}$ and so

$$|G| = |Gx||G_x| \leq \frac{(2k-1)!}{(k-1)!k!}k!(k-1)! = (2k-1)!$$

Thus the full automorphism group of O_k cannot be larger than $(2k-1)!$ which is exactly the order of S_{2k-1}, so S_{2k-1} is the full automorphism group of O_k. □

7 Strongly regular graphs

This section will cover strongly regular graphs, hinted at in section 4. We will present the definition and main theorem for strongly regular graphs and use these to show a number of interesting results. We start with the definition:

Definition 7.1 A regular graph of valency k is said to be strongly regular if every pair of adjacent vertices has a constant number α of vertices adjacent to both of them, and every pair of non adjacent vertices has a constant number γ adjacent to both of them.

Theorem 7.2 Let (G, X) be a transitive permutation group of rank 3. Suppose that $D(\neq D_0)$ is a symmetric orbit of G on $X \times X$, then the associated graph $\Gamma(D)$ is strongly regular.

Proof First we show that $\Gamma(D)$ is indeed regular. Let N(x) be the set of vertices adjacent to x defined by $N(x) = \{y \in X | (x, y) \in D\}$. Let x and y be any two vertices in D, then there exists $g \in G$ such that $gx = y$. By theorem 6.4 G is a group of automorphisms of $\Gamma(D)$ so $|N(x)| = |N(gx)| = |N(y)| = k$ which shows that $\Gamma(D)$ is regular with valency k.

Now let N(x,y) be the set of vertices adjacent to both x and y defined as $N(x, y) = \{z \in X|$. Suppose that x, y, x', y' are vertices in D with x, y and x', y' being distinct such that $\{x, y\}$ and $\{x', y'\}$ are edges. Since D is a orbit there exists a $g \in G$ such that $gx = x'$ and $gy = y'$. The permutation g also gives induces a map from $N(x, y)$ to $N(x', y')$ by sending z to gz. Since g is a permutation this map is a bijection, thus $N(x, y) = N(x', y') = \alpha$ for some constant α.

Now instead suppose that x, y, x', y' are vertices in D with x, y and x', y' being distinct such that (x, y) and (x', y') are not edges. Then since (G,X) is of rank 3, and $(x, y), (x', y') \notin D_0$, they must both belong to the same orbit D'. Then again there is a g such that $gx = x'$ and $gy = y'$ which induces a bijection sending z to gz. This gives that $N(x, y) = N(x', y') = \gamma$ for some constant γ. This shows that $\Gamma(D)$ is strongly regular. □

It can be interesting to study what parameters (k, α, γ) are feasible for a strongly regular graph, as there are clearly combinations that are not possible. Most obvious might be the condition $k \geq \gamma$ and $k \geq \alpha$ since the shared adjacent vertices cannot be higher than the valency.

The following theorem is an important theorem for strongly regular graphs and impose severe restriction on the realisability of the parameters. The proof is however somewhat involved and does not fit into the scope of this work. For a proof see for example 4.4 in 4.4 N.L Biggs, A.T White- Permutation groups and combinatorial structures.

Theorem 7.3: If a strongly regular graph Γ with parameters (k, α, γ) exists, then either:
i) $k = 2\gamma$ and $\alpha = \gamma - 1$, or
ii) $(\alpha - \gamma)^2 + 4(k - \gamma)$ is a perfect square, say s^2, and the expression:

$$m = \frac{k}{2ys}((k - 1 + \gamma - \alpha)(s + \gamma - \alpha) - 2\gamma)$$

is a positive integer.

We can use this theorem to see if some parameters (k, α, γ) are feasible for a strongly regular graph. If neither i) nor ii) holds, the parameters are not possible.

Example 7.4:

Lets look at the parameters $(k, 0, 1)$. These will all be graphs with no cycles of length 3, since $\alpha = 0$ means that no adjacent vertices shares another adjacent vertex creating a 3-cycle.

We know that either i) or ii) from theorem 7.1.2 must hold. If i) is true we get that k=2. If ii) is true we get

$$s^2 = (\alpha - \gamma)^2 + 4(k - \gamma) = 4k - 3$$

$$m = \frac{k}{2s}(ks + k - 2)$$

where s,m are integers.

By substituting in $k = \frac{s^2+3}{4}$ into the expression for m we eliminate k and get the following expression.

$$m = \frac{(s^2 + 3)(\frac{1}{4}s(3 + s^2) + \frac{1}{4}(3 + s^2) - 2)}{8s}$$

We can gather the different s terms to get a polynomial in s:

$$s^5 + s^4 + 6s^3 - 2s^2 + (9 - 32m)s - 15 = 0$$

From this expression we see that s must divide 15, so $s = 1, 3, 5, 15$. Putting these values into the expression $k = \frac{s^2+3}{4}$ gives us $k = 1, 3, 7, 57$. Thus the parameters $(k, 0, 1)$ are only feasible for $k = 1, 3, 7, 57$

What can we say about graphs with the more general parameters $(k, 0, \gamma)$, $\gamma \geq 2$? We will show the following proposition:

Proposition 7.5 For each value of

$$\gamma \neq 2, 4, 6$$

the parameters $(k, 0, \gamma)$, $\gamma \geq 2$, only have a finite number of corresponding values of k.

Proof The proof follows the same idea as the previous example. If the parameters $(k, 0, \gamma)$, $\gamma \geq 2$ are feasible then by theorem 7.2 we have that either i) $k = 2\gamma$ and $\alpha = y - 1$ or ii) must hold. Since $\gamma \geq 2$ and $\alpha = 0$, therefore $\alpha = y - 1$ cannot be true and thus ii) has to be satisfied. This gives

$$s^2 = \gamma^2 + 4k - 4\gamma$$

and that

$$m = \frac{k}{2ys}((k - 1 + \gamma)(s + \gamma) - 2\gamma)$$

is a positive integer. Substituting $k = \frac{s^2 - \gamma^2 + 4\gamma}{4}$ into the expression for m yields:

$$m = \frac{(s^2 + 4\gamma - \gamma^2)(-2\gamma + (s + \gamma)(-1 + \gamma + \frac{1}{4}(s^2 + 4\gamma - \gamma^2)))}{8\gamma s}$$

Continuing with gathering the terms for s and simplifying gives the following expression,

$$\begin{aligned} m = \frac{s^4}{32\gamma} + \frac{s^3}{32} + \frac{(s^2(-1 + 3 - \frac{\gamma^2}{2}))}{8\gamma} + \frac{s(-3\gamma + 3\gamma^2 - \gamma^3/2))}{8\gamma} + \\ + \frac{-4\gamma + 9\gamma^2 - 3\gamma^3 + \frac{\gamma^4}{4}}{8\gamma} + \frac{-12\gamma^2 + 11\gamma^3 - 3\gamma^4 + \frac{\gamma^3}{4}}{8s\gamma} \end{aligned} \tag{1}$$

Finally by writing (1) as a polynomial in s:

$$\begin{aligned} 0 = \frac{s^5}{4} + \frac{\gamma s^4}{4} + (-1 + 3\gamma - \frac{\gamma^2}{2})s^3 + (-3\gamma + 3\gamma^2 - \gamma^3/2))s^2 + \\ (-4\gamma + 9\gamma^2 - 3\gamma^3 + \frac{\gamma^4}{4} - 8\gamma m)s + (-12\gamma^2 + 11\gamma^3 - 3\gamma^4 + \frac{\gamma^3}{4}) \end{aligned} \tag{2}$$

Thus

$$-12\gamma^2 + 11\gamma^3 - 3\gamma^4 + \frac{\gamma^3}{4}$$

must be divisible by s. Calculating the roots gives $\gamma_1 = 2$, $\gamma_2 = 4$ and $\gamma_3 = 6$. Thus for $\gamma \neq 2, 4, 6$ there are only a finite number of possibilities for s, i.e the divisors of

$$-12\gamma^2 + 11\gamma^3 - 3\gamma^4 + \frac{\gamma^3}{4}$$

and thus also only a finte number of corresponding values of k. □

What can then be said for $\gamma = 2, 4, 6$? We look at the specifc case where $\gamma = 2$ and prove the following proposition:

Proposition 7.6: The parameters $(k, 0, 2)$ are feasible if and only if $k = t^2 + 1$, where t is an integer not congruent to 0 (mod 4).

Proof: We start by assuming that the parameters $(k, 0, 2)$ are feasible. Then by theorem 7.1.2 we have that

$$s^2 = \gamma^2 + 4k - 4\gamma = 4k - 4$$

is a perfect square and that

$$m = \frac{k}{2ys}((k+1)(s+2) - 4)$$

is an integer. From $s^2 = 4k - 4$ we get that $s = 2\sqrt{k-1}$ is an integer. For this to be true $\sqrt{k-1} = t$ for some positive integer t, which gives that k is on the form $k = t^2 + 1$. Making the substitutions $s = 2t$ and $k = t^2 + 1$ in the equation for m and simplifying gives

$$m = \frac{t^4 + t^3 + 3t^2 + t + 2}{4}$$

Now, since m is an integer $t^4 + t^3 + 3t^2 + t + 2$ has to be divisible by 4, this gives that $t^4 + t^3 + 3t^2 + t$ is an even number that is not divisible by 4. Since every term contains t, t also cannot be divisible by 4. Thus t has to be a positive integer that is not congruent to 0 (mod 4) which is what we wanted to show. □

Using proposition 7.6 we see that the parameter $(5, 0, 2)$ should be feasible. What would such a graph look like? We will try to create such a graph in the following example.

Example 7.7:

Suppose that Γ_5 is a strongly regular graph with parameters $(5, 0, 2)$. We let * be any vertex and label its adjacent vertices by 1,2,3,4 and 5. These vertices then all need to be adjacent to 4 more veritces but cannot be adjacent to eachother since $\alpha = 0$. Thus 1 must be adjacent to 4 new vertices, we label these 12,13,14 and 15.

The vertex 1 currently shares one vertex, *, with all the vertices $2, 3, 4$ and 5, but since they are not adjacent they need to share 2 adjacent vertices. Therefore the vertices 2,3,4,5 all need to be connected to 1 of the vertices 12,13,14,15 each. Without any loss of generality say that these edges are $\{12, 2\}, \{13, 3\}, \{14, 4\}, \{15, 5\}$.

From here we see vertex 2 is currently adjacent to two vertices but need to have 5 neighbours. Any new edge from vertex 2 to another vertex would create a 3-circuit, so we need 3 new vertices adjacent to 2. We label these 23,24 and 25. Again now, vertex 2 only share 1 adjacent vertex with 3,4 and 5. By the same reasoning we need to add edges $\{23, 3\}, \{24, 4\}, \{25, 5\}$.

Following this procedure we see that we need to add vertices $34, 35$ adjacent to vertex 3, as well as the edges $\{34, 4\}$ and $\{35, 5\}$ and finally add a vertex 45 adjacent to 4 and 5. From here we can again look at vertex 12. It is not and can not be adjacent to vertices 3,4,5 since this would create a 3-circuit. Thus it needs to share 2 adjacent vertices with all of these. The only possibility for this that avoids 3-circuits is to add the edges $\{12, 34\}, \{12, 35\}, \{12, 45\}$ and 12 now have all of its five adjacent vertices as well as sharing two adjacent vertices with all nonadjacent vertices. Proceeding in the exact same way see that we need to add the edges $\{13, 24\}, \{13, 25\}, \{13, 45\}$ completing vertex 13, edges $\{14, 23\}, \{14, 25\}, \{14, 35\}$ completing vertex 14, edges $\{15, 23\}, \{15, 24\}, \{15, 34\}$. The remaining vertices 23,24,25,34,35,45 have already had edges added to them. They still have however have unique edges that needs to be added, these are $\{23, 45\}, \{24, 35\}, \{25, 34\}$ completing the graph.

8 Final remarks

As we have seen algebraic methods from group theory provide powerful tools to study combinatorial objects like graphs, while graphs in turn can be used to study the properties of groups. Tools and concepts from different parts of mathematics can often find use in a different branch, showing a cohesiveness and beauty of mathematics. For further interest in the topic the reader can look into project 4.2 which also connects the topic to combinatorial- designs which fell outside the scope of this work.

9 References

Dummit,David. Foot. Richard. 2004. Abstract Algebra. 3rd edition. John Wiley Sons, Inc.

Grimaldi, Ralph. 2003. Discrete and combinatorial mathematics. 5th edition. Pearson Addison Wesley.

Biggs, N., White, A. (1979). Permutation Groups and Combinatorial Structures (London Mathematical Society Lecture Note Series). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511600739