Université Libre de Bruxelles

Faculté des Sciences

Département de Mathématique

Polyhedra Associated to Symmetric and Alternating Groups

Mémoire présenté en vue de l'obtention du grade de
Master en Sciences Mathématiques

Ann Kiefer

Promoteur: Dimitri Leemans

Année académique 2009–2010

Contents

Remerciements

Tout d'abord, je tiens à exprimer toute ma reconnaissance à mon promoteur Dimtri Leemans, qui m'a soutenue pendant cette dernière année avec autant de conseils utiles que de paroles motivantes.

J'adresse également le plus grand merci aux professeurs qui, à l'école secondaire comme à l'université, m'ont transmis leur passion des mathématiques.

J'aimerais aussi remercier mes parents pour avoir rendu possibles ces cinq merveilleuses années à l'Université Libre de Bruxelles. Je les remercie également pour leur soutien et leur compréhension tout au long de ce parcours.

Enfin, pour leur soutien moral, leur aide et leur patience concernant toute question informatique, mes amis ont toute ma gratitude.

Introduction (fr)

Les polyèdres ont été étudiés en mathématiques depuis longtemps. Des balles en pierre, qui illustrent les symétries des cinq polyèdres réguliers convexes, ont été trouvées en Écosse. Elles datent de la première moitié du troisième millénaire av. J.C. Bien que ce sujet ait déjà fasciné les gens si tôt, il est toujours encore étudié (et amélioré). Cependant les polytopes, et en particulier les polyèdres, ont toujours constitué des sujets à part des autres sujets mathématiques. D'autres sujets qui sont liés à ce mémoire sont les groupes de Coxeter (voir [17]) et les géométries d'incidence (voir [3]). Ces sujets-là sont apparus au 20e siècle et ce n'est que récemment que les mathématiciens font un lien entre ces trois domaines. Le lien entre les géométries minces, régulières, résiduellement connexes, à diagramme linéaire et les polytopes abstraits réguliers, dont une version détaillée se trouve dans [27], est bien connu. Dans [17], McMullen et Schulte expliquent le lien entre les C-groupes à diagramme linéaire et les polytopes réguliers abstraits. Il n'y a qu'un petit pas entre les C-groupes à diagramme linéaire et les groupes de Coxeter. Les C-groupes à diagramme linéaire ne sont en fait que des quotients de ces derniers. Ceci est expliqué dans [17]. Aujourd'hui on considère les C-groupes à diagramme linéaire, les géométries minces, régulières, résiduellement connexes, à diagramme linéaire et les polytopes abstraits réguliers comme essentiellement les mêmes objets mathématiques. De plus, tout polytope abstrait régulier peut être vu comme le quotient d'un polytope universel, ce dernier n'étant rien d'autre que le polytope attribué à un groupe de Coxeter donné. Donc il y a deux points de vue différents pour étudier les polytopes abstraits réguliers; l'un provenant de la géométrie d'incidence (en utilisant les géométries minces, régulières, résiduellement connexes, à diagramme linéaire) et l'autre provenant de la théorie des groupes (en utilisant les C-groupes à diagramme linéaire). Des articles comme [2], [12] et [7] traitent le premier point de vue. Dans [16], Leemans et Vauthier construisent un atlas de polytopes en utilisant la géométrie d'incidence. Le point de vue de la théorie des groupes est utilisé par exemple dans [13], [14], [15] et [11]. De plus Hartley a construit un atlas de polytopes [9], similaire à [16], en utilisant le deuxième point de vue.

Dans ce mémoire, nous essayons de déterminer à isomorphisme près le nombre de polyèdres abstraits sur lesquels les groupes symétriques et alternés agissent comme groupes d'automorphisme réguliers. Ce problème est proche d'un problème ouvert proposé dans [21]. Dans cet article, Schulte et Weiss discutent de plusieurs problèmes ouverts liés aux polytopes. Le problème 32, dû à Hartley, est notamment le suivant:
Trouver des polytopes réguliers, chiraux ou autres dont les groupes d'automorphismes sont des groupes alternés $Alt(n)$. En particulier, pour un rang r donné, pour quel n, $Alt(n)$, apparaît-il comme groupe d'automorphisme d'un polytope régulier ou chiral de rang r ?

Dans ce mémoire nous faisons l'inverse de ce qui est fait normalement en théorie des polytopes. D'habitude on se donne un polytope, respectivement une géométrie, et on étudie les groupes agissant sur ce polytope ou cette géométrie. Ici nous choisissons d'abord un groupe, notamment $Sym(n)$ et $Alt(n)$, et nous essayons de construire des C-groupes à diagramme linéaire isomorphes à ce groupe. Nous avons choisi cette approche, au lieu de celle de la géométrie d'incidence, parce que dans ce cas, elle est plus facile à utiliser. Nous avons déjà réalisé un travail similaire pour les groupes de Suzuki (voir [11]). Cependant le cas des groupes symétriques et alternés s'avère beaucoup plus compliqué. D'un côté, même si l'ordre des groupes de Suzuki croît très vite, ils sont beaucoup plus faciles à manipuler car leurs seuls sous-groupes susceptibles d'être isomorphes à des C-groupes à diagramme linéaire de rang 3 ou plus, sont aussi des groupes de type Suzuki. D'un autre côté, le nombre d'involutions dans un groupe de Suzuki donne la possibilité d'utiliser la théorie des nombres et de travailler avec des diviseurs. L'ordre d'un groupe symétrique ou alterné de degré n est un multiple de tout entier inférieur ou égal à n. De plus par le théorème de Cayley (voir [20]), tout groupe fini d'ordre n est isomorphe à un sous-groupe de $Sym(n)$. Nous devons donc travailler avec une liste énorme de sous-groupes. Ces arguments rendent le travail très difficile.

Une première étape dans ce mémoire est de calculer le centralisateur d'une involution dans $Sym(n)$ et $Alt(n)$. Bien que ce travail ait déjà été fait pour un élément général de $Sym(n)$ ou $Alt(n)$, nous l'avons refait pour les involutions par notre propre méthode. Ceci ne donne pas seulement une version plus simple du centralisateur, mais le fait de l'avoir refait nous-mêmes nous a beaucoup aidés à mieux comprendre la forme générale du centralisateur. De plus nous avons réussi à déterminer une formule générale, qui donne le nombre de paires d'involutions, qui commutent, dans $Sym(n)$ et $Alt(n)$ pour un n donné. Les cas de $Sym(6)$ et $Alt(6)$ sont étudiés séparément à cause de leur groupe d'automorphisme extraordinaire. Nous avons réussi à les finir complètement et à avoir des résultats qui correspondent à ceux de l'atlas dans [16]. De plus nous donnons quelques idées pour la suite du travail.

Ce mémoire contient cinq chapitres. Dans le premier chapitre nous rappelons des définitions sur les polytopes, les C-groupes à diagramme linéaire et les groupes symétriques et alternés, que nous jugeons nécessaires afin de pouvoir comprendre ce mémoire. La première section de ce chapitre est principalement basée sur le livre [17] de McMullen et Schulte. La deuxième section se base sur différents livres de la théorie des groupes, comme [4], [5], [10], [20], [23] et [28]. Dans le deuxième chapitre, nous parlons d'un sujet relativement nouveau, les CPR graphes. Ce chapitre se base essentiellement sur un article de Pellicer [19]. Nous avons également utilisé la thèse de doctorat [18] de ce dernier. Les CPR graphes s'avèrent très utiles lors du travail avec des polytopes et C-groupes à diagramme linéaire. Le fait d'approfondir ce sujet nous a aidés à mieux comprendre les polytopes. Nous avons utilisé les CPR graphes surtout dans les chapitres 4 et 5 pour justifier l'isomorphisme, respectivement le non-isomorphisme, entre un C-groupe à diagramme linéaire et un groupe symétrique ou alterné donné. Dans le chapitre 3, nous exposons ce qui est déjà connu pour les polyèdres des groupes symétriques et alternés. De plus nous expliquons la démarche à suivre pour compter les polyèdres à isomorphisme près. Dans les deux derniers chapitres nous traitons les cas des groupes symétriques et alternés séparément et nous essayons de déterminer des formules générales dans les deux cas. Ce sont donc les deux derniers chapitres qui constituent notre contribution personnelle à ce sujet. Finalement dans les annexes, nous analysons des cas spéciaux de $Sym(6)$, que nous avons laissés de côté dans la section 4.3. De plus un tableau montre les résultats de l'atlas [16] concernant les groupes symétriques et alternés. Deux autres tableaux donnent des résultats pour nos formules générales pour des petites valeurs de n. Ces tableaux montrent que même pour des petites valeurs de n, les résultats des formules croissent rapidement, ce qui montre à nouveau l'étendue du sujet.

Pour conclure, nous avons réellement fait quelques nouvelles contributions au sujet. Cependant nous n'avons pas pu achever tout le travail, car le but était tout simplement trop ambitieux et le sujet trop vaste pour un mémoire.

Introduction (En)

Polyhedra have been studied in mathematics for a long time. In Scotland stone balls were found, that illustrate the symmetry groups of the regular convex polyhedra. They are estimated to date from the first half of the third millennium B.C. Although started so early, the subject is still studied (and improved) today. However polytopes, and particularly polyhedra, have always been a subject separated from the other mathematical subjects. Other subjects, linked to this Master's thesis, are Coxeter groups (see [17]) and incidence geometry (see [3]). They only came up in the 20th century and it has only been recently that mathematicians link these three domains. The link between thin regular residually connected geometries with a linear diagram and abstract regular polytopes is well known. A very detailed version of it can be found in [27]. In [17], McMullen and Schulte explain the link between string C-groups and abstract regular polytopes. It is just a small step from string C-groups to Coxeter groups. String C-groups are just quotients of the latter. This is explained in [17]. Thus today we adopt the point of view that string C-groups, thin regular residually connected geometries with a linear diagram and abstract regular polytopes are essentially the same objects. Moreover every abstract regular polytope may be considered as a quotient of a universal polytope, which is nothing else than the polytope corresponding to a given Coxeter group. Hence to study abstract regular polytopes there are two different points of view; one from the incidence geometry (by using thin residually connected geometries with a linear diagram) and one from group theory (by using string C-groups). Articles such as [2], [12] and [7] deal with the first approach. In [16], Leemans and Vauthier build an atlas of polytopes by using incidence geometry. The group theory approach is used for instance in [13], [14], [15] and in [11]. Moreover Hartley constructed an atlas of polytopes [9], similar to [16], by using this second approach.

In this Master's thesis we try to compute, up to isomorphism, the number of abstract regular polyhedra on which the symmetric and alternating

groups act as automorphism groups. This problem is close to an open problem stated in [21]. In this article Schulte and Weiss discuss important open problems linked to polytopes. Problem 32, asked by Hartley, is the following:
Find regular, chiral or other polytopes whose automorphism groups are alternating groups $Alt(n)$. In particular, given a rank r, for which n does $Alt(n)$ occur as automorphism group of a regular or chiral polytope of rank r?

In this Master's thesis we do the inverse of what is normally done in polytope theory. Usually a polytope, respectively a geometry, is chosen and the groups acting on this polytope or geometry are studied. Here we first choose a group, namely $Sym(n)$ and $Alt(n)$, and we try to construct string C-groups isomorphic to this group. We have chosen this approach instead of the one coming from incidence geometry, because it is simpler to handle in this case. We have already done a similar work for the Suzuki groups (see [11]). However the case of the symmetric and alternating groups turns out to be much more complicated. On the one side, even if the order of Suzuki groups increases quickly, they are easy to get under control as their only subgroups, possible to be isomorphic to string C-groups of rank higher than 3, are also groups of Suzuki type. On the other side, the number of involutions in a Suzuki group allows to work with divisors and number theory. The orders of the symmetric and alternating group of degree n are multiples of every integer smaller than n. Furthermore, by Cayley's theorem (see [20]), every finite group of order n is isomorphic to a subgroup of $Sym(n)$. So we have to deal with a large range of subgroups. These arguments make the work very difficult.

A first step for this thesis is to compute the centralizer of an involution in $Sym(n)$ and $Alt(n)$. Although this work has already been done for a general element in $Sym(n)$ and $Alt(n)$, we did it again by our own method for involutions. This gives not only a simpler version, but it is a good way to understand the general formula better. Moreover we managed to get a general formula counting the pairs of commuting involutions in $Sym(n)$ and $Alt(n)$ for a given n. The cases $Sym(6)$ and $Alt(6)$ are treated separately, because of their particular automorphism group. We finished them completely, obtaining results corresponding to the results of the atlas [16]. Furthermore we give some ideas for future work.

This Master's thesis contains five chapters. In the first chapter we recall definitions about polytopes, string C-groups and the symmetric and alternating groups, we consider necessary to understand this work. The first section of this chapter is essentially based on a book by McMullen and Schulte [17]. The second section is based on several books about group theory, namely [4], [5], [10], [20], [23] and [28]. In the second chapter we treat a relatively new subject, called the CPR graphs. This chapter is mainly based on an article by Pellicer [19]. We also used the PhD thesis [18] of the last author. The CPR graphs turn out to be very useful in studying polytopes and string C-groups. These graphs helped to understand the polytopes better and we mainly use the CPR graphs in chapter 4 and 5 to check if a string C-group is isomorphic to a given symmetric or alternating group or not. In chapter 3 we extend what is already known about the link between polyhedra and symmetric and alternating groups. Moreover we explain the steps we take to count the polyhedra up to isomorphism. In the last two chapters we deal with the symmetric and alternating groups separately and try to get general formulas for both of them. Thus the last two chapters contain our contribution to this subject. Finally in the appendices, we analyse some special cases of $Sym(6)$, which we did not analyse in section 4.3. Moreover a table shows the results from the atlas [16] concerning the symmetric and alternating groups. Two other tables give the results of our general formulas for small n. These tables show that even for small n the results of the formula quickly increase, which shows again the vastness of this subject.

To conclude, we effectively did some new contributions to the subject. However we could not finish the work, because the goal was too ambitious and the subject too wide-ranging for a Master's thesis.

Chapter 1

Definitions and Notations

1.1 Polytopes and C-groups

1.1.1 Regular Convex Polytopes

In this thesis we work with *abstract regular polytopes*. To motivate the definition of the latter, we recall in this section some definitions about regular convex polytopes. Most of the definitions are based on [17].

Recall that a subset K of an n-dimensional euclidean space $\mathbb{E}^n$ is *convex* if, for each two of its points x and y, it contains the line segment

$$[xy] := \{(1-\lambda)x + \lambda y \mid 0 \leq \lambda \leq 1\}.$$

The intersection of two convex sets is again convex, and hence the convex hull *conv* S of a set $S \subseteq \mathbb{E}^n$ is well defined as the smallest convex set which contains S.

Definition 1.1.1. *A convex polytope is the convex hull of a finite set of points.*

Recall that an affine subspace K of $\mathbb{E}^n$ is a subset that contains each line

$$xy := \{(1-\lambda)x + \lambda y \mid \lambda \in \mathbb{R}\}$$

for every points x and y in K. The affine hull *aff* S of a set S is defined in the same way as the convex hull. Then a polytope P is k*-dimensional* or a k*-polytope*, if its affine hull is k-dimensional. We refer to 2-polytopes as *polygons* and to 3-polytopes as *polyhedra*.

Remark 1.1.2. *In this thesis we work with polyhedra, but in this chapter we give all the definitions for a general k-polytope.*

We now define the faces of a convex polytope. We say that a hyperplane is valid for a convex polytope P, if one of its closed sides contains P, i.e. if $cx = \alpha$ is the defining equation of the hyperplane, then all the points of P satisfy $cx \geq \alpha$ or all the points of P satisfy $cx \leq \alpha$.

Definition 1.1.3. *A face of a convex polytope P is either the empty set, either P itself or the intersection of P and a finite number of valid hyperplanes.*

$\emptyset$ and P itself are called *improper* faces. All the other faces are referred to as *proper* faces. Set $\mathcal{P}(P) = \mathcal{P}$ the set of all faces of a polytope P. A face of dimension j is called a j-face and more specifically the faces of dimension 0, 1, $n-2$ and $n-1$ of a convex n-polytope are called *vertices*, *edges*, *ridges* and *facets* respectively.

We now list various properties of a convex n-polytope P, which will motivate many of the definitions of an abstract regular polytope.

- $\mathcal{P}$ is a lattice under the partial ordering $F \leqslant G$ if and only if $F \subseteq G$. The meet of two faces F and G is then $F \wedge G := F \cap G$, and the join of two faces $F \vee G$ is defined as the smallest face of $\mathcal{P}$ containing F and G.
- If $F < G$ are two faces of P with dim G - dim $F = 2$, then there are exactly two faces H of P such that $F < H < G$.
- For every F, G of P with $F \leqslant G$, the section
$$G/F := \{H \in \mathcal{P} \mid F \leqslant H \leqslant G\}$$
of $\mathcal{P}$ is isomorphic to the face-lattice of a polytope of dimension dim G - dim $F - 1$.

Two faces are called *incident* if $F \leqslant G$ or $G \leqslant F$.

- If dim $P \geq 2$, then the face-lattice $\mathcal{P}$ is *connected* if two proper faces F and G can be joined by a chain $F =: F_0, F_1, \ldots, F_k := G$ of proper faces of P, such that F_{i-1} and F_i are incident for $i = 1, \ldots, k$. Furthermore $\mathcal{P}$ is called *strongly connected* if the same is true for every section G/F of $\mathcal{P}$ such that dim $G \geq$ dim $F + 3$.

We call two polytopes P and Q *(combinatorially) isomorphic* if their face-lattices $\mathcal{P}(P)$ and $\mathcal{P}(Q)$ are isomorphic, so that there is a one-to-one correspondence preserving inclusion. Similarly P and Q are dual if $\mathcal{P}(P)$ and $\mathcal{P}(Q)$ are anti-isomorphic, giving a one-to-one inclusion reversing correspondence between the faces of P and those of Q. The dual of a polytope P is noted P^*.

A *flag* of an n-polytope P is a maximal subset of pairwise incident faces of P; thus it is of the form $\{F_{-1}, F_0, \dots, F_{n-1}, F_n\}$, with

$$F_{-1} \subset F_0 \subset \dots \subset F_{n-1} \subset F_n.$$

For an n-polytope P, we always have $F_{-1} := \emptyset$ and $F_n := P$. The inclusions are strict so that $\dim F_j = j$ for each $j = 0, \dots, n-1$. The set of all flags is denoted $\mathcal{F}(P)$. Flags have the following properties.

- Let Φ be a given flag. For each $j = 0, \dots, n-1$, there exists a unique flag $\Phi^j \in \mathcal{F}(P)$ which differs from Φ in its j-face alone. Two such flags Φ and Φ^j are called *adjacent*, or more exactly, *j-adjacent*.

- P is *strongly flag-connected*. This means that for each two flags Φ and Ψ of P, there exists a chain $\Phi =: \Phi_0, \Phi_1, \dots, \Phi_k := \Psi$, such that Φ_{i-1} and Φ_i are adjacent for each $i = 1, \dots, k$, and $\Phi \cap \Psi \subseteq \Phi_i$ for each $i = 1, \dots, k-1$.

The *symmetry group* $G(P)$ of P consists of all the isometries of $\mathbb{E}^n$ conserving P.

Definition 1.1.4. *The convex polytope P is regular if $G(P)$ is transitive on the set $\mathcal{F}(P)$ of flags of P.*

There are alternative definitions for regularity of a convex polytope. Some of them can be found in [17].

An automorphism of a polytope P is a permutation γ of its face-lattice $\mathcal{P}$ which preserves inclusion. The automorphism group of P is denoted by $\Gamma(P)$. We say that P is *combinatorially regular* if $\Gamma(P)$ is transitive on $\mathcal{F}(P)$.

Theorem 1.1.5. *A combinatorially regular polytope is isomorphic to an ordinary regular polytope.*

A *reflexion* R in $\mathbb{E}^n$ is an involutory isometry. It has a mirror of fixed points $\{x \in \mathbb{E}^n \mid xR = x\}$. If this mirror is a hyperplane, we call the reflexion a *hyperplane reflexion*.

A *Coxeter group*[1] is one of the form $G := \langle R_0, R_1, \ldots, R_{n-1} \rangle$, which satisfies relations solely of the form

$$(R_i R_j)^{p_{ij}} = E,$$

where E is the identity and $p_{ij} = p_{ji}$ are positive integers (or infinity) satisfying $p_{jj} = 1$ for each $j = 0, \ldots, n-1$. We call G a *string (Coxeter) group* if $p_{ij} = 2$ whenever $0 \leq i < j - 1 \leq n - 1$. Hence in this case the positive integers $p_{j-1,j}$ with $j = 1, \ldots, n-1$ are left to be determined. Set $p_{j-1,j} = p_j$ and thus a string Coxeter group is denoted by $[p_1, \ldots, p_{n-1}]$. We get the following theorem.

Theorem 1.1.6. *The symmetry group of a regular convex n-polytope P is a finite string Coxeter group, with generators R_j for $j = 0, \ldots, n-1$ which are hyperplane reflexions, and $p_{j-1,j} \geq 3$ for $j = 1, \ldots, n-1$. Conversely, any finite string Coxeter group for which $p_{j-1,j} \geq 3$ for $j = 1, \ldots, n-1$ is the symmetry group of a regular convex polytope.*

With the regular convex n-polytope we can associate the *Schläfli symbol* or *Schläfli type* $\{p_1, \ldots, p_{n-1}\}$, where the p_j are given by theorem 1.1.6.

Example 1.1.7. *There are only five regular convex polyhedra. Their Schläfli symbols are respectively* $\{3,3\}, \{3,4\}, \{4,3\}, \{3,5\}$ *and* $\{5,3\}$.

1.1.2 Abstract Regular Polytopes

In this section we introduce the concept of abstract regular polytopes. We have based our work on [17].

An *abstract polytope $\mathcal{P}$ of (finite) rank n* (≥ -1), or more briefly, an *abstract n-polytope*, is a partially ordered set (or *poset* for short) satisfying certain properties. We will define those properties below. These conditions can be compared with those satisfied by convex polytopes. As an analogy to convex polytopes, the elements of $\mathcal{P}$ are called *faces*. Similarly two faces F and G of $\mathcal{P}$ are said to be *incident* if $F \leqslant G$ or $F \geqslant G$. A chain of $\mathcal{P}$ is a totally ordered subset of $\mathcal{P}$. A chain has *length* i (≥ -1) if it contains

[1] Coxeter groups are discussed in full generality in Chapter 3 of [17].

exactly $i+1$ faces. Note that by definition the empty set is a chain (of length -1). The *flags* are the maximal chains of $\mathcal{P}$ and the set of all flags is denoted by $\mathcal{F}(\mathcal{P})$. It is easy to see that each chain is contained in a flag of $\mathcal{P}$.

We now state the properties defining an abstract polytope.

(P1) $\mathcal{P}$ contains a least face and a greatest face; they are denoted by F_{-1} and F_n respectively.

(P2) Each flag of $\mathcal{P}$ has length $n+1$ or equivalently, each flag of $\mathcal{P}$ contains exactly $n+2$ faces, including F_{-1} and F_n.

For any two faces F and G of $\mathcal{P}$ with $F \leqslant G$, we call

$$G/F := \{H \mid H \in \mathcal{P}, F \leqslant H \leqslant G\}$$

a *section* of $\mathcal{P}$. We can identify a face F with the section F/F_{-1}. Note that each section itself is a poset with properties (P1) and (P2). The properties (P1) and (P2) imply that $\mathcal{P}$ has a natural *rank function*: if F is a face of $\mathcal{P}$, and the rank of F/F_{-1} is i, then we set rank $F = i$ and we call F a *face of* $\mathcal{P}$ *of rank* i, or more briefly an i-*face* of $\mathcal{P}$. It follows that rank $F_{-1} = -1$ and rank $F_n = n$ and these two faces are the only ones of these ranks. As before they are called the *improper* faces while the other faces are the *proper* ones. To emphasize the analogy with the convex polytopes we use the terms *vertices*, *edges*, *subfacets* (or *ridges*) and *facets* for faces of rank 0, 1, $n-2$ and $n-1$ respectively.

Our next property deals with the connectedness of $\mathcal{P}$. We say that a poset $\mathcal{P}$ with properties (P1) and (P2) is *connected* if either $n \leq 1$ or $n \geq 2$ and for any two proper faces F and G of $\mathcal{P}$, there exists a finite sequence of proper faces $F =: H_0, H_1, \ldots, H_{k-1}, H_k := G$ of $\mathcal{P}$ such that H_{i-1} and H_i are incident for i=1, …, k. We say that $\mathcal{P}$ is *strongly connected* if the same is true for each section of $\mathcal{P}$. Note that $\mathcal{P}$ is included in the sections of $\mathcal{P}$ because connectedness of each proper section of $\mathcal{P}$ does not imply connectedness of $\mathcal{P}$ itself. We are ready to state the next defining property.

(P3) $\mathcal{P}$ is strongly connected.

However an equivalent definition in terms of *flag-connectedness* is more useful. In the same way as with convex polytopes, we call two flags of $\mathcal{P}$ *adjacent* if they differ in exactly one face; if this face is of rank i, then they are called *i-adjacent*. Then $\mathcal{P}$ is *flag-connected* if any two flags Φ and Ψ can be joined by a sequence

$$\Phi =: \Phi_0, \Phi_1, \ldots, \Phi_{k-1}, \Phi_k := \Psi \tag{1.1}$$

of flags such that Φ_{j-1} and Φ_j are adjacent for $j = 1, \ldots, k$. Moreover $\mathcal{P}$ is *strongly flag-connected* if each section of $\mathcal{P}$ is flag-connected. Equivalently $\mathcal{P}$ is strongly flag-connected if any two distinct flags Φ and Ψ of $\mathcal{P}$ can be joined by a sequence of the form (1.1), such that Φ_{j-1} and Φ_j are adjacent for $j = 1, \ldots, k$ and $\Phi \cap \Psi \subseteq \Phi_j$ for $j = 0, \ldots, k$. It is trivial to see that flag-connectedness implies connectedness. The following property gives a more general result. We omit the proof here, but it can be found in [17].

Proposition 1.1.8. *Let $\mathcal{P}$ be a poset with properties (P1) and (P2). Then $\mathcal{P}$ is strongly connected if and only if it is strongly flag-connected.*

Hence the property (P3) may take an equivalent form.

(P3') $\mathcal{P}$ is strongly flag-connected.

The next and last defining property is responsible for the strong analogy between abstract and convex polytopes. It is also called the *diamond condition*.

(P4) For each $i = 0, 1, \ldots, n-1$, if F and G are two incident faces of $\mathcal{P}$, of ranks $i-1$ and $i+1$ respectively, then there are precisely *two* i-faces H of $\mathcal{P}$ such that $F < H < G$.

Property (P4) implies that, if $n \geq 1$, for each $j = 0, 1, \ldots, n-1$ and each flag Φ of $\mathcal{P}$, there exists exactly one adjacent flag differing from Φ in the j-face. This flag is denoted by Φ^j.

Let us now summarize the definition of an abstract polytope.

Definition 1.1.9. *An abstract n-polytope $\mathcal{P}$ is a poset satisfying properties (P1), (P2), (P3') and (P4).*

The terminology is chosen such that convex polytopes of dimension n are abstract n-polytopes.

An automorphism of an abstract polytope $\mathcal{P}$ is an isomorphism of $\mathcal{P}$ onto itself. The automorphism group of $\mathcal{P}$ is denoted by $\Gamma(\mathcal{P})$ and is often referred to as the group of $\mathcal{P}$. When discussing abstract polytopes we normally are interested in the isomorphism class of a polytope rather than in its actual representation. So isomorphic abstract polytopes are often considered to be the same. Analogically to convex polytopes, we define duality of abstract polytopes. For each abstract polytope $\mathcal{P}$ there exists, up to isomorphism, precisely one abstract polytope that is dual to $\mathcal{P}$. It is denoted by $\mathcal{P}^*$. It is immediate that $\mathcal{P}$ and $\mathcal{P}^*$ have the same automorphism group. Therefore, in this thesis, we also consider dual polytopes to be the same[2].

We introduce the Schläfli symbol for abstract polytopes. Suppose $n \geq 2$, $i \in \{0, 1, \ldots, n-1\}$, F is an $(i-2)$-face and G is an $(i+1)$-face of $\mathcal{P}$ such that F is incident with G. Then we denote $p_i(F, G)$ the number of i-faces (or $(i-1)$-faces) of $\mathcal{P}$ in the section G/F. In that case G/F is isomorphic to the polygon with Schläfli symbol $\{p_i(F, G)\}$. The polytope $\mathcal{P}$ is called *equivelar of combinatorial Schläfli type* $\{p_1, p_2, \ldots, , p_{n-1}\}$ if the numbers $p_i(F, G)$ depend only on i, but not on the faces F and G chosen. We then set $p_i := p_i(F, G)$. For convex polytopes this symbol coincides with the classical Schläfli symbol.

We now define regularity of abstract polytopes.

Definition 1.1.10. *An abstract n-polytope $\mathcal{P}$ is called regular if its automorphism group $\Gamma(\mathcal{P})$ is transitive on its flags.*

By theorem 1.1.5 a regular convex polytope is isomorphic to a combinatorially regular convex polytope. The definition of combinatorially regularity of convex polytopes is the same as definition 1.1.10. This implies the following theorem.

Theorem 1.1.11. *All regular convex polytopes are abstract regular polytopes.*

The next two properties are easy to prove and their proofs can be found in [17].

Proposition 1.1.12. *The group $\Gamma(\mathcal{P})$ of an abstract regular polytope $\mathcal{P}$ is simply flag-transitive. In particular, $|\Gamma(\mathcal{P})| = |\mathcal{F}(\mathcal{P})|$, if $\mathcal{P}$ is finite.*

---

[2]This is a convention we chose to adopt in this thesis. Other authors, such as Pellicer [19] or Hartley [9], always consider two dual polytopes as two different polytopes.

Proposition 1.1.13. *Let $\mathcal{P}$ be an abstract regular n-polytope.*
All sections of $\mathcal{P}$ are regular polytopes, and any two sections which are defined by faces of the same ranks are isomorphic. In particular $\mathcal{P}$ is equivelar and hence possesses a Schläfli symbol.

We now establish important results to link abstract polytopes to string C-groups, which are exposed in section 1.1.3 of this thesis. All these results are proven in [17]. The first property is crucial.

Proposition 1.1.14. *An abstract n-polytope $\mathcal{P}$ is regular if and only if for some flag Φ of $\mathcal{P}$ and each $j = 0, 1, \dots, n-1$, there exists a (unique) involutory automorphism ρ_j of $\mathcal{P}$ such that*

$$\Phi\rho_j = \Phi^j.$$

Take such a flag Φ and an involutory automorphism ρ_j for some j. Let Ψ be a different flag. By definition 1.1.10, there exists an automorphism $\gamma \in \Gamma(\mathcal{P})$ such that $\Phi\gamma = \Psi$. Thus $\Psi\gamma^{-1}\rho_j\gamma = \Psi^j$. Moreover it is trivial that if ρ_j is an involution, the conjugate $\gamma^{-1}\rho_j\gamma$ of ρ_j is also an involution. This shows that such involutory automorphisms as in property 1.1.14 exist for every flag in $\mathcal{P}$. Moreover we see that we may choose a *base flag* $\Phi = \{F_{-1}, F_0, \dots, F_k\}$ in $\mathcal{P}$. If ρ_j is the involutory automorphism mapping the base flag on its j-adjacent flag, conjugations of ρ_j map the other flags on their j-adjacent flags, and this for every $j = 0, 1, \dots, n-1$.

So to sum up, let $\mathcal{P}$ be an abstract regular n-polytope and take Φ a base flag of $\mathcal{P}$. Then the elements $\rho_0, \rho_1, \dots, \rho_{n-1}$ are called the *distinguished generators* of $\Gamma(\mathcal{P})$ (with respect to the base flag Φ). We get the following property, proved in [17].

Proposition 1.1.15. *Let $\mathcal{P}$ be an abstract regular n-polytope and $\rho_0, \rho_1, \dots, \rho_{n-1}$ the distinguished generators of its group with respect to some flag. Then*

$$\Gamma(\mathcal{P}) = \langle \rho_0, \dots, \rho_{n-1} \rangle.$$

Furthermore the distinguished generators satisfy a special property, called the *intersection property*.

Proposition 1.1.16. *Let $\rho_0, \dots, \rho_{n-1}$ be the distinguished generators of $\Gamma(\mathcal{P})$ and $N = \{0, 1, \dots, n-1\}$. If $I, J \subseteq N$, then*

$$\langle \rho_i \mid i \in I \rangle \cap \langle \rho_j \mid j \in J \rangle = \langle \rho_i \mid i \in I \cap J \rangle.$$

The next theorem describes exactly the automorphism group of an abstract regular n-polytope. Its proof involves various properties and lemmas about the distinguished generators, which we will not deepen in this thesis. They can all be found in [17].

Theorem 1.1.17. *Let $\mathcal{P}$ be an abstract regular n-polytope with Schläfli symbol $\{p_1, p_2, \ldots, p_{n-1}\}$. Then its automorphism group $\Gamma(\mathcal{P})$ is generated by involutions $\rho_0, \ldots, \rho_{n-1}$ satisfying $(\rho_i\rho_j)^{p_{ij}} = \varepsilon$ for $0 \leq i \leq j \leq n-1$ where*

$$p_{ij} = \begin{cases} 1, \text{ if } i = j, \\ p_j, \text{ if } i = j-1, \\ 2, \text{ if } i \leq j-2. \end{cases}$$

Moreover $\Gamma(\mathcal{P}) = \langle \rho_0, \ldots, \rho_{n-1} \rangle$ verifies the intersection property.

Note that theorem 1.1.17 implies that the generators ρ_i and ρ_j commute if $|i-j| \geq 2$.

1.1.3 C-groups

In section 1.1.2, we showed that the combinatorial structure of an abstract regular polytope is completely determined by the distinguished generators of its group $\Gamma(\mathcal{P})$. In this section we establish the theory about the so-called *string C-groups* and show that for every string C-group there exists an abstract regular polytope whose group is this string C-group. Together with section 1.1.2 we hence establish a one-to-one correspondence between abstract regular polytopes and string C-groups.

We begin with the definition of a C-group.

Definition 1.1.18. *Let Γ be a group generated by involutions $\rho_0, \ldots, \rho_{n-1}$. The group Γ is called a C-group*[3] *if Γ satisfies the intersection property with respect to its generators; that is for each $I, J \subseteq N$, with $N = \{0, 1, \ldots, n-1\}$,*

$$\langle \rho_i \mid i \in I \rangle \cap \langle \rho_j \mid j \in J \rangle = \langle \rho_i \mid i \in I \cap J \rangle.$$

In this thesis we will always abbreviate the sentence "Γ satisfies the intersection property with respect to its generators" by "the generators satisfy (IP)". It is immediate from the definition that the subgroups $\langle \rho_j \mid j \in J \rangle$ are themselves C-groups.

[3]The letter "C" stand for "Coxeter", though not every C-group is a Coxeter group.

Definition 1.1.19. *A C-group is called a string C-group if its generators satisfy the relations*

$$(\rho_i \rho_j)^2 = \varepsilon \text{ if } i, j = 0, \ldots, n-1 \text{ and } |i-j| \geq 2. \tag{1.2}$$

By theorem 1.1.17 if a group Γ is the automorphism group of an abstract regular polytope $\mathcal{P}$, then Γ is a string C-group.

The following theorem is the main characterization result. We only sketch the idea of the proof. The interested reader may find the complete proof in [17].

Theorem 1.1.20. *Let $n \geq 1$, and let $\Gamma = \langle \rho_0, \ldots, \rho_{n-1} \rangle$ be a string C-group. Then Γ is the automorphism group of an abstract regular n-polytope $\mathcal{P}$.*

Proof. We construct an abstract regular n-polytope $\mathcal{P}$ from the string C-group Γ. For $j = 0, \ldots, n-1$, we define

$$\Gamma_j := \langle \rho_i \mid i \neq j \rangle.$$

Set

$$\Gamma_{-1} = \Gamma_n := \Gamma.$$

For $j = -1, 0, \ldots, n$, we take the set of j-faces of $\mathcal{P}$ as the set of all right cosets $\Gamma_j \gamma$ in Γ, with $\gamma \in \Gamma$. Several lemmas and properties show among others that there is a partial order on $\mathcal{P}$, that Γ acts on $\mathcal{P}$ as a family of order preserving automorphisms and that this action is faithful. The main work is to prove that $\mathcal{P}$ satisfies properties (P1), ..., (P4). The details are done in section 2E of [17]. $\square$

This theorem implies the following corollary.

Corollary 1.1.21. *The string C-groups are precisely the groups of abstract regular polytopes.*

The one-to-one correspondence between abstract regular polytopes and string C-groups is now clearly established. This inspires us of considering abstract regular polytopes and string C-groups as being the same objects.

In real applications, the hardest property to verify for string C-groups is (IP). The following proposition simplifies this procedure by reducing the number of cases to verify.

Proposition 1.1.22. *Let $\Gamma = \langle \rho_0, \dots, \rho_{n-1} \rangle$ be a group generated by involutions which satisfy the relations (1.2), and suppose that its subgroup $\Gamma_{n-1} := \langle \rho_0, \dots, \rho_{n-2} \rangle$ is a string C-group (with respect to its generators).*

a) If $\Gamma_0 := \langle \rho_1, \dots, \rho_{n-1} \rangle$ is also a string C-group, and $\Gamma_{n-1} \cap \Gamma_0 = \langle \rho_1, \dots, \rho_{n-2} \rangle$, then Γ itself is a string C-group.

b) If $\Gamma_{n-1} \cap \langle \rho_k, \dots, \rho_{n-1} \rangle = \langle \rho_k, \dots, \rho_{n-2} \rangle$ for each $k = 1, \dots, n-1$, then Γ is also a string C-group.

1.2 The Symmetric and Alternating Groups

1.2.1 Definitions

In this section we recall basic definitions and results about symmetric and alternating groups. We mainly work with [23] and [28].

Definition 1.2.1. *Let Ω be a finite set. The symmetric group $Sym(\Omega)$ is the group of all permutations of the set Ω. In particular if $\Omega = \{1, 2, \dots, n\}$, where n is a positive integer, $Sym(\Omega)$ is denoted $Sym(n)$.*

Every permutation on $\Omega = \{1, 2, \dots, n\}$ is determined by the images of the elements of Ω. Thus there are exactly $n!$ different permutations and so

$$|Sym(n)| = n!$$

Let ρ be a permutation. A notation for ρ is obtained by considering the *cycles* of ρ. Every permutation ρ is written as a product of disjoint cycles. A permutation containing one cycle of length 2 and fixing all the other points is called a *transposition*. If it contains two cycles of length 2 and fixes all the other points, it is called a *bi-transposition*. The *cycle type* of a permutation is simply a list of the lengths of the cycles, usually abbreviated in some way.

Example 1.2.2. *The identity has cycle type (1^n) and a transposition has cycle type $(2, 1^{n-2})$. The permutation $(1,2)(3,4,5)(6,7)(8,9,10,11) \in Sym(20)$ has cycle type $(4, 3, 2^2, 1^9)$.*

The following property is easy to verify.

Proposition 1.2.3. *The symmetric group is generated by the set of transpositions. More specifically the symmetric group is generated by all* $(1, i)$ *with* $2 \leq i \leq n$.

If n is big, it may be hard to check this property. So there is a lemma which is useful to determine whether a group G is isomorphic to $Sym(n)$ or not. It can be found in [20].

Lemma 1.2.4. *If a subgroup* Γ *of* $Sym(n)$ *contains the transposition* $(n-1, n)$ *as well as a subgroup acting transitively on* $\{1, \dots, n-1\}$ *while keeping* n *fixed, then* $\Gamma = Sym(n)$.

We now define the alternating group.

Definition 1.2.5. *A permutation* ρ *is said to be even if* ρ *is the product of an even number of transpositions*[4]*. Otherwise* ρ *is called an odd permutation. The normal subgroup of* $Sym(n)$ *consisting of all even permutations is called the alternating group on* n *elements, and we denote it by* $Alt(n)$.

It is easy to prove that

$$|Alt(n)| = \frac{n!}{2}.$$

In analogy to property 1.2.3, we have the following property for the alternating groups.

Proposition 1.2.6. *The alternating group* $Alt(n)$ *is generated by the set of all* 3*-cycles.*

In this thesis we will often work with conjugacy classes. So a natural question to ask is when two permutations in $Sym(n)$, respectively $Alt(n)$, are conjugate. The following properties give the answer. They are very well-known results, that can be found in a lot of books about permutation groups (for instance [23], [10] or [28]).

Proposition 1.2.7. *Two permutations are conjugate in* $Sym(n)$ *if and only if they have the same cycle type.*

---

[4]There are several equivalent definitions of an *even permutation*, but this is the easiest one to work with.

For $Alt(n)$ the problem is a bit more complicated. If two permutations of same cycle type are conjugate only by odd permutations, then they are not conjugate in $Alt(n)$. Whereas in $Sym(n)$ there is one conjugacy class for each cycle type, in $Alt(n)$ there exists cycle types corresponding to two different conjugacy classes. In fact the following property is proven in [28], in chapter 2.

Proposition 1.2.8. *The conjugacy classes in $Alt(n)$ correspond to cycle types if and only if there is a cycle of even length or there are two cycles of equal length, whereas a cycle type consisting of distinct odd lengths corresponds to two conjugacy classes in $Alt(n)$.*

1.2.2 The Automorphism Group of $Sym(n)$ and $Alt(n)$

We denote the *automorphism group* of a group G by $Aut(G)$.

Definition 1.2.9. *The inner automorphisms of a group G are the automorphisms Φ_g for $g \in G$ defined by*

$$\begin{aligned} \Phi_g : G &\to G \\ x &\mapsto g^{-1}xg. \end{aligned}$$

The group of inner automorphisms of G is denoted by $Inn(G)$. Furthermore $Inn(G)$ is a normal subgroup of $Aut(G)$.

It is easy to check that $\Phi_g \Phi_h = \Phi_{gh}$, and that $\Phi_g = \Phi_h$ if and only if $gh^{-1} \in Z(G)$, where $Z(G)$ is the centre of G. Hence the map Φ defined by

$$\begin{aligned} \Phi : G &\to Inn(G) \\ g &\mapsto \Phi_g \end{aligned}$$

is a homomorphism with kernel $Z(G)$. Therefore

$$Inn(G) \cong G/Z(G).$$

Definition 1.2.10. *The outer automorphism group of G, denoted by $Out(G)$, is defined as the quotient $Aut(G)/Inn(G)$.*

Note that, despite its name, the elements of the outer automorphism group are not automorphisms. This group is merely a quotient group, not a subgroup of $Aut(G)$.

We now state the following well-known result (for more details see [23]).

Theorem 1.2.11. *If $n \geq 3$ and $n \neq 6$, any automorphism of $Sym(n)$ is inner and any automorphism of $Alt(n)$ is obtained by conjugation with an element in $Sym(n)$. Thus*

$$Aut(Sym(n)) = Aut(Alt(n)) = Sym(n).$$

Hence for $n \neq 6$, every automorphism in $Sym(n)$ and $Alt(n)$ is a conjugation by an element of $Sym(n)$.

In the case $n = 6$, the following property holds.

Proposition 1.2.12. *There are exceptional automorphisms in $Sym(6)$ and $Alt(6)$. More precisely,*

$$Aut(Sym(6)) = Aut(Alt(6)) \text{ and } |Aut(Sym(6)) : Inn(Sym(6))| = 2.$$

Hence if we will work in $Sym(6)$, respectively $Alt(6)$, later, we have to be careful, because not every automorphism will be obtained by conjugation with elements of $Sym(6)$. There are automorphisms in $Sym(6)$, respectively $Alt(6)$ that are no conjugation. The next property gives a more precise result on this. Its proof may be found in [23].

Proposition 1.2.13. *Any exceptional automorphism of $Sym(6)$ maps transpositions to permutations of cycle type (2^3). Any exceptional automorphism of $Alt(6)$ exchanges the two conjugacy classes of elements of order 3.*

1.2.3 The Linear Groups and Exceptional Isomorphisms

This section is mainly based on [28] and [25].

Let V be a vector space of dimension n over a finite field $\mathbb{F}_q$ of order $q = p^f$. The *general linear group* $GL(V)$ is the set of invertible linear maps from V to itself. Without much loss of generality, we may take V as the vector space $\mathbb{F}_q^n$ of n-tuples of elements of $\mathbb{F}_q$, and identify $GL(V)$ with the group of invertible $n \times n$ matrices over $\mathbb{F}_q$. This group is denoted by $GL(n, q)$. The center Z of $GL(n, q)$, which consists of all the scalar matrices λI_n, where I_n is the identity matrix and $0 \neq \lambda \in \mathbb{F}_q$, is a cyclic normal subgroup of $GL(n, q)$. The quotient $GL(n, q)/Z$ is called the *projective linear group*, and is denoted $PGL(n, q)$. The determinant map is a group homomorphism from $GL(n,q)$ onto the multiplicative group of the field. So its kernel is a normal subgroup, called the *special linear group* and denoted $SL(n,q)$. It consists of all the matrices of determinant 1. Similarly we can quotient $SL(n,q)$ by its center and we obtain the *projective special linear group* $PSL(n,q)$[5].

We quickly discuss the outer automorphisms of these groups, because we will use these results later. For more details and proofs, we suggest to read [28]. Outer automorphisms of all the classical groups may be divided in *diagonal*, *field* and *graph* automorphisms. The diagonal automorphisms are induced by conjugation by diagonal matrices (with respect to a suitable basis). In the case of the linear groups, $PGL(n,q)$ acts as a group of automorphisms of $PSL(n,q)$. The quotient $PGL(n,q)/PSL(n,q)$ is called the group of diagonal outer automorphisms.

The field automorphisms are induced by automorphisms of the underlying field. In the case of $GL(n,q)$ the automorphism group of the field $\mathbb{F}_q$, generated by the *Frobenius* automorphism $x \mapsto x^p$, induces an automorphism of $GL(n,q)$ by mapping each matrix entry to its pth power. Taking the semidirect[6] product of $GL(n,q)$ with this group of field automorphisms gives us a group $\Gamma L(n,q)$. Correspondingly the extensions of $SL(n,q)$, $PGL(n,q)$ and $PSL(n,q)$ by the induced group of field automorphisms is denoted $\Sigma L(n,q)$, $P\Gamma L_(n,q)$ and $P\Sigma L(n,q)$.

In the case of the linear group, the graph automorphism is best explained by the concept of *duality*. In matrix terms, duality replaces each matrix by the transpose of its inverse. This gives an automorphism of the general and special linear group. Note that for $n = 2$, duality is an inner automorphism of $SL(2,q)$ induced by conjugation with $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. For $n > 2$ however, duality is not inner, even in $GL(n,q)$. In [28], it is shown that these three classes are the only outer automorphisms of $PSL(n,q)$.

To finish this section, we recall some known isomorphisms between symmetric and linear groups and between alternating and linear groups. The

[5]As defined here $PSL(n,q)$ is not necessarily a subgroup of $PGL(n,q)$. However there is an obvious isomorphism between $PSL(n,q)$ and a normal subgroup of $PGL(n,q)$.

[6]The exact definitions of group products will be explained later in section 4.1.

most important isomorphisms are the following:

$$\begin{aligned} PSL(2,2) &\cong Sym(3) \\ PSL(2,3) &\cong Alt(4) \\ PSL(2,4) \cong PSL(2,5) &\cong Alt(5) \\ PSL(2,9) &\cong Alt(6) \\ PSL(4,2) &\cong Alt(8) \end{aligned} \tag{1.3}$$

We only prove the isomorphism $PSL(2,9) \cong Alt(6)$, because we will use it in section 5.3.

To show this isomorphism, it is convenient to work in $PSL(2,9)$ as a group of permutations of the 1-dimensional subspaces of $\mathbb{F}_9^2$. Therefore we label the 1-spaces by the ratio of its coordinates; that is $\langle(x,1)\rangle$ is labelled x and $\langle(1,0)\rangle$ is labelled ∞. Hence $PSL(2,9)$ acts on the set $\mathbb{F}_9 \cup \{\infty\}$, called the projective line on 10 points and denoted $PL(9)$. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,9)$ acts on the projective line as $z \mapsto \frac{az+b}{cz+d}$. Thus $PGL(2,9)$ acts faithfully on the projective line. Notice that any two points of the projective line determine a basis of the 2-space, up to scalar multiplications of the two basis vectors separately. Given any change of basis matrix, we can multiply by a diagonal matrix to make the determinant of the product 1. Thus $PSL(2,9)$ is also 2-transitive on the points of the projective line. In order to prove $PSL(2,9) \cong Alt(6)$, we associate the ten points of $PL(9)$ to the ten partitions of six points into two subsets of size 3. We set $\mathbb{F}_9 = \{0, \pm 1, \pm i, \pm 1 \pm i\}$, with $i^2 = -1$. Let the 3-cycle $(1,2,3)$ act on the points by $z \mapsto z+1$ and let $(4,5,6)$ act by $z \mapsto z+i$. The point ∞ is fixed by these two permutations and thus we associate the partition $(123|456)$ to the point ∞. We may chose the point 0 to correspond to the partition $(423|156)$. The rest of the correspondences is determined by the 3-cycles above. By adding the map $z \mapsto -\frac{1}{z}$ we generate the group $PSL(2,9)$. Moreover we can check that this map acts on the points in the same way as the bitransposition $(2,3)(1,4)$. Hence we have a homomorphism from $PSL(2,9)$ onto $Alt(6)$. It is easy to check that $|PSL(2,9)| = 360 = |Alt(6)|$ and thus the two groups are isomorphic.

We can even prove more. It is possible to prove that an odd permutation in $Sym(6)$ realises a field automorphism of $\mathbb{F}_9$ and hence that $Sym(6) \cong P\Sigma L(2,9)$.

Chapter 2

The CPR-Graphs

In this chapter we introduce the subject of *CPR graphs*. They are graphs associated to the automorphism group $\Gamma(\mathcal{P})$ of an abstract regular polytope $\mathcal{P}$. As seen in section 1.1, the group $\Gamma(\mathcal{P})$ of a polytope $\mathcal{P}$ is a string C-group. So in fact a CPR graph is a graph that encodes information about string C-groups. The term CPR stands for *C-group permutation representation*.

In section 2.1 we define CPR graphs and illustrate that they are useful tools while working with string C-groups. In section 2.2, we treat the special case where the string C-group is generated by exactly 3 involutions. Hence we associate them to polyhedra. Finally in section 2.3 we explain some results associated to symmetric and alternating groups, that are proved with the help of CPR graphs.

We mainly base this chapter on [19] but complete some explanations by referring to the PhD thesis of Pellicer, [18].

2.1 Definition of CPR Graphs

We first give the formal definition of a CPR graph.

Definition 2.1.1. *Let $\mathcal{P}$ be an abstract regular n-polytope and let $\Gamma(\mathcal{P}) = \langle \rho_0, \rho_1, \ldots, \rho_{n-1} \rangle$ be its automorphism group. Take π an embedding of $\Gamma(\mathcal{P})$ in the symmetric group $Sym(m)$ for some m*[1]*. The CPR*

[1] This is possible by Cayley's theorem. For more information on this subject see [20].

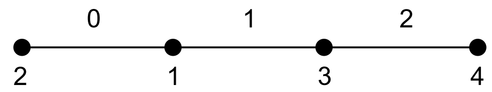

Figure 2.1: CPR graph of the tetrahedron

graph G of $\mathcal{P}$ given by π is a n-edge-labelled multigraph with vertex set $V(G) = \{1, 2, \ldots, m\}$ such that ij is an edge of G of label k if $(\pi\rho_k)i = j$.

The loops, obtained for $i = j$ play no role and are ignored. If the embedding π is clear from the context, we only refer to "a CPR graph of the polytope $\mathcal{P}$" or "a CPR graph of the string C-group Γ". In this thesis the embedding is always obvious, because we are working with symmetric and alternating groups. As the generators of the string C-group $\Gamma(\mathcal{P})$ are all involutions, the edges of each label k of a CPR graph G represent pairs of vertices of G interchanged by $\pi\rho_k$. Moreover all the edges of each label k form a matching on G.

Remark 2.1.2. *A matching in a graph G is a set M of independent edges.*

Definition 2.1.3. *An n-edge-labelled multigraph G with the properties that the set of edges of each label $k \in \{0, 1, \ldots, n-1\}$ forms a matching M_k on G, and that M_k represents a different pairing of the vertices of G from M_l for $k \neq l$, is called a proper n-edge-labelled graph.*

Using this definition and the reasoning before, we conclude that every CPR graph is a proper n-edge-labelled graph.

Remark 2.1.4. *Note that $\Gamma(\mathcal{P})$ may also be considered as a group of permutation on the flags of $\mathcal{P}$. In that case, G is just the Cayley graph of $\Gamma(\mathcal{P})$. Similarly one may consider $\Gamma(\mathcal{P})$ acting on the set of j-faces of $\mathcal{P}$, for $j = 0, \ldots, n-1$. Then G is called the j-face CPR graph of $\mathcal{P}$. However in this thesis we only work with $j = 0$. Hence if we speak about CPR graphs, it always means vertex CPR graphs.*

As an example, we establish the CPR graph of a tetrahedron. It's automorphism group is $\Gamma(\mathcal{P}) = \langle (1,2), (1,3), (3,4) \rangle = Sym(4)$. The CPR graph G contains 4 vertices, labelled $1, \ldots, 4$. There is an edge of label 0 between 1 and 2, an edge of label 1 between 1 and 3 and an edge of label 2 between 3 and 4. The CPR graph is shown in figure 2.1.

To simplify notations, $G_{0,\ldots,n-1}$ denotes from now on an n-edge-labelled graph with edge labels $0, \ldots, n-1$, and for any subset $I = \{i_1, \ldots, i_k\}$ of

$\{0, \ldots, n-1\}$, $G_{i_1,\ldots,i_k}$ denotes the spanning subgraph (including all the vertices of G) of $G_{0,\ldots,n-1}$ whose edge set consists of the edges with labels $i \in I$.

Given a CPR graph of a regular polytope $\mathcal{P}$, we can consider the faithful action of $\Gamma(\mathcal{P})$ on the vertices $\{1, \ldots, m\}$. This allows us to establish details of G given $\mathcal{P}$, and vice-versa.

We now give some useful propositions about CPR graphs.

Proposition 2.1.5. *Let $G = G_{0,\ldots,n-1}$ be a CPR graph of a regular polytope $\mathcal{P}$, and let $|i - j| \geq 2$. Then every connected component of $G_{i,j}$ is either a single vertex, a single edge, a double edge or an alternating square.*

We quickly explain the proof of this proposition.

Proof. $G_{i,j}$ is the union of the matchings determined by ρ_i and ρ_j. As they are involutions, the connected components are either *alternating* paths (including isolated vertices) or *alternating* even cycles (including double edges). A path of length greater than 1 means that the involutions ρ_i and ρ_j are not commuting. This contradicts the fact $|i - j| \geq 2$. Similarly an even cycle of length greater then 4 comes from a non-commuting pair of involutions. □

By observing the way in which the subgroup $\langle \rho_i, \rho_{i+1} \rangle = D_{2p_{i+1}}$, with p_{i+1} the order of $\rho_i \rho_{i+1}$, acts on each connected component of $G_{i,i+1}$, it is possible to establish the Schläfli symbol of a regular polytope given any of its CPR graphs. Details on this may be found in [19].

The next three results relate the automorphism group of a regular polytope to the automorphism group of its CPR graphs. We omit the proofs, but they are all explained in [19].

Lemma 2.1.6. *Let G be a CPR graph of a polytope $\mathcal{P}$, let Λ be any group of automorphism of G as a labelled graph, and let O_v be the orbit under Λ for each vertex v. Then the group*

$$N = \{\phi \in \Gamma(\mathcal{P}) \mid \phi(v) \in O_v \text{ for all } v \in V(G)\}$$

is a normal subgroup of $\Gamma(\mathcal{P})$.

Proposition 2.1.7. *Let G, $\mathcal{P}$ and N be as in lemma 2.1.6. Let G' be the n-edge labelled graph with vertex set*

$$V(G') = \{O_v \mid v \in V(G)\},$$

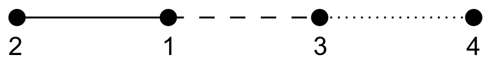

Figure 2.2: CPR graph of the tetrahedron

such that O_vO_w is an edge of G' labelled i if and only if $v'w'$ is an edge labelled i for some $v' \in O_v$ and some $w' \in O_w$. If G' is a CPR graph of a regular polytope $\mathcal{P}'$, then $\mathcal{P}'$ is the quotient[2] of $\mathcal{P}$ determined by the subgroup N of $\Gamma(\mathcal{P})$.

These two results show that the subgroup N plays an important role. Note that N might often be trivial.

Proposition 2.1.8. *Let Λ be a subgroup of the automorphism group $\Gamma(\mathcal{P})$ of a regular polytope $\mathcal{P}$, such that Λ does not contain any non-trivial normal subgroup of $\Gamma(\mathcal{P})$. Then, Λ determines a connected CPR graph for $\mathcal{P}$. Conversely, we can consider such a subgroup with any connected CPR graph G of $\mathcal{P}$.*

The last proposition may be used to find all connected CPR graphs for a given regular polytope $\mathcal{P}$ from the subgroup lattice of $\Gamma(\mathcal{P})$. Note that conjugate subgroups Λ give rise to the same CPR graph, up to isomorphism.

2.2 CPR Graphs and Polyhedra

In this section we show some particular results for CPR graphs of regular polyhedra. Hence from now on $n = 3$.

First we set a convention to denote CPR graphs of regular polyhedra. When working with CPR graphs of polyhedra, a black continued line corresponds to the edge labelled 0, a black dashed line to an edge labelled 1 and a black dotted line to an edge labelled 2. With this convention the CPR graph of the tetrahedron (see figure 2.1) becomes figure 2.2.

The aim of this section is to establish when a 3-labelled graph G is a CPR graph. We already know that G has to be a proper 3-edge-labelled graph. This condition encodes the information that $\Gamma(\mathcal{P})$ is a group generated by three involutions. The fact that two out of these three involutions commute

[2]The broader theory of quotient polytopes is beyond the scope of this work; nevertheless, the interested reader will find details in [17].

is expressed by proposition 2.1.5. We give now three criteria that help determine whether a 3-labelled graph is a CPR graph. In each case it only remains to prove the intersection property (this must unfortunately be done by hand). We omit again the proofs. They may be found in [19].

Remark 2.2.1. *It is possible to show that, in general, regular polytopes always have several connected CPR graphs. This is done in [18]. Therefore we establish all results for connected CPR graphs. Moreover, as we treat symmetric and alternating groups in this thesis, it is clear that their CPR graphs are connected, because these groups have transitive actions.*

Proposition 2.2.2. *Let $G = G_{0,1,2}$ be a connected, proper 3-edge-labelled graph satisfying the condition that every connected component of $G_{0,2}$ is either a single vertex, a single edge, a double edge or an alternating square. If $G_{0,1}$ (or $G_{1,2}$) has two connected components with at least two vertices such that their numbers of vertices are relatively prime, then G is a CPR graph.*

This proposition is purely based on the graph of G. The next proposition also involves the action of subgroups of $\Gamma(\mathcal{P})$ on G.

Proposition 2.2.3. *Let $G = G_{0,1,2}$ be a connected, proper 3-edge-labelled graph satisfying the condition that every connected component of $G_{0,2}$ is either a single vertex, a single edge, a double edge or an alternating square. If G has a vertex invariant under $\langle \rho_0, \rho_1 \rangle$ or under $\langle \rho_1, \rho_2 \rangle$, then G is a CPR graph.*

Proposition 2.2.4. *Let $G = G_{0,1,2}$ be a connected, proper 3-edge-labelled graph satisfying the condition that every connected component of $G_{0,2}$ is either a single vertex, a single edge, a double edge or an alternating square. If G has an edge u_0v_0 of label 1 such that no edge of label 0 (or dually, 2) is incident to either u_0 or v_0 and such that u_0v_0 is not the central edge of a connected component of $G_{0,1}$ that is a path of odd length, then $G_{0,1,2}$ is a CPR graph.*

These three criteria turn out to be very useful to find the third involution, once the two others are found. Unfortunately (IP) is still left to be checked by hand.

2.3 CPR Graphs applied to Symmetric and Alternating Groups

In this section we present two different results on symmetric and alternating groups. The results are each time established by using CPR graph techniques.

The first result deals with symmetric groups. In [16], it may be found that, up to isomorphism and duality, there are 35 polyhedra with automorphism group $Sym(7)$. This result is based on computer search. In his PhD thesis, Pellicer comes to the same result by using CPR graph techniques. Note that Pellicer counts the polyhedra up to isomorphism but not up to duality. Hence he gets a result of 64. In order to do that he constructs all the possible 3-labelled CPR graphs corresponding to $Sym(7)$. Hence he constructs proper 3-edge-labelled graphs on 7 vertices satisfying the condition that every connected component of $G_{0,2}$ is either a single vertex, a single edge, a double edge or an alternating square and such that

a) the graph is connected (otherwise it would not generate all of $Sym(7)$).

b) the group generated by the involutions satisfy the intersection property.

c) the group generated by the involutions is $Sym(7)$.

More details on this process may be found in [18].

The second result is about polyhedra having an automorphism group isomorphic to $Alt(n)$. In fact, in [19], and with more details in [18], the following theorem is proven.

Theorem 2.3.1. *No polyhedron has automorphism group isomorphic to $Alt(n)$ with $n \leq 4$ or $n = 6, 7, 8$.*
For $n = 5$ or $n \geq 9$ there is a polyhedron with automorphism group isomorphic to $Alt(n)$.

We only give the main ideas of the proof of this theorem.

Proof. To prove the first half of the theorem, we exclude the cases $n \leq 4$ by noticing that there are not enough involutions in $Alt(n)$ in these cases. For every $n = 6, 7, 8$, we try to construct all the possible CPR graphs and notice that their automorphism group is each time a subgroup of $Alt(n)$.

The second half is proven by showing each time a polyhedron whose automorphism group is $Alt(n)$. We do not prove the theorem for $n = 5$, because it is well known that $Alt(5)$ is the automorphism group of the hemi-dodecahedron, the hemi-icosahedron and the hemi-great dodecahedron. For $n \geq 9$, we first construct a family of CPR graphs representing regular polyhedra with automorphism group isomorphic to $Alt(8k + 1)$. Then we show that it is possible to modify these graphs in order to obtain regular polyhedra with automorphism group $Alt(n)$ for $n \geq 21$. For $9 \leq n \leq 20$, we have to construct each CPR graph separately. In [19], one may find a list of all these graphs. $\square$

Chapter 3

Known Results and Basic Idea

After having established the mathematical background with which we work in this Master's thesis, we now summarize the main result on which we base our research. This result comes mainly from article [22]. Some parts seem to us not very well explained in that article. We try to clear the situation up in section 3.1.

In section 3.2 we explain the basic idea we follow to find the number of abstract regular polyhedra on which symmetric and alternating groups act as automorphism groups.

3.1 Groups Generated by Three Involutions

In this section we prove two known results, on which we base this thesis. We take the proof from an article by *Cherkassoff* and *Sjerve* [22], but we make it a bit clearer by adding some details. We prove in which cases $Sym(n)$ and $Alt(n)$ have a presentation of the form

$$\langle \rho_0, \rho_1, \rho_2 \mid \rho_0^2 = \rho_1^2 = \rho_2^2 = id, \rho_0\rho_2 = \rho_2\rho_0, \mathrm{ETC}\rangle. \tag{3.1}$$

Here ETC denotes extra relations we need to generate a finite group[1]. We also avoid the trivial cases. So no ρ_i is equal to the identity and they are all mutually distinct. Moreover we do not want ρ_1 to commute with ρ_0 nor

[1]If we leave out these extra relations, we get an infinite Coxeter group. However here we want a finite group, that is the quotient of a Coxeter group defined by some extra relations. For more details on this subject, see [17].

with ρ_2[2]. In fact the article analyses in which cases $Sym(n)$ and $Alt(n)$ can be written in the form of a string C-group, but without paying attention to (IP). We will analyse this condition afterwards to link the article with our subject.

The two results of the article are given in the following theorems.

Theorem 3.1.1. *The symmetric group $Sym(n)$ has a presentation as in (3.1), if and only if $n \geq 4$.*

Theorem 3.1.2. *The alternating group $Alt(n)$ has a presentation as in (3.1) if and only if $n = 5$ or $n \geq 9$.*

First we prove theorem 3.1.1.

Proof. We split the proof in two parts: the negative part and the positive part. We first do the negative part. If $n = 1$ or $n = 2$, there are not even three involutions in $Sym(n)$. If $n = 3$, there are exactly 3 involutions in $Sym(3)$, namely $(1,2)$, $(1,3)$ and $(2,3)$. It is easy to see that no two out of these three involutions commute. Hence if $n < 4$, $Sym(n)$ cannot be written in the form (3.1).

To do the positive part, we distinguish between two cases, if n is odd or even. If n is odd, in particular $n = 2k+1$, we set

$$\begin{aligned} \rho_0 &= (3,4)(5,6)\dots(2k-1,2k), \\ \rho_1 &= (2,3)(4,5)\dots(2k,2k+1), \\ \rho_2 &= (1,2). \end{aligned} \tag{3.2}$$

We see that ρ_0, ρ_1 and ρ_2 are involutions and ρ_0 commutes with ρ_2. Moreover $(1,2) = \rho_2$, $(1,3) = \rho_1\rho_2\rho_1$, $(1,4) = \rho_0(1,3)\rho_0$, $(1,5) = \rho_1(1,4)\rho_1$ etc. Hence the three involutions generate all $(1,i)$ with $2 \leq i \leq n$. By proposition 1.2.3, these transpositions generate $Sym(n)$. So $\langle \rho_0, \rho_1, \rho_2 \rangle$, with ρ_0, ρ_1 and ρ_2 as in (3.2), is isomorphic to $Sym(n)$. This proves the odd part.

If n is even, hence if $n = 2k$, we set

$$\begin{aligned} \rho_0 &= (3,4)(5,6)\dots(2k-1,2k), \\ \rho_1 &= (2,3)(4,5)\dots(2k-2,2k-1), \\ \rho_2 &= (1,2). \end{aligned} \tag{3.3}$$

[2]This condition is explained in more details in section 3.2.

The same reasoning as in the odd part is applied. This finishes the proof of theorem 3.1.1. □

We can deduce the following corollary from theorem 3.1.1.

Corollary 3.1.3. *For $n \geq 4$, the symmetric group $Sym(n)$ can be written as a string C-group $\langle \rho_0, \rho_1, \rho_2 \rangle$. In particular $Sym(n)$ is the automorphism group of at least one polyhedron.*

Proof. By theorem 3.1.1, we know that $Sym(n)$ has a presentation as in (3.1). We take ρ_0, ρ_1 and ρ_2 as in (3.2) if n is odd, respectively in (3.3) if n is even. The only thing that is left to verify is (IP). For $n = 4$ it is obvious that ρ_0, ρ_1 and ρ_2 verify (IP). For $n \geq 5$, we apply proposition 1.1.22. Set $\Gamma_2 = \langle \rho_0, \rho_1 \rangle$ and $\Gamma_0 = \langle \rho_1, \rho_2 \rangle$. The groups Γ_2 and Γ_0 are obviously string C-groups. The only thing that is left to check is that their intersection is $\langle \rho_1 \rangle$. It is clear that $\langle \rho_1 \rangle$ is contained in $\Gamma_2 \cap \Gamma_0$. No matter whether n is even or odd, the order of $\rho_1\rho_2$ is 6 and hence Γ_0 is a dihedral group of order 12. As $\Gamma_2 \cap \Gamma_0$ is a subgroup of Γ_0, its order must divide 12. Moreover, as $\Gamma_2 \cap \Gamma_0$ contains the group $\langle \rho_1 \rangle$ as a subgroup, its order is 2, 4, 6 or 12. Furthermore every element in Γ_2 fixes the elements 1 and thus every element in $\Gamma_2 \cap \Gamma_0$ fixes 1. There are only four different permutations in Γ_0 that fix 1, namely id, ρ_1, $(\rho_2\rho_1)^2\rho_2$ and $(\rho_1\rho_2)^3$. Thus the order of $\Gamma_2 \cap \Gamma_0$ is 2 or 4. If it was 4, $\Gamma_2 \cap \Gamma_0$ would contain exactly the four permutations mentioned above. So these four elements should be contained in Γ_2. The permutation $(\rho_1\rho_2)^3$ fixes the element 2. A non-trivial permutation in Γ_2 that fixes 2 is of the form $(\rho_1\rho_0)^m\rho_1$, where $(\rho_1\rho_0)^m$ maps 2 onto 3. However then $m = n - 1$ and so $(\rho_1\rho_0)^m\rho_1$ is simply the element ρ_0. Hence the only non-trivial permutation in Γ_2 that fixes 2 is ρ_0 and thus $(\rho_1\rho_2)^3$ is not in Γ_2. This means that the order of $\Gamma_2 \cap \Gamma_0$ is 2 and that $\Gamma_2 \cap \Gamma_0 = \langle \rho_1 \rangle$.

Remark 3.1.4. *The previous argument may be replaced by a geometric argument, but we preferred an algebraic version of it.*

Thus (IP) is verified and $\langle \rho_0, \rho_1, \rho_2 \rangle$ is a string C-group. By theorem 1.1.20, $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$ is the automorphism group of a polyhedron. We compute its Schläfli type.

$$\begin{aligned} \rho_0\rho_1 &= (2, 3, 5, \ldots, 4) \quad \rightarrow \quad p_1 = n - 1, \\ \rho_1\rho_2 &= (1, 3, 2)(4, 5)(6, 7)\ldots \quad \rightarrow \quad p_2 = 6. \end{aligned}$$

Hence we prove even more than corollary 3.1.3. We prove that for every $n \neq 4$, $Sym(n)$ acts as automorphism group on a polyhedron of Schläfli type $\{n-1, 6\}$. This result agrees with [16]. □

Now we prove theorem 3.1.2.

Proof. First we deal with the case $n = 5$. Set

$$\begin{aligned} \rho_0 &= (1,2)(3,4), \\ \rho_1 &= (1,2)(4,5), \\ \rho_2 &= (1,3)(2,4). \end{aligned} \tag{3.4}$$

The group $\langle \rho_0, \rho_1, \rho_2 \rangle$ is clearly of the form (3.1). Moreover if we take

$$\begin{aligned} c_1 &= \rho_0\rho_1 = (3,5,4), \\ c_2 &= \rho_2 c_1 \rho_2 = (1,5,2), \\ c_3 &= c_2^2 c_1 c_2 = (2,4,3), \end{aligned} \tag{3.5}$$

we see that c_1, c_2 and c_3 clearly generate $Alt(5)$. Hence $\langle \rho_0, \rho_1, \rho_2 \rangle$ has a presentation as in (3.1) and is isomorphic to $Alt(5)$.

To prove the rest of the theorem we divide again the proof in a negative and a positive part. First we do the negative part. As already stated in the proof of theorem 2.3.1, if $n \leq 4$, $Alt(n)$ has no presentation as in (3.1). We now deal with the cases $n = 6, 7, 8$. The easiest case is $Alt(7)$. Up to conjugacy, the first involution can be chosen in only one way, namely $(1,2)(3,4)$. As ρ_2 has to commute with ρ_0, there are two choices for ρ_2, either $(1,3)(2,4)$ or $(1,2)(5,6)$. In both cases the action of the group $\langle \rho_0, \rho_2 \rangle$ divides the 7 elements into four orbits; $\{1,2,3,4\}$, $\{5\}$, $\{6\}$ and $\{7\}$ in the first case and $\{1,2\}$, $\{3,4\}$, $\{5,6\}$ and $\{7\}$ in the second case. The involution ρ_1 consists of only two 2-cycles, so it cannot connect all these four orbits into one. Thus we have an intransitive action on the set $\{1, 2, \ldots, 7\}$. Hence ρ_0, ρ_1 and ρ_2 do not generate $Alt(7)$.

In the case $Alt(6)$ we have again two different possibilities for the choice of ρ_0 and ρ_2, namely $\rho_0 = (1,2)(3,4)$ and $\rho_2 = (1,3)(2,4)$ or $\rho_2 = (1,2)(5,6)$. The transitivity argument forces ρ_1 to be $(1,5)(2,6)$ or $(1,5)(4,6)$, up to conjugacy, in the first case and $(2,3)(4,5)$ or $(1,5)(2,3)$ in the second. In the article, the authors compute by machine the order of $\langle \rho_0, \rho_1, \rho_2 \rangle$ in each case and find out that it is strictly smaller than 360. We have elaborated an argument without computer in this thesis. This argument can be found in section 5.3.

The most extensive case is the case of $Alt(8)$. There are two possibilities for ρ_0 up to conjugacy: $(1,2)(3,4)$ and $(1,2)(3,4)(5,6)(7,8)$. For each possible ρ_0 the authors look at all the possible ρ_2 such that the two involutions commute. They do not distinguish between choices of ρ_2 that are conjugate by any conjugation leaving ρ_0 invariant. Furthermore they take the pairs $\{\rho_0, \rho_2\}$ as unordered pairs. This gives a list of seven essentially different choices.

Remark 3.1.5. *In the article the authors mention a list of five different choices, but in fact they forget two choices. We checked the pairs $\{\rho_0, \rho_2\}$, they forget, and it is impossible to find a third involution not commuting with ρ_0 and ρ_2 and such that the three involutions generate $Alt(8)$.*

Now for each of these different choices we take all the possible ρ_1 and compute the order of the group $\langle \rho_0, \rho_1, \rho_2 \rangle$. Every time the order is strictly smaller than the order of $Alt(8)$. We do not present the complete list of possibilities and their associated order here. The interested reader is invited to look it up in [22].

The positive part of the proof is done by induction. We show that it holds for $n = 9, 10, 11, 12, 13, 14, 15, 16$ and then we show that it holds for $Alt(n+8)$ if it holds for $Alt(n)$. We first establish the base cases of the induction. In each case, we define three involutions ρ_0, ρ_1 and ρ_2 satisfying the presentation (3.1). We exhibit an appropriate power $(\rho_0\rho_1)^m$ which is a 3-cycle c_1. Then we find another 3-cycle $c_2 = (i_p, i_q, j)$ where i_p and i_q are involved in c_1, but j is not. The 3-cycle c_1 generates $Alt(3)$ and adjoining c_2 then gives $Alt(4)$. The idea is to find a succession of 3-cycles c_3, c_4, c_5, …, adjoin them to the previous generators to produce a succession of groups isomorphic to $Alt(5), Alt(6), \ldots$. These extra 3-cycles are obtained from the previous ones by conjugation. The authors have analysed the 8 base cases and some details are shown in a table in the article (see table 1 of [22]). Hence for $n = 9, \ldots, 16$ we have three involutions ρ_0, ρ_1 and ρ_2, that satisfy (3.1) and that generate $Alt(n)$.

To establish the inductive step, we observe the following: for each triple of involutions defined above, there exists a partition of $\{1, 2, \ldots, n\}$ into two disjoint non-empty sets S_1 and S_2 and elements $i \in S_1$, $j \in S_2$

such that

$$\rho_0\rho_2 = \rho_2\rho_0, \tag{3.6a}$$
$$\rho_0(S_1) = S_1, \rho_0(S_2) = S_2, \rho_2(S_1) = S_1, \rho_2(S_2) = S_2, \tag{3.6b}$$
$$(i,j) \in \rho_1 \text{ and } \rho_1(S_1 \setminus \{i\}) = S_1 \setminus \{i\}, \rho_1(S_2 \setminus \{j\}) = S_2 \setminus \{j\}, \tag{3.6c}$$
$$(k,i) \in \rho_0 \text{ for some } k \neq i \text{ and } \rho_1(k) = k, \tag{3.6d}$$
$$(\rho_0\rho_1)^m \text{ is a 3-cycle, where } m \text{ is some integer.} \tag{3.6e}$$

Notice that condition (3.6e) is equivalent to the cycle decomposition of $(\rho_0\rho_1)$ having one 3-cycle and all other cycles of length relatively prime to 3. For each $n = 9, \ldots, 16$ the authors of the article show the elements i, j and k and exhibit the partition S_1 and S_2.

Now we extend this data to $Alt(n+8)$ as follows:

$$\begin{aligned}
\rho_0' &= \rho_0(n+1,n+2)(n+3,n+4)(n+5,n+6)(n+7,n+8)\\
\rho_1' &= \rho_1(i,,j)(i,n+1)(n+4,n+5)(n+8,j)\\
\rho_2' &= \rho_2(n+1,n+3)(n+2,n+4)(n+5,n+7)(n+6,n+8)\\
S_1' &= S_1 \cup \{n+1,n+2,n+3,n+4\}\\
S_2' &= S_2 \cup \{n+5,n+6,n+7,n+8\}\\
i' &= n+4, j' = n+5, k' = n+3
\end{aligned} \tag{3.7}$$

It is quite easy to show that the elements ρ_0', ρ_1' and ρ_2' are involutions in $Alt(n+8)$ satisfying conditions (3.6a) - (3.6e). We omit this proof here, but it is done in [22].

To sum up, until now we have shown that there exists three involutions ρ_0, ρ_1 and ρ_2, satisfying conditions (3.6a) - (3.6e), in $Alt(n)$ for $n = 9, \ldots, 16$. We have shown that we can construct such involutions in $Alt(n+8)$. Thus it follows that conditions (3.6a) - (3.6e) hold for $Alt(n)$, with $n \geq 9$. We now prove that such involutions, satisfying (3.6a) - (3.6e), generate $Alt(n)$.

The proof is again by induction on n. We know that it is true for $n = 9, \ldots, 16$. So we assume that $Alt(n)$ is generated by ρ_0, ρ_1, ρ_2 and we want to show that $Alt(n+8)$ is generated by ρ_0', ρ_1' and ρ_2'. By analysing every case for $n = 9, \ldots 16$, we observe that the 3-cycle $(\rho_0\rho_1)^m$ does not involve i or j. Therefore $c_1' = (\rho_0\rho_1)^{m'}$ is identical to c_1. Moreover, as ρ_0 and ρ_1 fix $S_1 \setminus \{i\}$ and $S_2 \setminus \{j\}$ and i and j are not involved in c_1, the 3-cycle c_1 involves only letters from S_1 or S_2. We suppose it is S_1. The case S_2 may be proven in exactly the same way.

Now we consider the sequence of 3-cycles in $Alt(n)$ up to the point where j is adjoined, say $c_1, c_2, \dots, c_{r+1}$, where $c_1 = (\rho_0\rho_1)^m$ and $c_t = W_t\gamma_t W_t^{-1}$, $2 \le t \le r+1$, for some word W_t in ρ_0, ρ_1, ρ_2 and some $\gamma_t \in \langle c_1, \dots, c_{t-1}\rangle$. The involution ρ_0 fixes all S_1 and the only element in S_1 that is mapped into S_2 by ρ_1 is i. However, in the 3-cycle c_{r+1}, the element $j \in S_2$ appears. Hence i must necessarily be involved in the permutation γ_{r+1}. So γ_{r+1} is of the form (i_1, i_2, i) for some $i_1, i_2 \in S_1 \setminus \{i\}$ and $c_{r+1} = (i_3, i_4, j)$ for some $i_3, i_4 \in S_1$.

An analysis of the base case reveals that in each case $W_{r+1} = \rho_1$ and that all the subsequent conjugations are also by generators. We make the inductive assumption that this occurs in $Alt(n)$.

Let W'_t denote the word in $\rho'_0, \rho'_1, \rho'_2$ obtained by replacing each occurrence of ρ_j by ρ'_j. Then the 3-cycles $c'_t = W'_t\gamma'_t W'^{-1}_t$ are identical to c_t for $1 \le t \le r$. Let us compute the 3-cycle $c'_{r+1} = \rho'_1\gamma_{r+1}\rho'_1$. We know that $\rho_1\gamma_{r+1}\rho_1 = (i_3, i_4, j)$. So $\gamma_{r+1} = \rho_1(i_3, i_4, j)\rho_1$, which gives us

$$\begin{aligned} c'_{r+1} = \rho'_1\gamma_{r+1}\rho'_1 &= \rho'_1\rho_1(i_3, i_4, j)\rho_1\rho'_1 \\ &= (i, n+1, j, n+8) \circ (i_3, i_4, j) \circ (i, n+8, j, n+1) \\ &= (i_3, i_4, n+1). \end{aligned}$$

Thus we have added the new letter $n+1$. Conjugation by $\rho'_0, \rho'_2, \rho'_0, \rho'_1, \rho'_0, \rho'_2, \rho'_0, \rho'_1$ in turn yields the new letters $n+2$, $n+4$, $n+3$, $n+5$, $n+6$, $n+8$, $n+7$ and j. Notice that all new conjugations are also by generators. All that remains now is to add the letters in $S_2 \setminus \{j\}$. To do this we merely follow the corresponding sequence in $Alt(n)$ replacing each occurrence of ρ_j by ρ'_j. This finishes the proof of theorem 3.1.2. □

In this case we may also extract a corollary from theorem 3.1.2.

Corollary 3.1.6. *For $n = 5$ and $n \ge 9$, the alternating group $Alt(n)$ can be written as a string C-group $\langle\rho_0, \rho_1, \rho_2\rangle$. In particular $Alt(n)$ is the automorphism group of at least one polyhedron.*

We do not proof this corollary because it was proven in a nice way by using the CPR graphs (see chapter 2, theorem 2.3.1).

Remark 3.1.7. *In [22], theorems similar to 3.1.1 and 3.1.2 are shown for the special linear groups $PSL(2, q)$ and the projective general linear groups $PGL(2, q)$. In fact $PSL(2, q)$ has a presentation as in (3.1) if and only if $q \neq 2, 3, 7, 9$. The case $q = 9$ may be deduced from theorem 3.1.2. As*

$Alt(6) \cong PSL(2,9)$ (see (1.3)), theorem 3.1.2 indicates that $PSL(2,9)$ does not have a presentation as in (3.1). The group $PGL(2,q)$ can be written in the form (3.1) if and only if $q \neq 2$.

3.2 Basic Idea of Work

In this section we explain the basic idea we are going to follow in the next two chapters. Let G be either the symmetric group $Sym(n)$ or the alternating group $Alt(n)$, for a given n. Theorem 1.1.20 and especially corollary 1.1.21 show that abstract regular polytopes and string C-groups may be considered as the same objects. In this thesis our goal is to count the number of abstract regular polyhedra on which G acts as automorphism group. Instead of looking "directly" for the polyhedra, we analyse in how many different ways G may be written as a string C-group. By theorem 1.1.20, we know that for each representation as a string C-group, generated by three involutions, there is a corresponding polyhedron.

By corollary 3.1.3, $Sym(n)$ has at least one representation as a string C-group for $n \geq 4$. Similarly, by corollary 3.1.6, $Alt(n)$ has at least one representation as a string C-group for $n = 5$ and $n \geq 9$. For these cases we want to establish a general formula, depending on n, and giving the exact number of polyhedra on which G has a regular action. Concretely, to find out in how many ways G can be written as a string C-group, we have to find out in how many ways we can choose three involutions $\rho_0, \rho_1, \rho_2 \in G$ such that ρ_0 and ρ_2 commute, the three involutions verify (IP) and they generate all of G. As isomorphic string C-groups yield the same polyhedron we do this counting up to isomorphism. Moreover, we consider dual polyhedra to be equal. So we also do the counting up to duality. This means the following: if $\langle \rho_0, \rho_1, \rho_2 \rangle$ is the automorphism group of a polyhedron $\mathcal{P}$, then $\langle \rho_2, \rho_1, \rho_0 \rangle$ is the automorphism group of the dual polyhedron $\mathcal{P}^*$. Thus for us the groups $\langle \rho_0, \rho_1, \rho_2 \rangle$ and $\langle \rho_2, \rho_1, \rho_0 \rangle$ are the same and are counted only once.

The work is done in essentially five steps. In the first step we count how many non-isomorphic choices there are for an involution ρ_0 in G. By theorem 1.2.11, for $n \neq 6$ the counting is done up to conjugacy for $Sym(n)$ and up to conjugacy by an element in $Sym(n)$ for $Alt(n)$. For $n = 6$, the problem is a bit more difficult. It is analysed in section 4.3 and section 5.3.

The second step is to count in how many different ways, up to isomorphism, an involution ρ_2 commuting with ρ_0 can be added. Up to isomorphism here means that for $n \neq 6$, all choices of ρ_2 that are conjugate by an element in $Sym(n)$ leaving ρ_0 invariant are the same. One important computation to do is to calculate the centralizer $C_G(\rho_0)$ of ρ_0 in G. On the one hand, as ρ_2 commutes with ρ_0, ρ_2 is an involution of this centralizer. On the other hand, the conjugations leaving ρ_0 invariant are exactly the conjugations by elements of $C_{Sym(n)}(\rho_0)$. As mentioned above, the case $n = 6$ is done separately. As we count the polyhedra up to duality, we have to count the pairs $\{\rho_0, \rho_2\}$ as unordered pairs. In this process, we first choose an involution ρ_0 and then an involution ρ_2. Thus if we consider the pair $\{\rho_0, \rho_2\}$ as an unordered pair, we have counted several possibilities twice.

Once we have found the pairs $\{\rho_0, \rho_2\}$, we look for a third involution ρ_1 not necessarily commuting with the other two. In fact the definition of a string C-group (see (1.1.18) and (1.1.19)) sets no restrictions on ρ_1. However in this case we do not want the third involution to commute with any of the other two. Suppose it does and suppose it commutes with ρ_0 (the case if it commutes with ρ_2 is exactly the same and the case if it commutes with both ρ_0 and ρ_2 is even clearer). Then the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ is a group generated by three involutions, such that one commutes with the two others. Thus the string C-group can be written as

$$\langle \rho_0, \rho_1, \rho_2 \rangle = \langle \rho_0 \rangle \times \langle \rho_1, \rho_2 \rangle \cong \mathbb{Z}_2 \times D_{2k},$$

where k is the order of $\rho_1\rho_2$. For $n \geq 4$ this group is never isomorphic to the symmetric group of degree n. The same is true for the alternating group. Hence, as we want the string C-group to be isomorphic to G, we may immediately exclude the case where one involution commutes with the two others. So we look for a third involution that is not commuting with ρ_0 nor with ρ_2. Once again we take the third involution up to isomorphism, which means the same as up to conjugacy for $n \neq 6$. The case $n = 6$ is done completely separated. Hence two involutions ρ_1 and ρ_1' that are conjugate by an element leaving the pair $\{\rho_0, \rho_2\}$ invariant are considered the same.

Step four consists in checking (IP). Up to this step, we have found three involutions, two of them commuting. The only condition that is left, so that $\langle \rho_0, \rho_1, \rho_2 \rangle$ is a string C-group, is (IP). Proposition 1.1.22 helps a lot to check (IP). As we are working in rank 3, the two groups Γ_0 and Γ_2 have really simple structures. Indeed $\Gamma_2 = \langle \rho_0, \rho_1 \rangle$ and $\Gamma_0 = \langle \rho_1, \rho_2 \rangle$. By triviality Γ_2 and Γ_0 are string C-groups. This yields the following lemma.

Lemma 3.2.1. *Let ρ_0, ρ_1 and ρ_2 be three involutions such that ρ_0 and ρ_2 commute. Then $\langle \rho_0, \rho_1, \rho_2 \rangle$ is a string C-group if and only if*

$$\Gamma_2 \cap \Gamma_0 = \langle \rho_0, \rho_1 \rangle \cap \langle \rho_1, \rho_2 \rangle = \langle \rho_1 \rangle.$$

Finally we have got a list of string C-groups generated by three involutions in G. There is no guarantee that these groups are isomorphic to G. Three involutions in G may generate a subgroup of G, but not all of G. Thus the last step consists in checking which ones of the string C-groups are isomorphic to G. This step is really hard to do, because the symmetric and the alternating group have a lot of subgroups. In [11], we did the same work for Suzuki groups. However there the work was much easier, because the only subgroups of Suzuki groups, that could be generated by the three involutions we constructed, were themselves groups of Suzuki type.

To conclude, if we manage to do these five steps for a given n, we will get a general formula that computes the number of abstract polyhedra on which the symmetric group of degree n, respectively the alternating group of degree n, have a regular action.

Chapter 4

The Symmetric Groups

In the previous chapters, we have established the theory with which we are working. We have reminded the main definitions and results about abstract regular polyhedra, string C-groups and the symmetric groups. We have also explained the construction of CPR graphs and have developed some of their properties. We have summarized known results about polyhedra and symmetric groups, which constitute the basis for this thesis and have finally explained our basic idea of work.

In this chapter we start the real research part of this Master's thesis. As explained in section 3.2, we first have to establish a general formula to compute the centralizer of an involution in $Sym(n)$. This is done in section 4.1. In the following section we execute step 2 of the basic idea and count the number of pairs of commuting involutions in $Sym(n)$. In section 4.3, we do the particular case of $Sym(6)$. Finally we give a first general result for $Sym(n)$. In the last section of this chapter we draw a conclusion on our work about $Sym(n)$.

4.1 The Centralizer of an Involution in $Sym(n)$

We establish the general form of the centralizer of an involution ρ in $Sym(n)$, $C_{Sym(n)}(\rho)$. The centralizer of ρ_0 is useful to find the pairs of commuting involutions $\{\rho_0, \rho_2\}$ in $Sym(n)$.

We first recall the definitions of group products, which are used in the general form of the centralizer. Let G and H be groups.

The *direct product* of G and H is defined as

$$G \times H = \{(g,h) \mid g \in G, h \in H\},$$

with identity $1_{G\times H} = (1_G, 1_H)$ and group operations

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2),$$
$$(g,h)^{-1} = (g^{-1}, h^{-1}).$$

One can prove that the following definition is equivalent (see for example [20]).

Definition 4.1.1. *A group K is the direct product of two groups G and H if and only if G and H are normal subgroups of K, $K = GH$ and the intersection of G and H contains only the identity.*

A relaxation of these conditions, requiring only one subgroup to be normal, gives the *semidirect product* $G : H$ or $G :_\Phi H$, where $\Phi : H \to Aut(G)$ describes an action of H on G. We define

$$G : H = \{(g,h) \mid g \in G, h \in H\},$$

with identity element $1_{G:H} = (1_G, 1_H)$ and group operations

$$(g_1,h_1)(g_2,h_2) = (g_1g_2^{\Phi(h_1^{-1})}, h_1h_2),$$
$$(g,h)^{-1} = ((g^{-1})^{\Phi(h)}, h^{-1}).$$

Now suppose that H is a permutation group acting on $\{1,2,3,\dots,n\}$. Define $G^n := G \times G \times \dots \times G = \{(g_1,g_2,\dots,g_n) \mid g_i \in G\}$, the direct product of n copies of G, and let H act on G^n by permuting the n subscripts. That is $\Phi : G \to Aut(G^n)$ is defined by

$$\Phi(h) : (g_1,\dots,g_n) \mapsto (g_{1^{h^{-1}}},\dots,g_{n^{h^{-1}}}). \tag{4.1}$$

Then the *wreath product* $G \wr H$ is defined to be $G^n :_\Phi H$.

With these definitions we are ready to establish the centralizer of an involution.

Proposition 4.1.2. *Let ρ be an involution of cycle type $(2^k, 1^{n-2k})$ in $Sym(n)$, where $1 \leqslant k \leqslant \lfloor \frac{n}{2} \rfloor$.*
Then $C_{Sym(n)}(\rho) \cong E_{2^k} : Sym(k) \times Sym(n-2k)$, where E_{2^k} is an elementary abelian group of order 2^k. Consequently

$$|C_{Sym(n)}(\rho)| = 2^k \cdot k! \cdot (n-2k)!$$

As all involutions of the same cycle type are conjugate, by proposition 1.2.7, we can take, without any loss of generality, $\rho = (1,2)(3,4)\dots(2k-1,2k)$. First we prove the following lemma.

Lemma 4.1.3. *Let $h = h_1h_2h_3$ where h_1, h_2 and h_3 are defined as follows*

- $h_1 \in \langle (1,2),(3,4),\dots,(2k-1,2k)\rangle$,
- $h_2(2l-1) = 2m-1$ *and* $h_2(2l) = 2m$ *for* $1 \leqslant l, m \leqslant k$, $o(h_2) = 2$ *and* $h_2(x) = x$ *for every* $x > 2k$,
- h_3 *fixes the elements of* $\{1,2,\dots,2k\}$ *and permutes the elements of* $\{2k+1,2k+2,\dots,n\}$.

Then $h \in C_{Sym(n)}(\rho)$.

Proof. First take $x \in \{2k+1, 2k+2, \dots, n\}$.

$$\begin{aligned}
\rho^h(x) = h^{-1}\rho h(x) &= h^{-1}\rho h_1h_2h_3(x) \\
&= h^{-1}\rho h_1h_2(x') \quad \text{with } x' \in \{2k+1,2k+2,\dots,n\} \\
&= h^{-1}\rho h_1(x') \\
&= h^{-1}\rho(x') \\
&= h^{-1}(x') \\
&= x \qquad\qquad\qquad \text{because } h(x) = x' \\
&= \rho(x)
\end{aligned}$$

Now take $x \in \{1,2,\dots,2k\}$. Then we have two cases: either $x = 2l-1$ or $x = 2l$ for some $1 \leqslant l \leqslant k$.
First take the case where $x = 2l-1$.

$$\begin{aligned}
\rho^h(2l-1) = h^{-1}\rho h(2l-1) &= h^{-1}\rho h_1h_2h_3(2l-1) \\
&= h^{-1}\rho h_1h_2(2l-1) \\
&= h^{-1}\rho h_1(2m-1) \quad \text{with } 1 \leqslant m \leqslant k \\
&= h^{-1}\rho(2m) \\
&= h^{-1}(2m-1) \\
&= h_3^{-1}h_2^{-1}h_1^{-1}(2m-1) \\
&= h_3^{-1}h_2^{-1}(2m) \\
&= h_3^{-1}(2l) \\
&= 2l \\
&= \rho(2l-1)
\end{aligned}$$

Similarly one can show that $\rho^h(2l) = \rho(2l)$ for $1 \leqslant l \leqslant k$. Thus $\rho^h(x) = \rho(x)$ for every $x \in \{1, 2, \ldots, n\}$. Hence $\rho^h = \rho$ and $h \in C_{Sym(n)}(\rho)$. □

Lemma 4.1.4. *Let H be the set of all permutations h defined as in lemma 4.1.3. Then $H \cong E_{2^k} : Sym(k) \times Sym(n - 2k)$.*

Proof. First we consider only the permutations with $h_3 = id$, which are permutations h' of the form h_1h_2. Let H_1 and H_2 be the sets of all the permutations h_1 and h_2 respectively and $H' = \{h' \in H \mid h' = h_1h_2\}$. We want to show that $H' \cong E_{2^k} : Sym(k)$. The set H_1 is clearly isomorphic to E_{2^k}. The permutations h_2 do not act on the set $\{1, 2, \ldots, 2k\}$ in general but on the set of the k cycles $\{(1, 2), \ldots, (2k - 1, 2k)\}$. In fact every h_2 permutes these cycles by sending one on the other. So H_2 is isomorphic to $Sym(k)$. By definition $H' = H_1H_2$. H_1 acts on the set $\{1, 2, \ldots, 2k\}$ by mapping every odd element onto itself or onto an even element. H_2 acts on the set $\{1, 2, \ldots, 2k\}$ by mapping every odd element onto an odd element. So the intersection of H_1 and H_2 contains only the identity. Moreover, as H_2 acts on H_1 by permuting the cycles, it is easy to see that H_1 is a normal subgroup of H'. However H_2 is not a normal subgroup of H'. Take $(1, 3)(2, 4) \in H_2$ and $(1, 2) \in H'$,

$$(1, 3)(2, 4)^{(1,2)} = (2, 3)(1, 4) \notin H_2.$$

So H' is the semidirect product of H_1 and H_2 and $H' \cong E_{2^k} : Sym(k)$.

It now remains to show that $H \cong H' \times Sym(n-2k)$. Let H_3 be the set of all permutations of the form h_3. Thus H_3 is acting on the set $\{2k+1, \ldots, n\}$ by permuting the elements. So $H_3 \cong Sym(n - 2k)$. By definition every $h \in H$ is the product of an element in H' (which is the product of an element in H_1 and an element in H_2) and an element in H_3. Moreover as H' and H_3 are acting on different sets, their intersection is trivial and they both are normal subgroups of H. So H is the direct product of the groups H' and H_3. As $H' \cong E_{2^k} : Sym(k)$ and $H_3 \cong Sym(n - 2k)$, the lemma is proven. □

As shown in lemma 4.1.3, we have $H \leqslant C_{Sym(n)}(\rho)$. In order to prove that $H = C_{Sym(n)}(\rho)$, it suffices to show that they both have the same order. To do that, we need the following well known lemma.

Lemma 4.1.5. *Let G be a group and $g \in G$. Let $C_G(g)$ be the centralizer of g in G. Then*

$$|G| = |C_G(g)| \cdot |\{h \in G \mid h \text{ is conjugate to } g\}|$$

The next lemma gives the order of the group $C_{Sym(n)}(\rho)$.

Lemma 4.1.6. $|C_{Sym(n)}(\rho)| = 2^k \cdot k! \cdot (n-2k)!$

Proof. We compute the order of the group $C_{Sym(n)}(\rho)$. Set X the number of involutions conjugate to ρ. By lemma 4.1.5, we get

$$\begin{aligned} |Sym(n)| &= |C_{Sym(n)}(\rho)| \cdot X \\ \Rightarrow |C_{Sym(n)}(\rho)| &= \frac{|Sym(n)|}{X}. \end{aligned}$$

Let us compute X. Each involution that is conjugate to ρ must be of same cycle type as ρ. So X represents the number of involutions in $Sym(n)$ of cycle type $(2^k, 1^{n-2k})$.
For the first element in the first 2-cycle, there are n possibilities, for the second element $n-1$, etc. In a cycle it does not matter which element is the first and which is the second. As there are k cycles, we have to divide by 2^k. Moreover it has no impact on the permutation which cycle comes first, which second etc. So we have to divide by k! We finally get

$$X = \frac{n \cdot (n-1) \cdot (n-2) \ldots \cdot (n-2k+1)}{2^k \cdot k!}.$$

This gives us $|C_{Sym(n)}(\rho)|$:

$$\begin{aligned} |C_{Sym(n)}(\rho)| &= \frac{n!}{n \cdot (n-1) \cdot (n-2) \ldots \cdot (n-2k+1)/(2^k \cdot k!)} \\ &= \frac{n! \cdot 2^k \cdot k!}{n \cdot (n-1) \cdot \ldots \cdot (n-2k+1)} \\ &= 2^k \cdot k! \cdot (n-2k)! \end{aligned}$$

□

We are ready to prove proposition 4.1.2.

Proof. By lemma 4.1.3, $H \subseteq C_{Sym(n)}(\rho)$. Using lemma 4.1.4 we can compute the order of H.

$$|H| = |E_{2^k} : Sym(k) \times Sym(n-2k)| = 2^k \cdot k! \cdot (n-2k)!$$

Lemma 4.1.6 allows to conclude. As H is a subgroup of $C_{Sym(n)}(\rho)$ and has the same order, $C_{Sym(n)}(\rho)$ is exactly the group H. This H is isomorphic to $E_{2^k} : Sym(k) \times Sym(n-2k)$ and so proposition 4.1.2 is proven. □

Notice that the result of proposition 4.1.2 agrees with the general result of the centralizer of a permutation $\pi \in Sym(n)$, given in the following theorem[1].

Theorem 4.1.7. *Let π be an element of $Sym(n)$ of cycle type $(c_1^{k_1}, c_2^{k_2}, \ldots, c_r^{k_r})$, then the centralizer of π in $Sym(n)$ is a direct product of r wreath products $C_{c_i} \wr Sym(k_i)$, where C_{c_i} denotes a cyclic group of order c_i.*

$$C_{Sym(n)}(\pi) = [C_{c_1} \wr Sym(k_1)] \times \ldots \times [C_{c_r} \wr Sym(k_r)]$$

In proposition 4.1.2, we determine the centralizer of an involution ρ with k 2-cycles in $Sym(n)$. Such an involution has cycle type $(2^k, 1^{n-2k})$. According to theorem 4.1.7,

$$C_{Sym(n)}(\rho) = [C_2 \wr Sym(k)] \times [C_1 \wr Sym(n-2k)] \,. \tag{4.2}$$

By (4.1) the wreath product $C_2 \wr Sym(k)$ is defined as the semidirect product $C_2^k : Sym(k)$. The group C_2^k is the direct product of k cyclic groups of order 2 which is isomorphic to the group E_{2^k}. So the first term in $C_{Sym(n)}(\rho)$ is nothing else than $E_{2^k} : Sym(k)$. The group C_1 is cyclic of order 1, which corresponds to the trivial group. The wreath product of the trivial group with a group G is isomorphic to G. So the group $C_1 \wr Sym(n-2k)$ is isomorphic to $Sym(n-2k)$.

Hence the form in (4.2) is the same as the form in proposition 4.1.2 and therefore proposition 4.1.2 agrees with theorem 4.1.7.

4.2 Commuting Involutions in $Sym(n)$, $n \neq 6$

Having computed the general form of the centralizer of an involution in $Sym(n)$, we are ready to execute the basic idea of section 3.2. The first step consists of choosing an involution ρ_0, up to isomorphism. As already previously stated, we do this work for $n \neq 6$. We deal with the particular case $n = 6$ in section 4.3. If $n \neq 6$, choosing an involution ρ_0 in $Sym(n)$, up to isomorphism, is the same as choosing it up to conjugacy. By theorem 1.2.7, two involutions are conjugate in $Sym(n)$ if they have same cycle type. Hence the number of different possibilities for choosing ρ_0 in $Sym(n)$ equals

[1]We do not prove the theorem in this thesis, but the result and the proof can be found in [23].

the number of different cycle types for an involution in $Sym(n)$. Clearly an involution in $Sym(n)$ has cycle type $(2^k, 1^{n-2k})$ with k varying from 1 to $\lfloor \frac{n}{2} \rfloor$. Thus there are $\lfloor \frac{n}{2} \rfloor$ possibilities for choosing a first involution ρ_0 in $Sym(n)$. This finishes step 1.

We now initiate step 2, which consists of computing the number of pairs of commuting involutions in $Sym(n)$. In order to to this, we fix the involution ρ_0 and look at the number of possibilities of choosing ρ_2, up to conjugacy, such that ρ_2 commutes with ρ_0.

We first compute the number of *ordered* pairs of commuting involutions in $Sym(n)$, with $n \neq 6$. We prove the following lemma.

Lemma 4.2.1. *Let $n \neq 6$ be a positive integer. Up to isomorphism, there are*

$$-2 \cdot \lfloor \frac{n}{2} \rfloor + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lambda(k) \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1)$$

ordered pairs of commuting involutions ρ_0 and ρ_2 in $Sym(n)$, where

$$\lambda(k) = \begin{cases} \frac{k^2}{4} + k + 1 & \text{if } k \text{ even,} \\ \frac{k^2}{4} + k + \frac{3}{4} & \text{if } k \text{ odd.} \end{cases}$$

Proof. Suppose ρ_0 is an involution containing k cycles of length 2. Up to isomorphism, there is only one such involution, namely $(1,2)(3,4)\dots(2k-1,2k)$. As ρ_2 commutes with ρ_0, $\rho_2 \in C_{Sym(n)}(\rho_0) \cong E_{2^k} : Sym(k) \times Sym(n-2k)$.

First we count the possibilities for an involution ρ_2, that fixes every element in $\{2k+1,\dots,n\}$, i.e. an involution in $E_{2^k} : Sym(k)$. As we count them up to conjugacy, which is the same as up to isomorphism if $n \neq 6$, we have to figure out which of all these involutions are conjugate by an element of $C_{Sym(n)}(\rho_0)$. It is obvious that two conjugate involutions have the same cycle type. Moreover if an isomorphism, that fixes ρ_0, maps ρ_2 onto ρ_2', then ρ_2 and ρ_2' have the same number of 2-cycles of the form $(2r-1,2r)$, with $1 \leq r \leq k$ and the same number of 2-cycles of the form (s,t) with $|s-t| \geq 2$ and $s,t \leq 2k$. Otherwise, we may assume that ρ_2 has at least one more 2-cycle of the form $(2r-1,2r)$ and $\rho_2^g = \rho_2'$ for a permutation $g \in C_{Sym(n)}(\rho_0)$. This means that the conjugation by g maps at least one 2-cycle of the form $(2r-1,2r)$ onto a cycle of the form (s,t). However then $\rho_0^g \neq \rho_0$, which is a contradiction. On the other hand it is obvious to see that if two involutions have the same cycle type and the same number of cycles of the form $(2r-1,2r)$, with $1 \leq r \leq k$ and the same number

of cycles of the form (s,t) with $|s-t| \geq 2$ and $s,t \leq 2k$, then they are conjugate by an element of $C_{Sym(n)}(\rho_0)$.
Suppose that ρ_2 is composed of l 2-cycles, where m 2-cycles are of the form (s,t), with $m \leq l$ and $l-m$ 2-cycles are of the form $(2r-1,r)$. To count the number of such involutions ρ_2 up to isomorphism, we just have to count the number of possibilities for m. It is trivial to see that m has to be even. So m can take every even value between 0 and l. This gives us $\lfloor \frac{l}{2} \rfloor + 1$ possibilites for m, for a given l. However l can take every value between 0 (in this case ρ_2 is the trivial permutation) and k. If $\lambda(k)$ denotes the number, up to isomorphism, of possible involutions ρ_2 consisting only of elements in $\{1, 2, \ldots, 2k\}$, that commute with ρ_0, then we have

$$\begin{aligned}
\lambda(k) &= \sum_{l=0}^{k} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= k + 1 + \sum_{l=0}^{k} \lfloor \frac{l}{2} \rfloor \\
&= \begin{cases} k + 1 + 2 \cdot \displaystyle\sum_{l=0}^{\frac{k}{2}-1} l + \frac{k}{2} & \text{if } k \text{ is even} \\ k + 1 + 2 \cdot \displaystyle\sum_{l=0}^{\frac{k-1}{2}} l & \text{if } k \text{ is odd} \end{cases} \\
&= \begin{cases} k + 1 + 2 \cdot \dfrac{(\frac{k}{2} - 1) \cdot \frac{k}{2}}{2} + \dfrac{k}{2} & \text{if } k \text{ is even} \\ k + 1 + 2 \cdot \dfrac{\frac{k-1}{2} \cdot (\frac{k-1}{2} + 1)}{2} & \text{if } k \text{ is odd} \end{cases} \\
&= \begin{cases} \dfrac{k^2}{4} + k + 1 \text{ if } k \text{ even,} \\ \dfrac{k^2}{4} + k + \dfrac{3}{4} \text{ if } k \text{ odd.} \end{cases}
\end{aligned}$$

Now we consider the case where the cycle decomposition of ρ_2 involves also 2-cycles from the group $Sym(n-2k)$, i.e. 2-cycles containing the elements of $\{2k+1, \ldots, n\}$. In fact these 2-cycles are independent of the other ones. So we can simply multiply $\lambda(k)$ by the number of possibilities of forming involutions in $Sym(n-2k)$. As ρ_0 fixes all the elements in $\{2k+1, \ldots, n\}$, all the involutions of same cycle type of $Sym(n-2k)$ are conjugate by a permutation fixing ρ_0. To count the number of involutions in $Sym(n-2k)$, up to isomorphism, we just have to count the number of different cycle types. An involution of $Sym(n-2k)$ can have between 0 and $\lfloor \frac{n-2k}{2} \rfloor$ cycles of length 2. So there are $\lfloor \frac{n-2k}{2} \rfloor + 1$ different cycle types.

To compute the number of all the involutions ρ_2 that commute with a given ρ_0 of cycle type $(2^k, 1^{n-2k})$, we have to multiply $\lambda(k)$ by $\lfloor \frac{n-2k}{2} \rfloor + 1$. However the trivial permutation and ρ_0 itself are also among these constructions. So we have to subtract 2 from this number.

The number of 2-cycles involved in ρ_0 may vary between 1 and $\lfloor \frac{n}{2} \rfloor$. We have to sum up $\left(\lambda(k) \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) - 2\right)$ for every k between 1 and $\lfloor \frac{n}{2} \rfloor$. We get:

$$\begin{aligned}
&\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (\lambda(k) \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) - 2) \\
&= -2 \cdot \lfloor \frac{n}{2} \rfloor + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lambda(k) \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1).
\end{aligned}$$

□

We are interested in computing the number of *unordered* pairs of commuting involutions in $Sym(n)$. Hence we prove the following theorem.

Theorem 4.2.2. *Set $\lambda(k)$ as in lemma 4.2.1 and*

$$\psi(k,n) = \begin{cases} \left[\frac{1}{2}\left(k - \lfloor \frac{n-2k}{2} \rfloor\right)\right]^2 + \frac{1}{2}\left(k - \lfloor \frac{n-2k}{2} \rfloor\right) & \text{if } n \equiv 0, 1 \text{ mod } 4, \\ \\ \left[\frac{1}{2}\left(k - \lfloor \frac{n-2k}{2} \rfloor - 1\right)\right]^2 + k - \lfloor \frac{n-2k}{2} \rfloor & \text{if } n \equiv 2, 3 \text{ mod } 4, \end{cases}$$

$$\eta(n) = \begin{cases} \lfloor \frac{n}{4} \rfloor + 1 \text{ if } n \text{ is even}, \\ \lfloor \frac{n-1}{4} \rfloor + 1 \text{ if } n \text{ is odd}. \end{cases}$$

There are, up to isomorphism,

$$-\frac{3}{2} \cdot \lfloor \frac{n}{2} \rfloor + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lambda(k) \cdot (\frac{1}{2} \lfloor \frac{n-2k}{2} \rfloor + 1) - \frac{1}{2} \cdot \sum_{k=\eta(n)}^{\lfloor \frac{n}{2} \rfloor} \psi(k,n)$$

pairs of commuting involutions ρ_0 and ρ_2 in $Sym(n)$, with $n \neq 6$.

First we prove a useful lemma.

Lemma 4.2.3. *Let the ordered pair $[\rho_0, \rho_2]$ be a representative of one isomorphism class of commuting involutions. Moreover let ρ_0 be an involution of cycle type $(2^k, 1^{n-2k})$ and ρ_2 an involution of cycle type $(2^l, 1^{n-2l})$.*

If $k \neq l$ there exists an involution ρ'_0 of cycle type $(2^l, 1^{n-2l})$ and an involution ρ'_2 of cycle type $(2^k, 1^{n-2k})$, such that the unordered pairs $\{\rho_0, \rho_2\}$ and $\{\rho'_0, \rho'_2\}$ are isomorphic.
If $k = l$, no two classes of ordered pairs of commuting involutions are isomorphic, if seen as unordered pairs.

Proof. The first one to one correspondence is easy to see. In fact, take $[\rho_0, \rho_2]$ as described in the lemma. Then we take ρ'_0 of cycle type $(2^l, 1^{n-2l})$. As ρ_2 and ρ'_0 have same cycle type, they are conjugate by a permutation α. The involution ρ_0^α is of cycle type $(2^k, 1^{n-2k})$ and commutes with $\rho_2^\alpha = \rho'_0$, because ρ_0 commutes with ρ_2. Set $\rho'_2 = \rho_0^\alpha$. Hence $[\rho'_0, \rho'_2]$ is an ordered pair of commuting involutions and $\{\rho_0, \rho_2\}$ and $\{\rho'_0, \rho'_2\}$ are conjugate as unordered pairs. As the situation is symmetric in k and l, the one to one correspondence is established.
Suppose now that $k = l$ and suppose, by contradiction, that there exists two ordered pairs $[\rho_0, \rho_2]$ and $[\rho'_0, \rho'_2]$ from different isomorphism classes and a permutation α such that $\rho_0^\alpha = \rho'_2$ and $\rho_2^\alpha = \rho'_0$. Without loss of generality we may choose two representative pairs with $\rho_0 = \rho'_0$. Then

$$\rho'_2 = \rho_0^\alpha = \rho_0'^\alpha = \rho_2^{\alpha^2}.$$

This means that ρ_2 and ρ'_2 are conjugate with contradicts the fact that the two ordered pairs $[\rho_0, \rho_2]$ and $[\rho'_0, \rho'_2]$ are in different isomorphism classes. □

Imagine we have found all the conjugacy classes of ordered pairs of commuting involutions in $Sym(n)$. We now pick one pair of each class and set up a list. This lemma shows that for every ordered pair of commuting involutions in the list, of the form $[\rho_0, \rho_2]$ where ρ_0 and ρ_2 have different cycle types, there exists another ordered pair $[\rho'_0, \rho'_2]$ in the list such that the two pairs are isomorphic as unordered pairs. In terms of polytopes this means that they generate two dual polytopes. However an ordered pair in the list, of the form $[\rho_0, \rho_2]$, with ρ_0 and ρ_2 having the same cycle type, has no dual pair on that list. Hence, in order to compute the number of unordered pairs of commuting involutions in $Sym(n)$, we cannot just divide the formula in lemma 4.2.1 by 2. We first have to subtract the number of pairs $[\rho_0, \rho_2]$, where ρ_0 and ρ_2 have the same cycle type. This difference will be divided by 2 and finally we add again the number of pairs $[\rho_0, \rho_2]$, where ρ_0 and ρ_2 have the same cycle type.

Let us formulate this in a mathematical language and thus prove theorem 4.2.2.

Proof. First we have to compute the number of ordered pairs $[\rho_0, \rho_2]$ where ρ_0 and ρ_2 contain exactly k cycles, for a given $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$. Without any loss of generality, we may again fix $\rho_0 = (1,2)(3,4)\dots(2k-1,2k)$. We have to count the number of possibilities of choosing an involution ρ_2 of cycle type $(2^k, 1^{n-2k})$, being different from ρ_0 and commuting with ρ_0. As in the proof of lemma 4.2.1, we construct involutions of cycle type $(2^l, 1^{n-2l})$ and acting only on the set $\{1, 2, \dots, 2k\}$, i.e. fixing all the elements of the set $\{2k+1, \dots, n\}$. As we want ρ_2 to be of cycle type $(2^k, 1^{n-2k})$, we have to add $k-l$ 2-cycles acting on the set $\{2k+1, \dots, n\}$ and fixing the elements of $\{1, \dots, 2k\}$. The integer l may take every value between 0 and k if $\lfloor \frac{n-2k}{2} \rfloor$ is large enough, more precisely if $\lfloor \frac{n-2k}{2} \rfloor \geq k$, hence if

$$\begin{cases} n - 2k \geq 2k & \text{if } n \text{ even,} \\ n - 2k - 1 \geq 2k & \text{if } n \text{ odd,} \end{cases}$$
$$\Leftrightarrow \begin{cases} k \leq \dfrac{n}{4} & \text{if } n \text{ even,} \\ k \leq \dfrac{n-1}{4} & \text{if } n \text{ odd.} \end{cases}$$

Set

$$\nu(n) = \begin{cases} \dfrac{n}{4} & \text{if } n \text{ even,} \\ \dfrac{n-1}{4} & \text{if } n \text{ odd.} \end{cases}$$

Hence if $k \leq \nu(n)$, the integer l may take every value between 0 and k and 2-cycles involving only elements from the set $\{2k+1, \dots, n\}$ are added to get cycle type $(2^k, 1^{n-2k})$. To compute the number of possibilities for ρ_2 in this case, we have to compute the number of involutions consisting of l cycles, with $0 \leq l \leq k$, and fixing every element of the set $\{2k+1, \dots, n\}$. So we are in exactly the same situation as in the proof of lemma 4.2.1. Thus we get exactly $\lambda(k)$ possibilities, with $\lambda(k)$ defined as in lemma 4.2.1. However one of these possibilities is the case where $\rho_2 = \rho_0$. As we do not want this case, we have to subtract 1. Finally if $k \leq \nu(n)$, there are $\lambda(k) - 1$ ordered pairs of commuting involutions $[\rho_0, \rho_2]$ such that both ρ_0 and ρ_2 contain exactly k cycles.

If $k > \nu(n)$, the integer l cannot take every value between 0 and k. In fact there are not enough elements in $\{2k+1, \dots, n\}$ to complete the l cycles, if l is too small. Thus l may only take every value between $k - \lfloor \frac{n-2k}{2} \rfloor$ and k.

Set $\lambda'(k)$ the number of possibilities for ρ_2. We distinguish between two cases.

If $k - \lfloor \frac{n-2k}{2} \rfloor - 1$ is odd,

$$\begin{aligned}
\lambda'(k) = & \sum_{l=k-\lfloor \frac{n-2k}{2} \rfloor}^{k} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= \lambda(k) - \sum_{l=0}^{k-\lfloor \frac{n-2k}{2} \rfloor -1} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - \sum_{l=0}^{k-\lfloor \frac{n-2k}{2} \rfloor -1} \lfloor \frac{l}{2} \rfloor \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - 2 \cdot \sum_{l=0}^{\frac{1}{2}(k-\lfloor \frac{n-2k}{2} \rfloor -2)} l \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - \frac{1}{4}(k - \lfloor \frac{n-2k}{2} \rfloor - 2)(k - \lfloor \frac{n-2k}{2} \rfloor) \\
&= \lambda(k) - \frac{1}{2}(k - \lfloor \frac{n-2k}{2} \rfloor) - [\frac{1}{2}(k - \lfloor \frac{n-2k}{2} \rfloor)]^2.
\end{aligned}$$

If $k - \lfloor \frac{n-2k}{2} \rfloor - 1$ is even,

$$\begin{aligned}
\lambda'(k) = & \sum_{l=k-\lfloor \frac{n-2k}{2} \rfloor}^{k} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= \lambda(k) - \sum_{l=0}^{k-\lfloor \frac{n-2k}{2} \rfloor -1} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - \sum_{l=0}^{k-\lfloor \frac{n-2k}{2} \rfloor -1} \lfloor \frac{l}{2} \rfloor \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - \frac{1}{2}k + \frac{1}{2}\lfloor \frac{n-2k}{2} \rfloor + \frac{1}{2} - 2 \sum_{l=0}^{\frac{1}{2}(k-\lfloor \frac{n-2k}{2} \rfloor -3)} l \\
&= \lambda(k) - \frac{3}{2}k + \frac{3}{2}\lfloor \frac{n-2k}{2} \rfloor + \frac{1}{2} - \frac{(k - \lfloor \frac{n-2k}{2} \rfloor - 3)(k - \lfloor \frac{n-2k}{2} \rfloor - 1)}{4} \\
&= \lambda(k) - k + \lfloor \frac{n-2k}{2} \rfloor - [\frac{1}{2}(k - \lfloor \frac{n-2k}{2} \rfloor - 1)]^2.
\end{aligned}$$

Observe that the condition on $k - \lfloor \frac{n-2k}{2} \rfloor - 1$ may be formulated in an easier way. In fact,

- if $n \equiv 0 \ mod\ 4$ or $n \equiv 1 \ mod\ 4$,

$$\lfloor\frac{n-2k}{2}\rfloor \text{ is } \begin{cases} \text{even if } k \text{ is even} \\ \text{odd if } k \text{ is odd} \end{cases} \Rightarrow k - \lfloor\frac{n-2k}{2}\rfloor - 1 \text{ is odd.}$$

- if $n \equiv 2 \ mod\ 4$ or $n \equiv 3 \ mod\ 4$,

$$\lfloor\frac{n-2k}{2}\rfloor \text{ is } \begin{cases} \text{odd if } k \text{ is even} \\ \text{even if } k \text{ is odd} \end{cases} \Rightarrow k - \lfloor\frac{n-2k}{2}\rfloor - 1 \text{ is even.}$$

Hence the condition $k - \lfloor\frac{n-2k}{2}\rfloor - 1$ odd is equivalent to $n \equiv 0, 1 \ mod\ 4$ and the condition $k - \lfloor\frac{n-2k}{2}\rfloor - 1$ even is equivalent to $n \equiv 2, 3 \ mod\ 4$.

Thus

$$\lambda'(k) = \begin{cases} \lambda(k) - \frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor) - [\frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor)]^2 & \text{if } n \equiv 0, 1 \ mod\ 4, \\ \lambda(k) - k + \lfloor\frac{n-2k}{2}\rfloor - [\frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor - 1)]^2 & \text{if } n \equiv 2, 3 \ mod\ 4. \end{cases}$$

Once again we have to subtract 1 from $\lambda(k)'$ as one of these possibilities is the case $\rho_0 = \rho_2$.

Set $\lambda''(k)$ the number of pairs of commuting involutions $[\rho_0, \rho_2]$ with ρ_0 and ρ_2 containing both exactly k cycles. By the former reasoning we get

$$\lambda''(k) = \begin{cases} \lambda(k) - 1 & \text{if } k \leq \nu(n), \\ \lambda(k) - \psi(k, n) - 1 & \text{if } k > \nu(n), \end{cases} \tag{4.3}$$

where

$$\psi(k, n) = \begin{cases} [\frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor)]^2 + \frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor) & \text{if } n \equiv 0, 1 \ mod\ 4, \\ [\frac{1}{2}(k - \lfloor\frac{n-2k}{2}\rfloor - 1)]^2 + k - \lfloor\frac{n-2k}{2}\rfloor & \text{if } n \equiv 2, 3 \ mod\ 4. \end{cases}$$

Thus the number of pairs of commuting involutions $[\rho_0, \rho_2]$ with ρ_0 and ρ_2 containing the same number of cycles, is the sum of all $\lambda''(k)$ for $1 \leq k \leq \lfloor\frac{n}{2}\rfloor$.

To compute the general number of unordered pairs of commuting involutions in $Sym(n)$, we subtract this sum from the formula in lemma 4.2.1, divide by 2 and then add again the sum. Define $\eta(n)$ as in theorem 4.2.2.

Then the number of unordered pairs of commuting involutions in $Sym(n)$ is

$$\begin{aligned}
&\frac{1}{2}\cdot\left[-2\cdot\lfloor\frac{n}{2}\rfloor+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)\cdot(\lfloor\frac{n-2k}{2}\rfloor+1)-\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda''(k)\right]+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda''(k)\\
=&\frac{1}{2}\cdot\left[\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)\lfloor\frac{n-2k}{2}\rfloor+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)-\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)+\sum_{k=\eta(n)}^{\lfloor\frac{n}{2}\rfloor}\psi(k,n)+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}1\right]\\
&-\lfloor\frac{n}{2}\rfloor+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)-\sum_{k=\eta(n)}^{\lfloor\frac{n}{2}\rfloor}\psi(k,n)-\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}1\\
=&-\frac{3}{2}\cdot\lfloor\frac{n}{2}\rfloor+\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor}\lambda(k)\cdot\left(\frac{1}{2}\lfloor\frac{n-2k}{2}\rfloor+1\right)-\frac{1}{2}\cdot\sum_{k=\eta(n)}^{\lfloor\frac{n}{2}\rfloor}\psi(k,n).
\end{aligned}$$

This finishes the proof of theorem 4.2.2. □

Remark 4.2.4. *Table A.2 and table A.3 of section A.3 of the appendices show some results for the formulas of lemma 4.2.1 and theorem 4.2.2.*

Note that the formula of lemma 4.2.1 and the formula of theorem 4.2.2 give always the same result for n and $n+1$, with n even. This is evident for two reasons. On the one hand, if we look closely at the two formulas it is trivial that they give the same result for n and $n+1$. The formula of lemma 4.2.1 does not contain directly the integer n, but only the floor of $\frac{n}{2}$ and the floor of $\frac{n-2k}{2}$. Both values are the same for n and $n+1$, with n even. The formula of theorem 4.2.2 does not involve n directly neither, but also only the floor of $\frac{n}{2}$ and the floor of $\frac{n-2k}{2}$. Moreover the integer n is contained in the functions $\eta(n)$ and $\psi(k,n)$. In $\eta(n)$, the integer n is involved as n if it is even and as $n-1$ if it is odd. Hence $\eta(n)$ clearly gives the same result for n and $n+1$. The function $\psi(k,n)$ is computed differently depending on the value of $n \bmod 4$. There is one expression for $n \equiv 0,1 \bmod 4$ and another expression for $n \equiv 2,3 \bmod 4$. It is easy to see that either n and $n+1$ are equivalent to 0 and 1 modulo 4 or to 2 and 3 and thus $\psi(k,n)$ gives the same results for n and $n+1$, with n even. On the other side, we may consider the question directly, without looking at the formulas. We count, up to isomorphism, the number of ordered or unordered pairs of commuting involutions. We first fix an involution ρ_0 and then count how many involutions ρ_2 are commuting with the first involution, up to isomorphism. The first involution ρ_0 is also chosen up to isomorphism.

Hence we look how many different cycle decompositions an involution may have in $Sym(n)$. As the cycle decomposition of an involution consists only of 2-cycles and 1-cycles, the number of different possibilities is the same for $Sym(n)$ and $Sym(n+1)$, with n even. The same is true while counting all the possibilities for ρ_2. Therefore it is evident that table A.2 and table A.3 show the same result for n and $n+1$, with n even. We could have changed the formula in such a way that it only works for n even and if n is odd, one puts $n-1$ in the formula, but we thought that a formula is always nicer if it works for all n.

4.3 The Particular Case of $Sym(6)$

The lemma and the theorem of the previous section only work for $n \neq 6$. In this section we treat the case $n = 6$. As an analogy to lemma 4.2.1 and theorem 4.2.2, we prove the following lemma for $n = 6$.

Lemma 4.3.1. *Up to isomorphism, there are* 5 *pairs of commuting involutions in* $Sym(6)$.

First we can apply the formula of theorem 4.2.2 to compute the number of pairs of involutions in $Sym(6)$, up to conjugacy, but it does not give the final result. It merely determines an intermediate step. As the automorphism group of $Sym(6)$ is twice bigger than $Sym(6)$ (see proposition 1.2.12), there are automorphisms that do not act on $Sym(6)$ by conjugacy. These automorphisms may fuse the orbits obtained up to conjugacy. The formula computed in theorem 4.2.2 gives 9 unordered pairs of involutions in $Sym(6)$ (see table A.3 of the appendices)

It remains to prove that the outer automorphisms of $Sym(6)$ fuse these 9 conjugacy classes into 5 orbits. We determine a representative of each of the conjugacy classes. However first we consider the conjugacy classes of ordered pairs of commuting involutions. The formula of lemma 4.2.1 gives us 14 (see table A.2 of the appendices) ordered pairs of commuting involutions in $Sym(6)$. The list below shows a representative of each class.

$$\rho_0 = (1,2) \text{ and } \rho_2 = (3,4) \tag{4.4a}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (3,4)(5,6) \tag{4.4b}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (1,2)(3,4) \tag{4.4c}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (1,2)(3,4)(5,6) \tag{4.4d}$$

$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (5,6) \tag{4.5a}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,2) \tag{4.5b}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,2)(5,6) \tag{4.5c}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,3)(2,4) \tag{4.5d}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,3)(2,4)(5,6) \tag{4.5e}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,2)(3,4)(5,6) \tag{4.5f}$$

$$\rho_0 = (1,2)(3,4)(5,6) \text{ and } \rho_2 = (1,3)(2,4)(5,6) \tag{4.6a}$$
$$\rho_0 = (1,2)(3,4)(5,6) \text{ and } \rho_2 = (1,2)(3,4) \tag{4.6b}$$
$$\rho_0 = (1,2)(3,4)(5,6) \text{ and } \rho_2 = (1,3)(2,4) \tag{4.6c}$$
$$\rho_0 = (1,2)(3,4)(5,6) \text{ and } \rho_2 = (1,2) \tag{4.6d}$$

Above we computed that there are only 9 classes of unordered pairs. So some of these representatives are isomorphic as unordered pairs. It is easy to see that the following pairs are dual: (4.4b) and (4.5a), (4.4c) and (4.5b), (4.4d) and (4.6d), (4.5e) and (4.6c) and (4.5f) and (4.6b). Indeed we are left with 9 conjugacy classes. To analyse how the outer automorphisms act on these 9 conjugacy classes, we use a geometric way, more specifically generalized quadrangles.

4.3.1 The Geometric Way

First we give some preliminary definitions and basic properties. We mainly refer in this section to [26].

Generalized Quadrangles

Definition 4.3.2. *A geometry of rank* 2 *is a triple* $\Gamma = (\mathcal{P}, \mathcal{L}, I)$, *where* $\mathcal{P}$ *and* $\mathcal{L}$ *are disjoint non-empty sets and* $I \subseteq \mathcal{P} \times \mathcal{L}$ *is a relation, the incidence relation.*

Definition 4.3.3. *A subgeometry*[2] *of* $\Gamma = (\mathcal{P}, \mathcal{L}, I)$ *is a geometry* $\Gamma' = (\mathcal{P}', \mathcal{L}', I')$ *with* $\mathcal{P}' \subset \mathcal{P}, \mathcal{L}' \subset \mathcal{L}$ *and* $I' = I \cap (\mathcal{P}' \times \mathcal{L}')$.

[2] When considering geometries Γ satisfying special axioms, we are usually interested only in those subgeometries which satisfy the same axioms.

In this thesis we often omit the specification "of rank 2". The elements of $\mathcal{P}$ are called the *points* and the elements of $\mathcal{L}$ *lines* or *blocks*. The sets $\{p, L\}$, with $p \in \mathcal{P}$, $L \in \mathcal{L}$, $p\ I\ L$, are the *flags*[3]. An *antiflag* is a set $\{p, L\}$, where p and L are not incident. For a point $p \in \mathcal{P}$, the set $\Gamma(p) = \{L \in \mathcal{L} \mid p\ I\ L\}$ of all lines through p is the *pencil* of p, and for $L \in \mathcal{L}$ the *point row* of the line L is defined by $\Gamma(L) = \{p \in \mathcal{P} \mid p \in L\}$. If all point rows have the same cardinality $s+1$ and if all pencils have the same cardinality $t+1$, then $\Gamma = (\mathcal{P}, \mathcal{L}, I)$ is said to be of *order* (s, t). If $s = t$, then Γ is said to have order s. A geometry is called *thick* if all point rows and all pencils have cardinalities at least 3, and it is called *slim* if $s = 2$. With these definitions we are able to define a *generalized n-gon*.

Definition 4.3.4. *A weak generalized n-gon is a geometry $\Gamma = (\mathcal{P}, \mathcal{L}, I)$ such that the following two axioms are satisfied.*

(i) Γ *contains no ordinary k-gon (as a subgeometry), for $2 \leqslant k < n$.*

(ii) Any two elements $x, y \in \mathcal{P} \cup \mathcal{L}$ are contained in some ordinary n-gon (again as a subgeometry) in Γ, a so-called apartment.

A generalized n-gon is a weak generalized n-gon Γ which satisfies also the following axiom.

(iii) There exists an ordinary $(n+1)$-gon (as a subgeometry) in Γ.

Remark 4.3.5. *An ordinary polygon is the geometry arising in the obvious way from a (regular) polygon in the real Euclidean plane.*

So a generalized quadrangle is a generalized 4-gon. The definition of a generalized quadrangle can be rephrased as follows (for the proof see [26]).

Lemma 4.3.6. *A geometry $\Gamma = (\mathcal{P}, \mathcal{L}, I)$ is a weak generalized quadrangle if and only if the following axioms (i) and (ii), or (i) and (ii)' hold.*

(i) Let $\{p, L\}$ be an antiflag. Then there exists a unique flag $\{q, M\}$ of the geometry such that $pIMIqIL$.

[3] In general, a *flag* of the geometry of rank n can be any set of pairwise incident elements. A *maximal flag* of a geometry is a *flag* that is maximal for the incidence relation. So in rank 2 geometries the sets $\{p, L\}$ are in fact *maximal flags*, but as there are practically no other possibilities to construct a *flag* (except for the singletons and the empty set), we will always talk about *flags* in this thesis.

(ii) Every point lies on at least two but not all lines, and dually every line carries at least two but not all points.

(ii)' Every point is on at least two lines, and any two points are contained in at most one line. Also, every line carries at least two points.

A geometry Γ is a generalized quadrangle if and only if Γ is thick, axiom (i) holds, and Γ contains some antiflag.

We need some definitions about isomorphisms. Let $\Gamma = (\mathcal{P}, \mathcal{L}, I)$ and $\Gamma' = (\mathcal{P}', \mathcal{L}', I')$ be two geometries.

Definition 4.3.7. *An isomorphism from Γ to Γ' is an application $\alpha : \mathcal{P} \cup \mathcal{L} \to \mathcal{P}' \cup \mathcal{L}'$ satisfying the following conditions.*

(i) α is bijective.

(ii) α maps every point to a point and every line to a line or every point to a line and every line to a point.

(iii) $\forall p \in \mathcal{P}, L \in \mathcal{L} \quad p\ I\ L \Leftrightarrow \alpha(p)\ I\ \alpha(L)$.

Definition 4.3.8. *A correlation of Γ is an isomorphism from Γ to Γ.*

Definition 4.3.9. *An automorphism of Γ is a correlation of Γ which maps every point to a point and every line to a line.*

Generalized Quadrangles and the Symmetric Group of Degree 6

To prove Lemma 4.3.1, we use a special construction of a generalized quadrangle[4]. We denote by $\mathcal{P}$ the set of all 15 transpositions in the symmetric group $Sym(6)$ and by $\mathcal{L}$ the set of all 15 fixed-point-free involutions in $Sym(6)$. We then define the incidence relation by $\sigma\ I\ \tau \Leftrightarrow \sigma\tau = \tau\sigma$ for $\sigma \in \mathcal{P}, \tau \in \mathcal{L}$.

Lemma 4.3.10. *The geometry $(\mathcal{P}, \mathcal{L}, I)$ defined as above is a generalized quadrangle of order $(2, 2)$.*

---

[4]Historically this geometry comes from the *fifteen schoolgirls problem* proposed by Kirkman in 1850 in *The Lady's and Gentleman's Diary*. It is in fact a Steiner system $S(2, 3, 15)$. Details about this may be found in [1] and [8]

Proof. Take σ a transposition. Then σ commutes with τ if and only if one of the three 2-cycles of τ equals the 2-cycle of the transposition σ. So σ is contained in exactly three lines and hence the pencil of every transposition is of cardinality 3. In the same way, a fixed-point-free involution τ commutes with σ if and only if the 2-cycle involved in σ is equal to one of the three cycles in τ, which means that a fixed-point-free involution commutes with exactly 3 transpositions. So the cardinality of the point row of any $\tau \in \mathcal{L}$ is equal to 3. This means that the geometry is thick and has order $(2, 2)$.

Let us show that axiom (i) holds. Take an antiflag $\{p, L\}$ where $p = (a, b)$ and $L = (a, c)(b, d)(e, f)$, with $a, b, c, d, e, f \in \{1, 2, 3, 4, 5, 6\}$. Set $q = (e, f)$ and $M = (a, b)(c, d)(e, f)$. Clearly $\{q, M\}$ is a flag and $pIMIqIL$. It is trivial, by construction, that this flag $\{q, M\}$ is unique.

Finally it is easy to see that the geometry contains at least one antiflag.

□

Figure 4.1 gives a representation of this geometry.

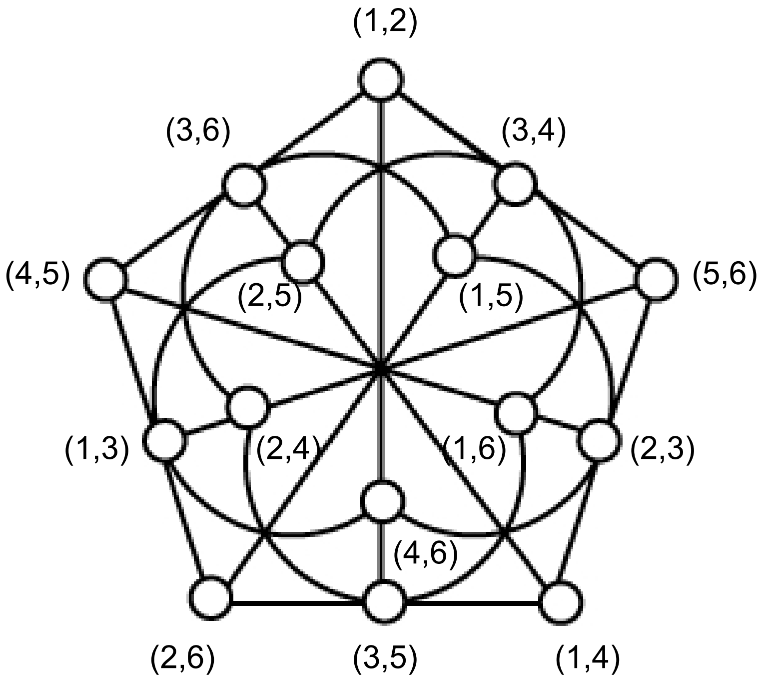

Figure 4.1: Generalized symplectic quadrangle

The lines in figure 4.1 are the involutions consisting of three 2-cycles and the points are the transpositions.

The automorphism group of the geometry $(\mathcal{P}, \mathcal{L}, I)$ is $Sym(6)$, but the correlation group is twice bigger than $Sym(6)$[5]. This means that the automorphisms of $Sym(6)$ lying outside $Sym(6)$ map fixed-point-free involutions on transpositions, as seen in proposition 1.2.13. This clearly shows that these automorphisms cannot be obtained by conjugacy

The involutions in $Sym(6)$ are either transpositions, bi-transpositions or fixed-point-free involutions. The transpositions are the points of this geometry and the fixed-point-free involutions are the lines. It remains to represent the bi-transpositions in this geometry. It is trivial to see that there is a one-to-one correspondence between the bi-transpositions of $Sym(6)$ and the flags of the generalized quadrangle $(\mathcal{P}, \mathcal{L}, I)$. So every bi-transposition can be represented by a flag.

Example 4.3.11. *The bi-transposition* $(1, 2)(3, 4)$ *corresponds to the flag* $\{(5, 6), (1, 2)(3, 4)(5, 6)\}$ *and the bi-transposition* $(1, 2)(5, 6)$ *corresponds to the flag* $\{(3, 4), (1, 2)(3, 4)(5, 6)\}$.

We now choose an outer automorphism φ of $Sym(6)$. It is quite easy to show that the mapping φ

$$\begin{aligned} (1,2)(3,4)(5,6) &\leftrightarrow (5,6) \\ (1,3)(2,4)(5,6) &\leftrightarrow (3,4) \\ (1,4)(2,3)(5,6) &\leftrightarrow (1,2) \end{aligned} \tag{4.7}$$

can be extended in a correlation of the quadrangle, respectively an outer automorphism of $Sym(6)$[6]. The mapping φ acts on the 9 representatives of the conjugacy classes and maps each representative of (4.4) on a representative of (4.6). More precisely φ maps (4.4a) on (4.6a), (4.4b) on (4.6b) etc. Representatives of the classes in (4.5) are mapped on another representative of these classes. More precisely (4.5a) is mapped on (4.5f), (4.5b) is mapped on (4.5e) etc. Thus in the end we are left with 7 orbits of ordered pairs of commuting involutions. If we also consider duality and let φ acting on the 9 unordered pairs, we are left with the following 5 representatives of

[5] This is a well-known fact about this specific quadrangle, see [26].

[6] We established the requested correlation by hand, but we do not see the interest of including it in this thesis.

the 5 orbits of pairs of commuting involutions:

$$\rho_0 = (1,2) \text{ and } \rho_2 = (3,4) \tag{4.8a}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (3,4)(5,6) \tag{4.8b}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (1,2)(3,4) \tag{4.8c}$$
$$\rho_0 = (1,2) \text{ and } \rho_2 = (1,2)(3,4)(5,6) \tag{4.8d}$$
$$\rho_0 = (1,2)(3,4) \text{ and } \rho_2 = (1,3)(2,4) \tag{4.8e}$$

These 5 orbits cannot be fused together by any automorphism of $Sym(6)$, In fact we have already seen that a conjugation does not fuse them together. On the other hand there are other outer automorphisms than the mapping φ described in (4.7). However every outer automorphism of $Sym(6)$ can be constructed in such a geometric way and thus maps transpositions on fixed-point-free involutions and bi-transpositions on bi-transpositions. Therefore no outer automorphism fuses the 5 orbits in (4.8) together.

Hence lemma 4.3.1 is proven.

4.3.2 Polyhedra with Automorphism Group $Sym(6)$

The previous section showed that there are, up to isomorphism, 5 pairs of commuting involutions in $Sym(6)$. We want to see which of these 5 pairs can be extended by a third involution ρ_1, that is not commuting neither with ρ_0 nor with ρ_2, such that ρ_0, ρ_1 and ρ_2 satisfy (IP) and generate all of $Sym(6)$. We analyse each pair $\{\rho_0, \rho_2\}$ separately to find out if it can be extended by a third involution ρ_1 not commuting with ρ_0 and ρ_2 and such that (IP) is satisfied and the three involutions generate $Sym(6)$. We first consider the cases that will not generate all of $Sym(6)$, namely the cases (4.8a), (4.8c) and (4.8e).

(4.8a): $\rho_0 = (1,2)$ and $\rho_2 = (3,4)$

There is only one choice for ρ_1, up to isomorphism. In fact ρ_1 must not commute with ρ_0 and ρ_2 and ρ_0, ρ_1 and ρ_2 should generate $Sym(6)$. The transitivity of $Sym(6)$ forces ρ_1 to be $(1,3)(2,5)(4,6)$, up to isomorphism. All the other possibilities for ρ_1, such as for example $(1,4)(2,5)(3,6)$, are conjugate to $(1,3)(2,5)(4,6)$ by an element fixing the pair $\{(1,2),(3,4)\}$. What is left to verify is the fact that ρ_0, ρ_1 and ρ_2 satisfy (IP) and that the

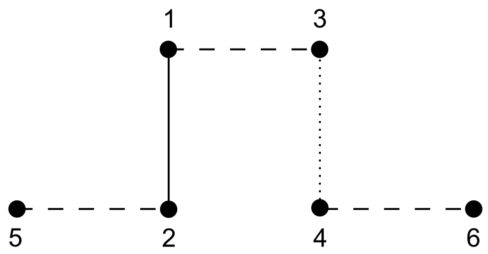

Figure 4.2: CPR graph of $\langle(1,2),(1,3)(2,5)(4,6),(3,4)\rangle$

group $\langle\rho_0,\rho_1,\rho_2\rangle$ is isomorphic to $Sym(6)$. As (IP) is always long to verify, we prove that ρ_0, ρ_1 and ρ_2 do not generate $Sym(6)$. We want to use the CPR graphs, more precisely lemma 2.1.6 to get a contradiction.

The CPR graph of the group $\langle(1,2),(1,3)(2,5)(4,6),(3,4)\rangle$ is drawn in figure 4.2.

However in this case the CPR graph argument does not work. In fact the CPR graph in figure 4.2 has no non-trivial automorphism. Hence we use another argument to prove that $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$.

We compute the following elements

$$\begin{aligned}\rho_0\rho_1 &= (1,5,2,3)(4,6),\\ \rho_1\rho_2 &= (1,4,6,3)(2,5),\\ \rho_0\rho_2 &= (1,2)(3,4).\end{aligned}$$

These elements are all in $\langle\rho_0,\rho_1,\rho_2\rangle$ and using them we define new elements α and β, as follows,

$$\begin{aligned}\alpha &= \rho_0\rho_2\left(\rho_0\rho_1\right)^2 = (1,2)(3,4)\circ(1,2)(3,5) = (3,4,5),\\ \beta &= \rho_0\rho_2\left(\rho_1\rho_2\right)^2 = (1,2)(3,4)\circ(1,6)(3,4) = (1,2,6).\end{aligned}$$

By definition, α and β are in $\langle\rho_0,\rho_1,\rho_2\rangle$ and

$$\langle\alpha,\beta\rangle = \langle\alpha\rangle\times\langle\beta\rangle = E_{3^2} = E_9.$$

Moreover,

$$\begin{array}{ll}\alpha^{\rho_0} = \alpha & \beta^{\rho_0} = \beta^{-1}\\ \alpha^{\rho_1} = \beta^{-1} & \beta^{\rho_1} = \alpha^{-1}\\ \alpha^{\rho_2} = \alpha^{-1} & \beta^{\rho_2} = \beta.\end{array}$$

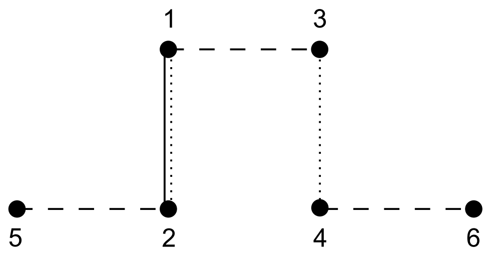

Figure 4.3: CPR graph of $\langle(1,2),(1,3)(2,5)(4,6),(1,2)(3,4)\rangle$

Therefore E_9 is a normal subgroup of $\langle\rho_0,\rho_1,\rho_2\rangle$ and so $\langle\rho_0,\rho_1,\rho_2\rangle$ is merely a subgroup of $Sym(6)$, but not all $Sym(6)$.

Thus the pair $\{(1,2),(3,4)\}$ cannot be extended in a string C-group that is isomorphic to $Sym(6)$.

(4.8c): $\rho_0=(1,2)$ and $\rho_2=(1,2)(3,4)$

Once again the transitivity of $Sym(6)$ and the fact that ρ_1 must not commute neither with ρ_0 nor with ρ_2 force ρ_1 to be the involution $(1,3)(2,5)(4,6)$, up to isomorphism. As in the case before, the CPR graph argument does not work (see figure 4.3).

However we may use nearly the same argument as in the case before to prove that $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$. Set $\rho_2'=\rho_2\rho_0=(3,4)$. Then

$$\langle\rho_0,\rho_1,\rho_2\rangle=\langle\rho_0,\rho_1,\rho_2'\rangle.$$

However the group $\langle\rho_0,\rho_1,\rho_2'\rangle$ is exactly the group we have examined in the case above. As $\langle\rho_0,\rho_1,\rho_2'\rangle$ is not isomorphic to $Sym(6)$, $\langle\rho_0,\rho_1,\rho_2\rangle=\langle(1,2),(1,3)(2,5)(4,6),(1,3)(2,4)\rangle$ is not isomorphic to $Sym(6)$ neither.

Hence there exists no ρ_1 such that $\langle(1,2),\rho_1,(1,2)(3,4)\rangle\cong Sym(6)$.

(4.8e): $\rho_0=(1,2)(3,4)$ and $\rho_2=(1,3)(2,4)$

In this case, there are several different possibilities for ρ_1, namely $(1,5)(2,6)$ or $(1,5)(4,6)$ and $(1,5)(2,6)(3,4)$ or $(1,5)(4,6)(2,3)$.

Remark 4.3.12. *The possibility* $\rho_1=(1,5)(3,6)$ *may be considered the same as* $(1,5)(2,6)$*. Both are conjugate by the element* $(2,3)$ *and conjugacy by* $(2,3)$ *maps* ρ_0 *on* ρ_2*. In fact this conjugacy does not fix the involutions*

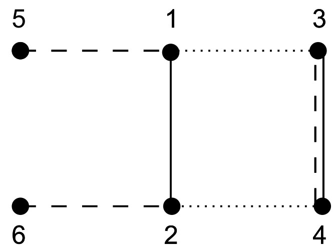

Figure 4.4: CPR graph of $\langle(1,2)(3,4),(1,5)(2,6)(3,4),(1,3)(2,4)\rangle$

ρ_0 and ρ_2, but fixes the unordered pair $\{\rho_0, \rho_2\}$, which is enough, as we are counting the polyhedra up to isomorphism and duality.

If $\rho_1 = (1,5)(2,6)$ or $\rho_1 = (1,5)(4,6)$, the group $\langle\rho_0, \rho_1, \rho_2\rangle$ is a group generated only by even permutations. Hence $\langle\rho_0, \rho_1, \rho_2\rangle$ is a subgroup of $Alt(6)$ and cannot be isomorphic to $Sym(6)$. The question if $\langle(1,2)(3,4),(1,5)(2,6),(1,3)(2,4)\rangle$ or $\langle(1,2)(3,4),(1,5)(4,6),(1,3)(2,4)\rangle$ are isomorphic to $Alt(6)$ is analysed in section 5.3.3.

For $\rho_1 = (1,5)(2,6)(3,4)$, we get the CPR graph shown in figure 4.4.

Assume $\langle(1,2)(3,4),(1,5)(2,6)(3,4),(1,3)(2,4)\rangle$ is a string C-group (hence satisfies (IP)), $\langle(1,2)(3,4),(1,5)(2,6)(3,4),(1,3)(2,4)\rangle \cong Sym(6)$ and let $\mathcal{P}$ be the polyhedron whose automorphism group is $\Gamma(\mathcal{P}) = \langle(1,2)(3,4),(1,5)(2,6)(3,4),(1,3)(2,4)\rangle$. $\Lambda = \{id, (1,2)(3,4)(5,6)\}$ is an automorphism group of the CPR graph in figure 4.4 and divides the six points into three orbits, namely $O_1 = O_2 = \{1,2\}$, $O_3 = O_4 = \{3,4\}$ and $O_5 = O_6 = \{5,6\}$. By Lemma 2.1.6,

$$N = \{\phi \in Sym(6) \mid \phi(v) \in O_v \text{ for all } v \in V(G)\} = \langle(1,2),(3,4),(5,6)\rangle \cong E_8$$

is a normal subgroup of $\Gamma(\mathcal{P}) = Sym(6)$. This is a contradiction as $Alt(6)$ is the only normal subgroup of $Sym(6)$. Thus $\langle\rho_0, \rho_1, \rho_2\rangle \not\cong Sym(6)$.

The case $\rho_1 = (1,5)(4,6)(2,3)$ is treated by exactly the same argument. We do not give the details here, but the interested reader finds it in appendix A.1.

We now consider the two cases, where it is possible to find a third involution ρ_1 such that the three involutions satisfy (IP) and generate $Sym(6)$.

(4.8b): $\rho_0 = (1,2)$ and $\rho_2 = (3,4)(5,6)$

Up to isomorphism, ρ_1 may be the involution $(1,3)(4,5)$, $(1,3)(2,5)$ or $(1,3)(4,5)(2,6)$.

Remark 4.3.13. *Although* $(1,3)(4,5)$ *and* $(1,3)(2,5)$ *are not conjugate by a conjugacy fixing the pair* $\{\rho_0, \rho_2\}$, $(1,3)(4,5)(2,6)$ *and* $(1,3)(2,5)(4,6)$ *are. In fact conjugation by the element* $(5,6)$ *maps* $(1,3)(4,5)(2,6)$ *onto* $(1,3)(2,5)(4,6)$ *and fixes both* ρ_0 *and* ρ_2.

If ρ_1 is the second or the third involution, it can be shown, by using the CPR graphs and lemma 2.1.6, that $\langle \rho_0, \rho_1, \rho_2 \rangle \ncong Sym(6)$. This is done in appendix, A.1.

In the first case, the situation is different. $\langle (1,2), (1,3)(4,5), (3,4)(5,6) \rangle$ is a subgroup of $Sym(6)$ containing the transposition $(1,2)$. Moreover

$$\rho_1\rho_2 = (1,4,6,5,3),$$

and hence $\langle \rho_1, \rho_2 \rangle$ is transitive on the set $\{1,3,4,5,6\}$ and keeps 2 fixed. By lemma 1.2.4, ρ_0, ρ_1 and ρ_2 generate $Sym(6)$. It remains to show that ρ_0, ρ_1 and ρ_2 satisfy (IP). We use lemma 3.2.1.

Set $\Gamma_0 = \langle \rho_1, \rho_2 \rangle$ and $\Gamma_2 = \langle \rho_0, \rho_1 \rangle$ and look at the intersection of Γ_2 and Γ_0. Clearly $\langle \rho_1 \rangle$ is contained in the intersection. As $\rho_0\rho_1 = (1,2,3)(4,5)$ is of order 6, the group Γ_2 is a dihedral group of order 12. The group $\Gamma_0 \cap \Gamma_2$ is a subgroup of Γ_2 and hence its order divides 12. As it contains the cyclic group $\langle \rho_1 \rangle$, its order is 2, 4, 6 or 12. The product $\rho_1\rho_2$ is of order 5 and thus Γ_0 is a dihedral group of order 10. By this reasoning $\Gamma_0 \cap \Gamma_2$ is of order 2 or 10. Combining the two ideas, $\Gamma_0 \cap \Gamma_2$ is of order 2 and hence is equal to $\langle \rho_1 \rangle$. By lemma 3.2.1 (IP) holds.

Thus $\langle (1,2), (1,3)(4,5), (3,4)(5,6) \rangle$ is isomorphic to the group $Sym(6)$ and is the automorphism group of a polyhedron. We compute the Schläfli type of this polyhedron.

$$\begin{aligned} \rho_0\rho_1 &= (1,2,3)(4,5) & &\rightarrow p_1 = 6 \\ \rho_1\rho_2 &= (1,4,6,5,3) & &\rightarrow p_2 = 5 \end{aligned}$$

Hence we get one polyhedron of Schläfli type $\{6,5\}$ with automorphism group isomorphic to $Sym(6)$.

(4.8d): $\rho_0 = (1,2)$ and $\rho_2 = (1,2)(3,4)(5,6)$

This is in fact a very similar case to the previous one. There are once again three possibilities for ρ_1, up to isomorphism: $(1,3)(4,5)$, $(1,3)(2,5)$ or $(1,3)(4,5)(2,6)$. By exactly the same argument as before, the second and the third possibility fail, while for $\rho_1 = (1,3)(4,5)$, $\langle \rho_0, \rho_1, \rho_2 \rangle$ is a string C-group isomorphic to $Sym(6)$. The details are done in appendix A.1.

We compute the Schläfli type of this string C-group.

$$\begin{aligned} \rho_0\rho_1 &= (1,2,3)(4,5) && \to p_1 = 6 \\ \rho_1\rho_2 &= (1,4,6,5,3,2) && \to p_2 = 6 \end{aligned}$$

$Sym(6)$ is then also the automorphism group of a polyhedron of Schläfli type $\{6,6\}$.

To conclude, we get the following theorem.

Theorem 4.3.14. *Up to isomorphism and duality, $Sym(6)$ is the automorphism group of exactly 2 abstract regular polyhedra. These 2 polyhedra have Schläfli type $\{6,5\}$ and $\{6,6\}$.*

Remark 4.3.15. *In [16] Leemans and Vauthier have come to the same result for $Sym(6)$, with the help of a computer.*

4.4 A First General Result and Perspectives

In the sections above, we have found the number of pairs of commuting involutions in $Sym(n)$. We even finished the case for $n = 6$ completely. In this section we give a first general result about polyhedra having a symmetric group as automorphism group. Moreover we formulate ideas for further work.

We start with a first general result for the symmetric groups.

Proposition 4.4.1. *Let $\rho_0 = (1,2)$ and $\rho_2 = (3,4)$ in $Sym(n)$. For $n = 4,5$, there is a unique polyhedron, up to isomorphism, whose automorphism group is $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$. For $n = 4$ it is a polyhedron of Schläfli type $\{3,3\}$. For $n = 5$ it is a polyhedron of Schläfli type $\{4,6\}$. If $n > 5$, there is no polyhedron whose automorphism group is $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$.*

Proof. First notice that by taking $\rho_0 = (1,2)$ and $\rho_2 = (3,4)$, ρ_0 is commuting with ρ_2. We have to choose an involution ρ_1 that does neither commute with $(1,2)$ nor with $(3,4)$, such that $\langle\rho_0,\rho_1,\rho_2\rangle$ satisfies (IP) and $\langle\rho_0,\rho_1,\rho_2\rangle \cong Sym(n)$.

First we consider the case $n = 4$. Then ρ_1 has to be an involution of $Sym(4)\backslash\big(C_{Sym(4)}(\rho_0) \cup C_{Sym(4)}(\rho_2)\big)$. By proposition 4.1.2, we can compute $C_{Sym(4)}(\rho_0)$ and $C_{Sym(4)}(\rho_2)$. So we get

$$\begin{aligned}&C_{Sym(4)}(\rho_0) = \{id,(1,2),(1,2)(3,4),(3,4)\} = C_{Sym(4)}(\rho_2)\\ &\Rightarrow \rho_1 \in \{(1,3),(1,4),(2,3),(2,4),(1,3)(2,4),(1,4)(2,3)\}\,.\end{aligned}$$

Now we let all the automorphisms, that fix the pair $\{\rho_0,\rho_2\}$, act on ρ_1 and we get that, up to isomorphism, $\rho_1 = (1,3)$ or $\rho_1 = (1,3)(2,4)$. The first case is treated as an example in section 2.1 (see figure 2.1) and is associated to a tetrahedron. The automorphism group of the tetrahedron is $Sym(4)$. Hence the first case gives us a polyhedron with automorphism group $Sym(4)$. Moreover the Schläfli type of the tetrahedron is well known to be $\{3,3\}$.

If $\rho_1 = (1,3)(2,4)$, we can see that the group $\langle(1,2),(3,4)\rangle$ is a normal subgroup of $\langle\rho_0,\rho_1,\rho_2\rangle$. However $\langle(1,2),(3,4)\rangle$ is clearly not a normal subgroup of $Sym(4)$ and hence $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(4)$.

Now we consider the case $n = 5$. We compute $C_{Sym(5)}(\rho_0)$ and $C_{Sym(5)}(\rho_2)$. Moreover we want the group $\langle\rho_0,\rho_1,\rho_2\rangle$ to act transitively on the set $\{1,\dots,5\}$. Hence, up to isomorphism, there is only one possible choice for ρ_1, namely $(1,3)(2,5)$. By lemma 1.2.4, we can easily check that $\langle(1,2),(1,3)(2,5),(3,4)\rangle \cong Sym(5)$. Condition (IP) is checked by using lemma 3.2.1. Set $\Gamma_2 = \langle\rho_0,\rho_1\rangle$ and $\Gamma_0 = \langle\rho_1,\rho_2\rangle$. The group $\langle\rho_1\rangle$ is obviously contained in $\Gamma_2 \cap \Gamma_0$. Moreover the group Γ_2 is a dihedral group of order 8 and the group Γ_0 is a dihedral group of order 12. Hence $\Gamma_2 \cap \Gamma_0$ is of order 2 or 4. As every permutation in Γ_2 fixes the element 4, 4 must be fixed under the action of $\Gamma_2 \cap \Gamma_0$. There are four permutations in Γ_0 fixing 4, namely the identity, ρ_1, $(\rho_2\rho_1)^2\rho_2$ and $(\rho_2\rho_1)^3$. If $\Gamma_2 \cap \Gamma_0$ is of order 4, it contains these four permutations and thus they are also contained in Γ_2. Hence $(\rho_2\rho_1)^3$ should be in Γ_2. However $(\rho_2\rho_1)^3 = (2,5)$ and it is easy to see that the only permutation in Γ_2 that permutes 2 and 5 is ρ_1. However it does not fix the elements 1 and 3. Hence $(\rho_2\rho_1)^3 \notin \Gamma_2$ and therefore $\Gamma_2 \cap \Gamma_0$ is equal to the cyclic group $\langle\rho_1\rangle$. By lemma 3.2.1 (IP) is verified. So $\langle(1,2),(1,3)(2,5),(3,4)\rangle \cong Sym(5)$ is the automorphism group of a polyhedron. We compute its Schläfli symbol.

$$\begin{aligned} \rho_0\rho_1 &= (1,5,2,3) && \Rightarrow p_1 = 4 \\ \rho_1\rho_2 &= (1,4,3)(2,5) && \Rightarrow p_2 = 6 \end{aligned}$$

So $Sym(5)$ is the automorphism group of a polyhedron of Schläfli type $\{4,6\}$.

Consider finally the case $n > 5$. Take first $n \geq 7$. The involutions ρ_0 and ρ_2 partition the set $\{1,2,3,4\}$ in $(n-2)$ orbits, namely $\{1,2\}$, $\{3,4\}$ and all the single orbits of the form $\{k\}$, with $k \geq 5$. As we want $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$ and as $Sym(n)$ has only one orbit on its elements, the involution ρ_1 has to map one element of the first orbit on one of the second. The elements $1, 2, 3$ and 4 are now in one orbit and two of them form a 2-cycle of ρ_1. There are 2 elements left in the orbit, but there are at least 3 elements left, that are in no 2-cycle of ρ_0, ρ_2 and ρ_1. Therefore it is impossible that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ is transitive on $\{1, \ldots, n\}$.
If $n = 6$, the only possible choice for ρ_1, up to isomorphism, such that $\langle \rho_0, \rho_1, \rho_2 \rangle$ is transitive, is the involution $(1,3)(2,5)(4,6)$. However we have already seen in section 4.3 that the three involutions $(1,2), (3,4)$ and $(1,3)(2,5)(4,6)$ do not generate $Sym(6)$. □

We make this result more general.

Proposition 4.4.2. *Let ρ_0 and ρ_2 be two commuting involutions in $Sym(n)$. Suppose ρ_0 has cycle type $(2^k, 1^{n-2k})$ and ρ_2 has cycle type $(2^l, 1^{n-2l})$, with exactly m 2-cycles involving only elements from the set $\{1, 2, \ldots, 2k\}$ and $l - m$ 2-cycles involving elements from the set $\{2k+1, \ldots, n\}$. Within the m 2-cycles, j 2-cycles are of the form (s,t) with $|s-t| \geq 2$ and j even.*
Then the pair $\{\rho_0, \rho_2\}$ can be extended by a third involution ρ_1 such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$ if and only if

$$n \leq 2k + 2l - 2m + j + 2. \tag{4.9}$$

Remark 4.4.3. *Of course, it is understood that n is big enough so that it is possible to have ρ_0 and ρ_2, for the given k, l and m, in $Sym(n)$. Moreover if j cycles in ρ_2 are of the form (s,t) with $|s-t| \geq 2$, $m - j$ 2-cycles correspond to 2-cycles involved in ρ_0.*

Proof. As ρ_0 and ρ_2 commute, $\rho_2 \in E_{2^k} : Sym(2k) \times Sym(n-2k)$, by proposition 4.1.2. As ρ_1 is also an involution, ρ_1 just involves 2-cycles in its cycle decomposition. We construct an involution ρ_1 such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$.

The j 2-cycles of ρ_2 permutes some 2-cycles of ρ_0 and give $\frac{j}{2}$ orbits of each time 4 different elements (note that j is even). To fuse these $\frac{j}{2}$ orbits into one orbit, ρ_1 involves a 2-cycle containing an element of the first orbit an an element of the second orbit, a 2-cycle containing an element of the second orbit an an element of the third orbit and so on. This gives $(\frac{j}{2} - 1)$ 2-cycles involved in ρ_1, respectively no 2-cycle if $j = 0$. There are 3 elements left in the first and the last orbit and 2 elements in the other orbits. This gives us $j + 2$ elements that are not involved yet in a 2-cycle of ρ_1. We call such elements "free" elements.

The involution ρ_0 splits $2k - 2j$ elements in orbits of cardinal 2. To fuse these orbits into one orbit, ρ_1 involves $(k-j-1)$ 2-cycles containing elements of different orbits (respectively no 2-cycles again if $k - j = 0$). There are only 2 free elements left. Moreover at this point the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ splits the $2k$ elements involved in ρ_0 into two orbits. To fuse these orbits together, we have to take an element of each one and construct a new 2-cycle. Hence we are left with $(j + 2 - 1) + 1 = j + 2$ free elements.

Now all the elements that are not fixed by ρ_0 are fused into one orbit under the action of $\langle \rho_0, \rho_1, \rho_2 \rangle$. Out of the $2l$ elements not fixed by ρ_2, $2m$ elements are contained in that one orbit, already constructed. So there are $2l - 2m$ elements left, that are split into $l - m$ orbits of cardinal 2. To fuse these elements into one orbit, ρ_1 involves $l - m - 1$ new 2-cycles (or no 2-cycle in the case $l - m = 0$). There are 2 free elements left and we have again two orbits. ρ_1 must involve one more 2-cycle to fuse these orbits together. So there are now again $j + 2$ free elements left.

At this point all the elements not fixed by ρ_0 or ρ_2 are in one orbit under the action of the group $\langle \rho_0, \rho_1, \rho_2 \rangle$. First we count how many elements are fixed by the group $\langle \rho_0, \rho_2 \rangle$, because these elements are still in orbits of size 1. The involution ρ_0 moves $2k$ elements. The involution ρ_2 moves some of these $2k$ elements and $2l - 2m$ elements different from the first ones. Thus there are $2k + 2l - 2m$ elements in the one big orbit and $n - 2k - 2l + 2m$ elements contained in single orbits under the action of $\langle \rho_0, \rho_1, \rho_2 \rangle$. So ρ_1 must involve some more 2-cycles each containing one element of the last $n - 2k - 2l + 2m$ elements and one element of the big orbit.

This is only possible if there are enough free elements left in the big orbit, hence if

$$\begin{aligned} j+2 &\geq n-2k-2l+2m \\ \Leftrightarrow n &\leq 2k+2l-2m+j+2. \end{aligned}$$

This shows that if $n \leq 2k+2l-2m+j+2$, then the construction above is possible and gives one orbit under the action of the group $\langle \rho_0, \rho_1, \rho_2 \rangle$. Hence $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$.

On the contrary, if $n > 2k+2l-2m+j+2$, there are not enough elements left to fuse the elements fixed under the action of $\langle \rho_0, \rho_2 \rangle$, into one orbit together with the other elements. Hence in that case, it is impossible to find an involution ρ_1 such that $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$.

□

With this last proposition, proposition 4.4.1 is proven very quickly. If $\rho_0 = (1,2)$ and $\rho_2 = (3,4)$, then $k=1$, $l=1$, $m=0$, $j=0$ and so $(1,2)$ and $(3,4)$ can be extended by a third involution such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$ if and only if

$$n \leq 2+2-0+0+2 = 6.$$

If $n > 6$, there exists no involution ρ_1 such that $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$, hence there exists no involution ρ_1 such that $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$. If $n \leq 6$, we are sure that there exists at least one such ρ_1. It is left to verify that there exists an involution ρ_1 such that $\langle \rho_0, \rho_1, \rho_2 \rangle$ does not only act transitively on $\{1, \ldots, n\}$, but is also isomorphic to $Sym(n)$ and such that the three involutions ρ_0, ρ_1 and ρ_2 verify (IP). Furthermore it should be verified that the third involution does not commute with the two others. However, this is mostly the case. These verifications are done in the proof of proposition 4.4.1.

We now propose some ideas to follow for further work on this subject. The next step in our work would be step 3 (see section 3.2). In order to do this we fix the pair $\{\rho_0, \rho_2\}$ and look for a third involution not commuting with these two involutions, up to isomorphism and duality. Because of duality, we may always suppose that the involution ρ_2 involves more 2-cycles than the involutions ρ_0. Thus if ρ_0 is of cycle type $(2^k, 1^{n-2k})$ and ρ_2 of cycle type $(2^l, 1^{n-2l})$, then $l \geq k$.

Furthermore, proposition 4.4.2 does not directly involve polyhedra, but may be very useful for further work. Instead of initiating exclusively step 3, we could make a mix of step 3 and step 5. We want the three involutions to generate $Sym(n)$. Hence we want the three involutions to act transitively on the set $\{1, \ldots, n\}$. Suppose we have a fixed pair $\{\rho_0, \rho_2\}$ of commuting involutions. Then proposition 4.4.2 indicates for which n we may find a third involution, such that $\langle \rho_0, \rho_1, \rho_2 \rangle \cong Sym(n)$, and for which n this will be impossible. This idea suggests to pay attention to two arguments. First, while checking step 5 (which may be done without any problem before step 4), proposition 4.4.2 already indicates for which pair $\{\rho_0, \rho_2\}$ and which n, we do not even have to check step 5, because we already know that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$, whatever ρ_1 we have chosen, is not isomorphic to $Sym(n)$. Moreover, instead of only looking for a third involution ρ_1 not commuting with ρ_0 and ρ_2, we may look for a third involution not commuting with the other *and* such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \ldots, n\}$. Note that often, if ρ_1 is chosen such that $\langle \rho_0, \rho_1, \rho_2 \rangle$ is transitive on $\{1, \ldots, n\}$, then the non-commuting condition is satisfied automatically.

4.5 Conclusion

To finalize this chapter, we quickly discuss what we have done so far.

We have established a formula to compute the centralizer of an involution in $Sym(n)$, for a general n (see proposition 4.1.2). Although the general formula of a centralizer of an element in $Sym(n)$ is well known (see theorem 4.1.7), this work was important. The work was done independently of the existing theorem 4.1.7. This allowed us to understand the centralizers of involutions in $Sym(n)$ much better. Moreover, our new formula reveals more clearly the structure of these centralizers. Hence it constitutes a useful step in this thesis.

Furthermore, we have got a general formula for computing the number of ordered and unordered pairs of commuting involutions in $Sym(n)$ (see 4.2.1 and 4.2.2). This is not only a useful step in the search for polyhedra whose automorphism groups are symmetric groups, but may also be used in other research areas. Clearly this formula is useful to look for regular polytopes, of general dimension, whose automorphism groups are symmetric groups. This work is done for specific dimensions by several mathematicians [6][7]. Moreover it is an interesting result in general group theory. Articles, as for example [22], show that people are interested in commuting involutions.

[7] In [6], Leemans and Carrancho will prove results about the symmetric group of degree n and its polytopes of rank k, with $3 \leq k \leq n-1$.

To illustrate that our basic idea is correct, we have done the case $Sym(6)$ completely by hand, without the help of a computer.

Unfortunately we have not finished the work we had planned in the beginning, the problem being much more complex than we thought. We have initiated step 3 of the basic idea and have given some ideas for future work. However the fact that one has to consider both the centralizer of ρ_0 and of ρ_2 and looking for an involution not contained in both and counting them up to conjugacy, turns the problem into a very complex problem. Table A.1 also shows the complexity of the problem, as the number of polyhedra quickly increases.

To conclude, the problem of finding the number of polyhedra on which a symmetric group acts as automorphism group, is much too complex for a Master's thesis, but the work done in this thesis constitutes a good start.

Chapter 5

The Alternating Groups

In this chapter we try to do the same work, as we did in chapter 4, for the alternating groups. In this first section we establish the general form of the centralizer of a given involution in $Alt(n)$. Given proposition 4.1, this work is not very difficult any more and the section is quickly concluded. In section 5.2, we construct a formula computing the number of unordered and the number of ordered pairs of commuting involutions in $Alt(n)$. This work finishes step 2 of the basic idea for the alternating groups. Then, in section 5.3, we deal with the special case $n = 6$. In section 5.4, we give some ideas for future work and finally in the last section, we draw a conclusion on this work.

5.1 The Centralizer of an Involution in $Alt(n)$

In section 4.1, we have established the general form of a centralizer of an involution in the symmetric group of degree n. In this section we do the same work for the alternating group of degree n. We prove the following proposition

Proposition 5.1.1. *Let ρ be an involution with of cycle type $(2^k, 1^{n-2k})$ in $Alt(n)$. Then $C_{Alt(n)}(\rho) = \{\sigma \in E_{2^k} : Sym(k) \times Sym(n-2k) \mid \sigma \in Alt(n)\}$ and we also get $|C_{Alt(n)}(\rho)| = 2^{k-1} \times k! \times (n-2k)!$*

Proof. We know that $Alt(n) \leqslant Sym(n)$. So $C_{Alt(n)}(\rho) \leqslant C_{Sym(n)}(\rho)$. Moreover, as an involution contains at least one cycle of even length, proposition

1.2.8 implies that the conjugacy class of an involution in $Alt(n)$ corresponds to the class of all involutions of same cycle type. Thus it is the same as the conjugacy class of that involution in $Sym(n)$. Hence by lemma 4.1.5 $C_{Alt(n)}(\rho)$ is not equal to $C_{Sym(n)}(\rho)$, but is merely a subgroup of index 2 of it. In fact it is the subgroup of all even permutations of $C_{Sym(n)}(\rho)$. Also the order of $C_{Alt(n)}(\rho)$ is half of the order of $C_{Sym(n)}(\rho)$. □

5.2 Commuting Involutions in $Alt(n)$, $n \neq 6$

As in section 4.2, we start with step 1 of the basic idea. By theorem 1.2.8, all involutions of same cycle type in $Alt(n)$ are conjugate and thus the number of possibilities of choosing a first involution ρ_0, up to conjugacy, equals the number of different cycle types in $Alt(n)$, with $n \neq 6$. Again, the case $n = 6$ is analysed separately in section 5.3. An involution in $Alt(n)$ has cycle type $(2^k, 1^{n-2k})$ with k an even integer between 1 and $\lfloor \frac{n}{2} \rfloor$. Hence there are $\lfloor \frac{n}{4} \rfloor$ different possibilities, up to isomorphism, for choosing a first involution ρ_0 in $Alt(n)$. This finishes step 1.

Step 2 of the basic idea consists of choosing a second involution ρ_2, commuting with ρ_0, in $Alt(n)$, once ρ_0 is fixed. Hence we choose a pair of commuting involutions in $Alt(n)$.

We first compute, in the following lemma, the number of *ordered* pairs of commuting involutions in $Alt(n)$ for $n \neq 6$.

Lemma 5.2.1. *Let $n \neq 6$ be a positive integer. Up to isomorphism, there are $\mu(n)$ ordered pairs of commuting involutions ρ_0 and ρ_2 in $Alt(n)$, where*

$$\mu(n) = -2 \cdot \lfloor \frac{n}{4} \rfloor + \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \left[\lambda_e(k) \cdot \lceil \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil + \lambda_o(k) \cdot \lfloor \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rfloor \right]$$

and

$$\lambda_e(k) = \frac{k^2}{8} + \frac{3k}{4} + 1,$$
$$\lambda_o(k) = \frac{k^2}{8} + \frac{k}{4}.$$

Proof. We start in the same way as in the proof of lemma 4.2.1. We take ρ_0 an involution of cycle type $(2^k, 1^{n-2k})$, k even, and $\rho_2 \in C_{Alt(n)}(\rho_0) =$

$\{\sigma \in E_{2^k} : Sym(k) \times Sym(n-2k) \mid \sigma \in Alt(n)\}$. We proceed in the same way by counting first the possibilities for an involution ρ_2 acting only on elements of $\{1, 2, \ldots, 2k\}$.

We consider the involutions up to isomorphism and $Aut(Alt(n)) = Aut(Sym(n))$. By proposition 1.2.8, if an involution is conjugate to ρ_2 in $Sym(n)$, then in $Alt(n)$ it is also conjugate to ρ_2. Therefore we can apply the same reasoning as in the proof of lemma 4.2.1 and we suppose ρ_2 is composed of l 2-cycles, where m 2-cycles are of the form (s,t), with $|s-t| \geq 2$ and $s,t \leq 2k$, $m \leq l$ and $l-m$ 2-cycles are of the form $(2r-1, 2r)$, with $1 \leq r \leq k$. We have to count the number of possibilities for m, with m even. So, as before, m can take every even value between 0 and l, which gives us $\lfloor \frac{l}{2} \rfloor + 1$ possibilities for m, for a given l. What changes now are the possibilities for l. In the previous proof, l could take every value between 0 and k. In this proof, we have to distinguish between the case when l takes an even value and when l takes an odd value. Let $\lambda_e(k)$ denote the number of possible involutions ρ_2 with an even number of 2-cycles involving only elements of $\{1, 2, \ldots, 2k\}$. Then

$$\begin{aligned}
\lambda_e(k) &= \sum_{\substack{l=0 \\ l \text{ even}}}^{k} \left(\frac{l}{2} + 1\right) \\
&= \frac{k}{2} + 1 + \sum_{\substack{l=0 \\ l \text{ even}}}^{k} \frac{l}{2} \\
&= \frac{k}{2} + 1 + \sum_{j=0}^{\frac{k}{2}} j \\
&= \frac{k}{2} + 1 + \frac{\frac{k}{2} \cdot (\frac{k}{2} + 1)}{2} \\
&= \frac{k}{2} + 1 + \frac{k^2}{8} + \frac{k}{4} \\
&= \frac{k^2}{8} + \frac{3k}{4} + 1.
\end{aligned}$$

Let $\lambda_o(k)$ denote the number of possible involutions ρ_2 with an odd number of 2-cycles involving elements in $\{1, 2, \ldots, 2k\}$. Then

$$\begin{aligned}
\lambda_o(k) &= \sum_{\substack{l=0 \\ l \text{ odd}}}^{k} (\lfloor \frac{l}{2} \rfloor + 1) \\
&= \frac{k}{2} + \sum_{\substack{l=0 \\ l \text{ odd}}}^{k} \lfloor \frac{l}{2} \rfloor \\
&= \frac{k}{2} + \sum_{j=0}^{\frac{k}{2}-1} j \\
&= \frac{k}{2} + \frac{\frac{k}{2} \cdot (\frac{k}{2} - 1)}{2} \\
&= \frac{k}{2} + \frac{k^2}{8} - \frac{k}{4} \\
&= \frac{k^2}{8} + \frac{k}{4}.
\end{aligned}$$

As before we add the 2-cycles composed of elements of the set $\{2k+1, \ldots, n\}$. An involution in $Sym(n-2k)$ can have j 2-cycles with j a number between 0 and $\lfloor \frac{n-2k}{2} \rfloor$. As the involution ρ_2 is in $Alt(n)$, either l and j are even, or l and j are odd. There are exactly $\lceil \frac{1}{2}(\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil$ even integers between 0 and $\lfloor \frac{n-2k}{2} \rfloor$ and hence there are $\lceil \frac{1}{2}(\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil$ possibilities for j taking an even value. These possibilities have to be multiplied by $\lambda_e(k)$. On the other side there are $\lfloor \frac{1}{2}(\lfloor \frac{n-2k}{2} \rfloor + 1) \rfloor$ odd integers between 0 and $\lfloor \frac{n-2k}{2} \rfloor$, which gives us $\lfloor \frac{1}{2}(\lfloor \frac{n-2k}{2} \rfloor + 1) \rfloor$ possibilities for j taking an odd value. These possibilities have to be multiplied by $\lambda_o(k)$.

As before we have to subtract the two possibilities where ρ_2 is the identity and where ρ_2 is equal to ρ_0. In both cases l and j are even. So we have to subtract 2 from the number $\lambda_e(k) \cdot \lceil \frac{1}{2}(\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil$ and sum up all these possibilities for every even k between 1 and $\lfloor \frac{n}{2} \rfloor$. This leads to

$$\begin{aligned}
&\sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \left[(\lambda_e(k) \cdot \lceil \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil - 2) + \lambda_o(k) \cdot \lfloor \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rfloor \right] \\
&= -2 \cdot \lfloor \frac{n}{4} \rfloor \\
&\qquad + \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \left[\lambda_e(k) \cdot \lceil \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rceil + \lambda_o(k) \cdot \lfloor \frac{1}{2} \cdot (\lfloor \frac{n-2k}{2} \rfloor + 1) \rfloor \right].
\end{aligned}$$

□

With the help of lemma 5.2.1, we may compute the number of *unordered* pairs of commuting involutions in $Alt(n)$. This is done in the next theorem.

Theorem 5.2.2. *Let $\lambda''(k)$ be as in section 4.2 (see (4.3)) and $\mu(n)$ defined as in lemma 5.2.1. Then in $Alt(n)$, with $n \neq 6$, there are, up to isomorphism,*

$$\frac{1}{2}\left(\mu(n) + \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \lambda''(k)\right)$$

pairs of commuting involutions ρ_0 and ρ_2.

Proof. We can proceed in exactly the same way as in the proof of theorem 4.2.2. To compute the number of unordered pairs of commuting involutions in $Alt(n)$, we subtract the number of ordered pairs which have no dual pair, from $\mu(n)$, divide the whole by 2 and then add again the number of pairs which have no dual pair. In the case $Alt(n)$ the pairs of involutions which have no dual pair are also the pairs $[\rho_0, \rho_2]$ with ρ_0 and ρ_2 having the same cycle type. We may count them in exactly the same way as in the proof of theorem 4.2.2. Set again $\lambda''(k)$ the number of ordered pairs $[\rho_0, \rho_2]$ of commuting involutions with ρ_0 and ρ_2 of cycle type $(2^k, 1^{n-2k})$. The number of all the pairs $[\rho_0, \rho_2]$ having the same cycle type is again the sum of all the $\lambda''(k)$. However, as we are working in $Alt(n)$, we only take k even. Hence the number of pairs of commuting involutions which have no dual pair is

$$\sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \lambda''(k).$$

Thus the general formula to compute the number of unordered pairs of commuting involutions in $Alt(n)$ is

$$\frac{1}{2}\left(\mu(n) - \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \lambda''(k)\right) + \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \lambda''(k) = \frac{1}{2}\left(\mu(n) + \sum_{\substack{k=1 \\ k \text{ even}}}^{\lfloor \frac{n}{2} \rfloor} \lambda''(k)\right).$$

□

Remark 5.2.3. *In this case we did not simplify the general formula, because in the term $\lambda''(k)$ appears $\lambda(k)$, but the term $\mu(k)$ is computed based on the terms $\lambda_e(k)$ and $\lambda_o(k)$. Thus there is no possibility of simplifying the general formula.*

Remark 5.2.4. *Some results given by the formulas in lemma 5.2.1 and theorem 5.2.2 are shown in table A.2 and table A.3 in section A.3 of the appendices.*

Note that also in this case, the two formulas of lemma 5.2.1 and theorem 5.2.2 give the same result for n and $n+1$, with n even. Once again this is justified either by looking closely at the formulas, either by analysing the question directly, exactly as we did with the symmetric groups.

5.3 The Particular Case of $Alt(6)$

We now analyse the case $n = 6$. We first look for the pairs of commuting involutions in $Alt(6)$ and so we prove the following theorem.

Lemma 5.3.1. *In $Alt(6)$ there is only one pair of commuting involutions, up to isomorphism.*

First we can apply our formula for computing the number of ordered pairs of involutions in $Alt(6)$, up to conjugacy, but it does not give the final result. It merely determines an intermediate step. As the automorphism group of $Alt(6)$ is four times bigger than $Alt(6)$, there are automorphisms acting on $Alt(6)$ that are no conjugacy by any element in $Sym(6)$. These automorphisms may fuse the orbits obtained under the action of $Sym(6)$ on $Alt(6)$. Table A.2 in the appendices shows that the formula computed in theorem 5.2.2 gives 2 pairs of involutions in $Alt(6)$.

It remains to prove that the "outer"[1] automorphisms of $Alt(6)$ fuse these two orbits together. We will do this in two different ways, one geometric and one algebraic.

5.3.1 The Geometric Way

We prove Lemma 5.3.1 in a geometric way. We take the same reasoning as in section 4.3. The automorphism group of $Alt(6)$ is the same as the automorphism group of $Sym(6)$. In $Sym(6)$ we are left with 5 pairs of commuting involutions, up to isomorphism. They are shown in (4.8). Only

[1] The term "outer" is not really correct, as conjugacy by an element of $Sym(6)$ is also an outer automorphism of $Alt(6)$. However by "outer" we mean here the action of the outer automorphisms of $Sym(6)$ on $Alt(6)$.

the pair (4.8e) corresponds to a pair of commuting involutions in $Alt(6)$. Hence in $Alt(6)$ we are left with exactly one pair of commuting involutions, namely $(1,2)(3,4)$ and $(1,3)(2,4)$. Thus lemma 5.3.1 is proven.

5.3.2 The Algebraic Way

Although lemma 5.3.1 is proven in the section above, we prove it again in this section by using the fact that $Alt(6)$ is isomorphic to the group $PSL(2,9)$ (see (1.3)), the group of all matrices of determinant 1 with entries in $\mathbb{F}_9$ quotiented by the group of all scalar matrices of $SL(2,9)$. First we compute the form of an involution in $PSL(2,9)$. We set $\mathbb{F}_9 = \{0,1,i,i^2,i^3,i^4,i^5,i^6,i^7 \mid i^8 = 1\}$. It is easy to see that an involution has the following form:

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix},$$

with $a,b,c \in \mathbb{F}_9$ and $a^2 + bc = -1 = i^4$. If $a \in \{i^2, i^6\}$, then $bc = 0$. Either $b = 0$ and c takes one of the 8 values in $\mathbb{F}_9^*$, either $c = 0$ and b takes one of the 8 values in $\mathbb{F}_9^*$ or $b = c = 0$. This gives already $2 \cdot (8+8+1) = 34$ possibilities for choosing the entries a, b and c. If $a \in \mathbb{F}_9 \setminus \{i^2, i^6\}$, then for each $b \in \mathbb{F}_9^*$, there is exactly one c satisfying the equation, because $\mathbb{F}_9$ is a field. This gives $7 \cdot 8 = 56$ additional possibilities. To sum up there are 90 involutions in $SL(2,9)$ and 45 involutions in $PSL(2,9)$. This result agrees with the 45 involutions in $Alt(6)$ (see table A.1 in the appendices). As all the involutions in $Alt(6)$ have cycle type $(2^2, 1^2)$, all involutions are conjugate, by theorem 1.2.8. So are all involutions in $PSL(2,9)$. All the possible choices for ρ_0 are isomorphic. We choose ρ_0 to be the matrix

$$\begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix}.$$

Next we look for the involutions that commute with ρ_0.

$$\begin{aligned}
&\begin{pmatrix} a & b \\ c & -a \end{pmatrix}\begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix} = \begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix}\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \\
\Leftrightarrow &\begin{pmatrix} ai^6 & bi^2 \\ ci^6 & -ai^2 \end{pmatrix} = \begin{pmatrix} ai^6 & bi^6 \\ ci^2 & -ai^2 \end{pmatrix} \\
\Leftrightarrow &\begin{matrix} b = c = 0 \\ a^2 = -1 = i^4 \end{matrix} \quad \text{or} \quad \begin{matrix} a = 0 \\ bc = -1 = i^4 \end{matrix}
\end{aligned}$$

So an involution commuting with ρ_0 is either ρ_0, $-\rho_0$ or of the form

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \text{ with } bc = -1 = i^4.$$

As $\mathbb{F}_9$ is a field, for each $b \in \mathbb{F}_9^*$, there is exactly one $c \in \mathbb{F}_9^*$ satisfying $bc = -1$. Thus we get 8 different involutions commuting with ρ_0 in $SL(2,9)$, which means 4 different involutions in $PSL(2,9)$, as we did when we looked at $Alt(6)$ as a permutation group of degree 6 (see proposition 5.1.1). The four involutions are the following

$$\begin{pmatrix} 0 & i^2 \\ i^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i^4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i^3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i^3 \\ i & 0 \end{pmatrix}.$$

The former computations showed that these 4 involutions are divided in two conjugacy classes if we consider $Sym(6)$ acting on $Alt(6)$. It is well known that $Sym(6) \cong P\Sigma L(2,9)$ (see section 1.2.3). If we consider $P\Sigma L(2,9)$ acting on $PSL(2,9)$, the two classes are

$$\left\{ \begin{pmatrix} 0 & i^2 \\ i^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i^4 \\ 1 & 0 \end{pmatrix} \right\} \text{ and } \left\{ \begin{pmatrix} 0 & i \\ i^3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i^3 \\ i & 0 \end{pmatrix} \right\}.$$

In fact the conjugation by the matrix

$$\begin{pmatrix} i & 0 \\ 0 & i^7 \end{pmatrix} \in PSL(2,9)$$

maps the 2 involutions of the first conjugacy class one on the other and fixes ρ_0. The field automorphism which lies in $P\Sigma L(2,9)$ and which consists of mapping each matrix entry to its 3rd power gives the second conjugacy class and fixes ρ_0. By our former argument we are sure that the group $P\Sigma L(2,9)$ will not fuse these two conjugacy classes.

However the particularity of $Alt(6)$ and $Sym(6)$ is that their automorphism group is twice bigger than $Sym(6)$, that is the group $P\Gamma L(2,9)$ (see section 1.2.3). Long, but not difficult calculations show that in $P\Gamma L(2,9)$ the 2 classes are fused together. Set

$$\gamma = \begin{pmatrix} 1 & 0 \\ 0 & i^3 \end{pmatrix}.$$

It is easy to see that γ is in $P\Gamma L(2,9)$ without being in $P\Sigma L(2,9)$. The conjugation by γ fixes ρ_0 and fuses the 2 conjugacy classes. In fact

$$\begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix}^{\gamma} = \frac{1}{i^3} \begin{pmatrix} 1 & 0 \\ 0 & i^3 \end{pmatrix} \begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix} \begin{pmatrix} i^3 & 0 \\ 0 & 1 \end{pmatrix} = i^5 \begin{pmatrix} i & 0 \\ 0 & i^5 \end{pmatrix} = \begin{pmatrix} i^6 & 0 \\ 0 & i^2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & i^4 \\ 1 & 0 \end{pmatrix}^{\gamma} = \frac{1}{i^3} \begin{pmatrix} 1 & 0 \\ 0 & i^3 \end{pmatrix} \begin{pmatrix} 0 & i^4 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i^3 & 0 \\ 0 & 1 \end{pmatrix} = i^5 \begin{pmatrix} 0 & i^4 \\ i^6 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i^3 & 0 \end{pmatrix}.$$

To conclude, the algebraic way shows that all choices of ρ_0 in $Alt(6)$ are isomorphic and once ρ_0 fixed, all choices for choosing ρ_2 are isomorphic. Therefore, up to isomorphism there is only one pair of commuting involutions in $Alt(6)$, and we have proven Lemma 5.3.1.

5.3.3 Polyhedra with Automorphism Group $Alt(6)$

The two previous sections showed that there is, up to isomorphism, only one pair of commuting involutions in $Alt(6)$. We choose $\rho_0 = (1,2)(3,4)$ and $\rho_2 = (1,3)(2,4)$. We are looking for an involution ρ_1 that is not commuting neither with ρ_0 nor with ρ_2 and such that the three involutions satisfy (IP) and generate $Alt(6)$. We look at all the possibilities up to duality. As seen in section 4.3.2, case (4.8e), the transitivity of $Alt(6)$ forces ρ_1 to be the involution $(1,5)(2,6)$ or the involution $(1,5)(4,6)$, up to isomorphism and duality. We will show that in both cases, these three involutions do not generate all of $Alt(6)$.

On the contrary, assume that they do, with $\rho_1 = (1,5)(2,6)$ and suppose ρ_0, ρ_1 and ρ_2 satisfy (IP). We compute the Schläfli type of the polyhedron whose automorphism group is generated by the three involutions.

$$\begin{aligned}\rho_0\rho_1 &= (1,6,2,5)(3,4) \to p_1 = 4\\ \rho_1\rho_2 &= (1,5,3)(2,6,4) \to p_2 = 3\end{aligned}$$

The Schläfli type of this polyhedron is $\{4,3\}$, that is the Schläfli type of the cube. It is well known that the automorphism group of the cube is $Sym(4) \times \mathbb{Z}_2$. So $\langle \rho_0, \rho_1, \rho_2 \rangle$ has order at most 48 and can thus not be isomorphic to $Alt(6)$[2].

Suppose now $\rho_1 = (1,5)(4,6)$ and assume ρ_0, ρ_1 and ρ_2 satisfy (IP). We compute once again the Schläfli type.

$$\begin{aligned}\rho_0\rho_1 &= (1,2,5)(3,6,4) \to p_1 = 3\\ \rho_1\rho_2 &= (1,5,3)(2,4,6) \to p_2 = 3\end{aligned}$$

[2] It is a well known fact that the cube, like all the other regular convex polyhedra, is a universal polytope. Moreover every regular polytope is a quotient of a universal polytope and every automorphism group of a regular polytope is a quotient of the automorphism group of the corresponding universal polytope. Hence if the automorphism group of the universal polyhedron corresponding to the Schläfli type $\{4,3\}$ is strictly included in $Alt(6)$, the automorphism group of any polyhedron of this Schläfli type is strictly included in $Alt(6)$. For this see also theorem 1.1.6.

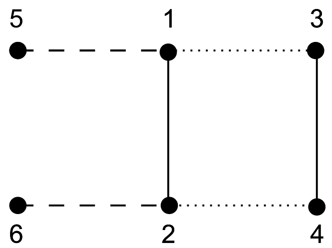

Figure 5.1: CPR graph of $\langle(1,2)(3,4),(1,5)(2,6),(1,3)(2,4)\rangle$

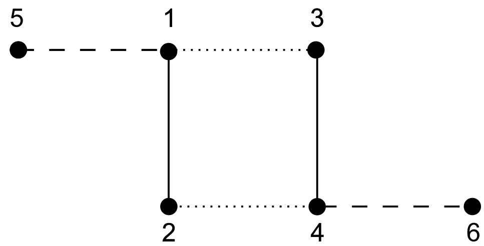

Figure 5.2: CPR of $\langle(1,2)(3,4),(1,5)(4,6),(1,3)(2,4)\rangle$

This time the Schläfli type of this polyhedron is $\{3,3\}$, which is the Schläfli type of the tetrahedron. The automorphism group of the tetrahedron is $Sym(4)$ which is strictly included in $Alt(6)$[3].

This confirms the following well known theorem (see for instance theorem 2.3.1):

Theorem 5.3.2. *No polyhedron has automorphism group isomorphic to* $Alt(6)$*.*

This theorem can also be showed by using the CPR graphs, more precisely lemma 2.1.6.

Suppose $\langle(1,2)(3,4),\rho_1,(1,3)(2,4)\rangle \cong Alt(6)$, with $\rho_1 = (1,5)(2,6)$ or $\rho_1 = (1,5)(4,6)$, and let $\mathcal{P}$ be the polyhedron whose automorphism group is $\langle(1,2)(3,4),\rho_1,(1,3)(2,4)\rangle$. So we suppose $\Gamma(\mathcal{P}) = Alt(6)$. The corresponding CPR graph for $\rho_1 = (1,5)(2,6)$ is shown in figure 5.1 and for $\rho_1 = (1,5)(4,6)$ in figure 5.2.

Both graphs have a non-trivial automorphism and hence by lemma 2.1.6, we get a normal subgroup of $Alt(6)$. This is a contradiction as $Alt(6)$ is simple.

[3]As the tetrahedron is a regular convex polyhedron, its automorphism group is a finite string Coxeter group by theorem 1.1.6, and we apply the same argument as before.

5.4 A First General Result and Perspectives

In this section we formulate the equivalent of proposition 4.4.2 for the alternating groups. In order to do this we introduce a new notation:

$$\|x\| = \max\{x, 0\}$$

In fact $\|x\|$ is equal to x if x is positive and 0 otherwise.

Proposition 5.4.1. *Let ρ_0 and ρ_2 be two commuting involutions in $Alt(n)$. Suppose ρ_0 has cycle type $(2^k, 1^{n-2k})$ and ρ_2 has cycle type $(2^l, 1^{n-2l})$, with exactly m 2-cycles involving only elements from the set $\{1, 2, \dots, 2k\}$ and $l - m$ 2-cycles involving elements from the set $\{2k+1, \dots, n\}$. Within the m 2-cycles, j 2-cycles are of the form (s, t) with $|s - t| \geq 2$ and j even. Set*

$$\omega = \|\frac{j}{2} - 1\| + \|k - j - 1\| + \|l - m - 1\| + \delta(k, j, l - m), \tag{5.1}$$

where

$$\delta(k, j, l - m) = \begin{cases} 2 \text{ if } j, l - m, k - j \neq 0, \\ 1 \text{ if exactly one term in } \{j, l - m, k - j\} \text{ is } 0, \\ 0 \text{ otherwise }. \end{cases}$$

For ω even, the pair $\{\rho_0, \rho_2\}$ can be extended by a third involution ρ_1 such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \dots, n\}$ if and only if

$$n \text{ even and } n \leq 2k + 2l - 2m + j + 2,$$
$$\text{or } n \text{ odd and } n \leq 2k + 2l - 2m + j.$$

For ω odd, the pair $\{\rho_0, \rho_2\}$ can be extended by a third involution ρ_1 such that the group $\langle \rho_0, \rho_1, \rho_2 \rangle$ acts transitively on the set $\{1, \dots, n\}$ if and only if

$$n \text{ even and } n \leq 2k + 2l - 2m + j,$$
$$\text{or } n \text{ odd and } n \leq 2k + 2l - 2m + j + 2.$$

Remark 5.4.2. *As in proposition 4.4.2, it is understood that n is big enough so that it is possible for ρ_0 and ρ_2, for the given k, l and m, to exist in $Alt(n)$. Moreover if j cycles in ρ_2 are of the form (s, t) with $|s - t| \geq 2$, $m - j$ 2-cycles correspond to 2-cycles involved in ρ_0.*

Proof. We start as in the proof of proposition 4.4.2 and construct ρ_1 in exactly the same way. However in this case we have a supplementary constraint, namely the fact that the number of 2-cycles involved in ρ_1 must be even. Let us sum up the hypotheses of the proof of proposition 4.4.2. To fuse all the elements involved in ρ_0 and ρ_2, the involution ρ_1 contains ω 2-cycles. In fact the first term in (5.1) fuses all the elements contained in the j 2-cycles of ρ_2 into one orbit. The second term fuses all the elements involved in ρ_0, but not in one of the j 2-cycles, into one orbit and the third term fuses the elements involved in ρ_2, but not yet contained in one of the latter orbits, into one orbit. If none of the terms $k-j$, j and $l-m$ is equal to 0, we have 3 orbits and so ρ_1 has to contain 2 ($=\delta(k,j,l-m)$) more 2-cycles to fuse these orbits together. If however exactly one of these terms is 0, ρ_1 must only contain one more 2-cycle to fuse the two orbits together. Otherwise, the $(k-j-1)$ 2-cycles fuse all the elements involved in ρ_0 and ρ_2 into one orbit and hence there is no need for a supplementary orbit. Hence ρ_1 contains at least ω 2-cycles. As in the proof of proposition 4.4.2, there are $n-2k-2l+2m$ elements left, that are still contained in single orbits and there are also $j+2$ free elements left. To fuse these $n-2k-2l+2m$ into the same big orbit, as the other elements, ρ_1 must contain at least $n-2k-2l+2m$ more 2-cycles. However ρ_1 must also contain an even number of 2-cycles. Hence if ω is even, $n-2k-2l+2m$ has to be even and if ω is odd, $n-2k-2l+2m$ has to be odd. The sign of $n-2k-2l+2m$ depends only on n. Thus if ω is even and n is even, or ω is odd and n is odd, we get again condition (4.9) (see proposition 4.4.2). Otherwise ρ_1 must contain one more 2-cycle to make the number of 2-cycles even. In that case 2 elements out of the $(j+2)$ free elements are involved in a supplementary 2-cycle and thus

$$\begin{aligned} j &\geq n-2k-2l+2m \\ \Leftrightarrow n &\leq 2k+2l-2m+j. \end{aligned}$$

If we put all these elements together, we get proposition 5.4.1. □

Let us take an example to illustrate the formula. We take the most simplest example, namely $\rho_0=(1,2)(3,4)$. We have seen before that, up to conjugacy, $\rho_2=(1,2)(5,6)$ or $\rho_2=(1,3)(2,4)$. First we consider the case $\rho_2=(1,2)(5,6)$. Then we have

$$k=2,\ l=2,\ m=1,\ ,j=0,\ \omega=0+1+0+1=2.$$

By proposition 5.4.1, it is possible to extend the pair $\{\rho_0,\rho_2\}$ by a third involution ρ_1 such that the three involutions act transitively on $\{1,2,\ldots,n\}$

if and only if

$$\begin{aligned} &n \text{ even and } n \leq 8, \\ \text{or } &n \text{ odd and } n \leq 6. \end{aligned}$$

Hence it is possible to extend $\{\rho_0, \rho_2\}$ by third involution if and only if n is equal to 6 or 8.

We consider now the case $\rho_2 = (1,3)(2,4)$. Then

$$k = 2,\ l = 2,\ m = 2,\ j = 2,\ \omega = 0 + 0 + 0 + 0 = 0.$$

It is possible to extend the pair $\{\rho_0, \rho_2\}$ by a third involution ρ_1 such that the three involutions act transitively on $\{1, 2, \dots, n\}$ if and only if

$$\begin{aligned} &n \text{ even and } n \leq 8, \\ \text{or } &n \text{ odd and } n \leq 6, \end{aligned}$$

hence, if n is equal to 4, 5, 6 or 8.

The next step in this work would be step 3 of the basic idea (see section 3.2). We have found the number of commuting involutions $\{\rho_0, \rho_2\}$. So we fix each pair and look for a third involution ρ_1 not commuting with the first two involutions. The counting is done up to isomorphism and duality. Thus we may again suppose that the involution ρ_2 involves more 2-cycles as the involution ρ_0. Again it is more efficient to make a mix of step 3 and step 5, by choosing only candidates ρ_1 such that the three involutions are transitive on the set $\{1, 2, \dots, n\}$. Proposition 5.4.1 may be helpful in order to do this.

5.5 Conclusion

As in the previous chapter, we now give a small feedback of what we have done for the alternating groups. The work is shorter and done faster than the one for the symmetric groups, because once the study is done for the symmetric groups, the work is much easier for the alternating groups. The results of this chapter are merely corollaries of those in chapter 4, because the basic idea was already fixed by doing the work for the symmetric groups. Although one has to be careful, because in the work with alternating groups, one may only consider involutions involving an even number of 2-cycles. So in this chapter we had just to adapt the previous work. There are nevertheless some interesting results in this chapter. In spite of what one may have expected, the formula for computing the number of unordered and ordered pairs of commuting involutions in $Alt(n)$ looks different from the one for $Sym(n)$.

Furthermore the transposition of the problem of the special case of $Alt(6)$ in the special linear group $PSL(2, 9)$, to see how the automorphism group works on $Alt(6)$, gives an interesting section, and turns the problem, which seems not so easy in $Alt(6)$, into a mere algebraic computation problem.

Also in this chapter we did not manage to achieve the final goal, because this chapter constitutes more or less an adaptation of our work on the symmetric groups to their only normal subgroups.

pour des bons headings dans les appendices

Appendix

A.1 Polyhedra with Automorphism Group $Sym(6)$: case by case analysis

In this section we analyse the cases which are left out in section 4.3.2.

(4.8e): $\rho_0 = (1,2)(3,4)$ and $\rho_2 = (1,3)(2,4)$

The only case left is the case $\rho_1 = (1,5)(4,6)(2,3)$. The CPR graph corresponding to $\langle(1,2)(3,4),(1,5)(4,6)(2,3),(1,3)(2,4)\rangle$ is shown in figure A.1.

$\Lambda = \{id,(1,4)(2,3)(5,6)\}$ is an automorphism group of the CPR graph in figure A.1. By Lemma 2.1.6, we get a normal subgroup $N = \langle(1,4),(2,3),(5,6)\rangle$ of $\langle\rho_0,\rho_1,\rho_2\rangle$. Thus $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$.

(4.8b): $\rho_0 = (1,2)$ and $\rho_2 = (3,4)(5,6)$

The cases left to analyse are the cases $\rho_1 = (1,3)(2,5)$ and $\rho_1 = (1,3)(4,5)(2,6)$. Their associated CPR graphs are shown in figure A.2 and A.3.

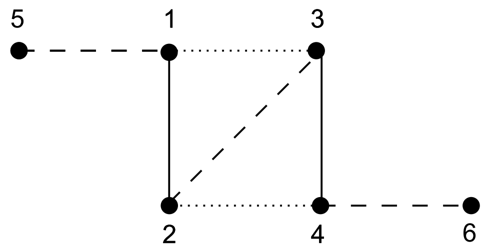

Figure A.1: CPR graph of $\langle(1,2)(3,4),(1,5)(4,6)(2,3),(1,3)(2,4)\rangle$

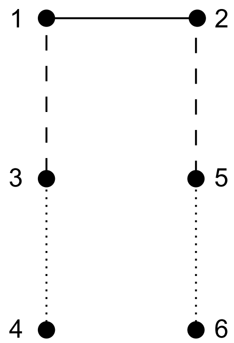

Figure A.2: CPR graph of $\langle(1,2),(1,3)(2,5),(3,4)(5,6)\rangle$

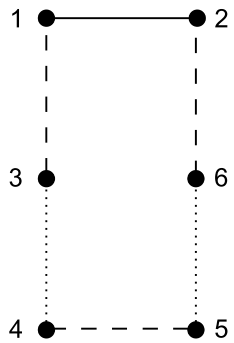

Figure A.3: CPR graph of $\langle(1,2),(1,3)(4,5)(2,6),(3,4)(5,6)\rangle$

The two CPR graphs have an axis of symmetry and hence, by lemma 2.1.6, $\langle\rho_0,\rho_1,\rho_2\rangle$ has each time a normal subgroup, different from $Alt(6)$. Thus for these two cases, $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$.

(4.8d): $\rho_0 = (1,2)$ and $\rho_2 = (1,2)(3,4)(5,6)$

None of the cases is done in section 4.3.2. So we do the three cases here. First we show that if ρ_1 is equal to $(1,3)(2,5)$ or to $(1,3)(4,5)(2,6)$, then $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$. In order to do this, we use once again the CPR graphs and lemma 2.1.6. The CPR graphs of these two cases are shown in figure A.4 and A.5.

As both the graph A.4 and the graph A.5 present a symmetry, we get a normal subgroup, different from $Alt(6)$ and hence $\langle\rho_0,\rho_1,\rho_2\rangle$ is not isomorphic to $Sym(6)$.

Let us now look at the case $\rho_1 = (1,3)(4,5)$. The group

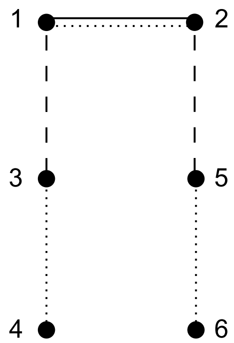

Figure A.4: CPR graph of $\langle(1,2),(1,3)(2,5),(1,2)(3,4)(5,6)\rangle$

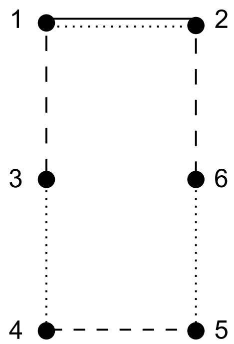

Figure A.5: CPR graph of $\langle(1,2),(1,3)(4,5)(2,6),(1,2)(3,4)(5,6)\rangle$

$\langle(1,2),(1,3)(4,5),(1,2)(3,4)(5,6)\rangle$ is a subgroup of $Sym(6)$ containing the transposition $(1,2)$. Moreover

$$\rho_1\rho_0\rho_2 = (1,4,6,5,3),$$

and hence the cyclic group $\langle\rho_1,\rho_0,\rho_2\rangle$ is transitive on the set $\{1,3,4,5,6\}$, while keeping 2 fixed. By lemma 1.2.4, ρ_0,ρ_1 and ρ_2 generate $Sym(6)$. It remains to show that they satisfy (IP). We use again lemma 3.2.1. We just have to prove that $\Gamma_2\cap\Gamma_0 = \langle\rho_1\rangle$. It is obvious that $\langle\rho_1\rangle$ is included in $\Gamma_2\cap\Gamma_0$. Every permutation of the group Γ_2 fixes the element 6. However the only non-trivial permutation in Γ_0 that fixes 6 is ρ_1. In fact $\rho_1\rho_2 = (1,4,6,5,3,2)$ and $\rho_2\rho_1 = (1,2,3,5,6,4)$. Powers of $\rho_1\rho_2$ or of $\rho_2\rho_1$ do not fix any element (except if the power is a multiple of 6). Thus non-trivial permutations in Γ_0, that fix an element, are either ρ_1 or are of the form $(\rho_1\rho_2)^m\rho_1$ or of the form $(\rho_2\rho_1)^m\rho_2$, with $1\le m\le 6$. As 6 is already fixed by ρ_1, only a permutation of the last form may fix 6. The permutation $(\rho_2\rho_1)^m\rho_2$ fixes 6 if and only if $(\rho_2\rho_1)^m$ maps 6 onto 5, and thus m has to be equal to 5. However $(\rho_2\rho_1)^5\rho_2 = \rho_1$. Hence $\Gamma_2\cap\Gamma_0 = \langle\rho_1\rangle$. Thus

$Sym(6) \cong \langle (1,2),(1,3)(4,5),(1,2)(3,4)(5,6) \rangle$ is the automorphism group of a polyhedron. Its Schläfli type is as given in section 4.3.2.

A.2 Known Results about Polyhedra Associated to Symmetric and Alternating Groups

In the atlas of abstract regular polytopes for small groups, [16], the work we try to do in this Master's thesis is done, by computer, for small groups. As the symmetric and alternating groups increase very fast, we only know the number of polyhedra for $Sym(n)$ and for $Alt(n)$ with $1 \leq n \leq 9$. They are shown in table A.1. This table shows for each symmetric and alternating group the automorphism group, the order of the group, the number of involutions contained in the group and the number of polyhedra on which the group acts as automorphism group.

G	$Aut(G)$	$\|G\|$	$\sharp$ involutions	$\sharp$ Polyhedra
$Sym(n), n \leq 3$	$Sym(n)$	≤ 6	≤ 3	0
$Alt(n), n \leq 4$	$Sym(n)$	≤ 12	≤ 3	0
$Sym(4)$	$Sym(4)$	24	9	2
$Alt(5)$	$Sym(5)$	60	15	2
$Sym(5)$	$Sym(5)$	120	25	4
$Alt(6)$	$P\Gamma L(2,9)$	360	45	0
$Sym(6)$	$P\Gamma L(2,9)$	720	75	2
$Alt(7)$	$Sym(7)$	2520	105	0
$Sym(7)$	$Sym(7)$	5040	231	35
$Alt(8)$	$Sym(8)$	20160	315	0
$Sym(8)$	$Sym(8)$	40320	763	68
$Alt(9)$	$Sym(9)$	181440	1323	41
$Sym(9)$	$Sym(9)$	362880	2619	129

Table A.1: Number of polyhedra on which $Sym(n)$ and $Alt(n)$ act as automorphism group.

A.3 Some Results on the Number of Commuting Involutions in $Sym(n)$ and $Alt(n)$

Lemma 4.2.1 and lemma 5.2.1 give a formula to compute the number of *ordered* pairs $[\rho_0, \rho_2]$ of commuting involutions in $Sym(n)$ and in $Alt(n)$ up to conjugacy. Except for $n = 6$, up to conjugacy corresponds to up to isomorphism and hence the formula gives the number of ordered pairs of commuting involutions in $Sym(n)$ and $Alt(n)$ up to isomorphism for $n \neq 6$. Results of these formulas are shown in table A.2.

Theorem 4.2.2 and theorem 5.2.2 give a formula to compute the number of *unordered* pairs $\{\rho_0, \rho_2\}$ of commuting involutions in $Sym(n)$ and $Alt(n)$, up to isomorphism, respectively up to conjugacy for $n = 6$. Some results of these formulas are given in table A.3.

n	$[\rho_0, \rho_2]$, with $\rho_0, \rho_2 \in Sym(n)$	$[\rho_0, \rho_2]$, with $\rho_0, \rho_2 \in Alt(n)$
1	0	0
2	0	0
3	0	0
4	4	1
5	4	1
6	14	2
7	14	2
8	33	9
9	33	9
10	64	13
11	64	13
12	111	30
13	111	30
14	178	40
15	178	40
16	270	72
17	270	72
18	392	92
19	392	92
20	550	145
30	2114	518
40	5725	1465
50	12664	3148

Table A.2: Number of ordered pairs of commuting involutions in $Sym(n)$ and $Alt(n)$, up to conjugacy.

n	$\{\rho_0, \rho_2\}$, with $\rho_0, \rho_2 \in Sym(n)$	$\{\rho_0, \rho_2\}$, with $\rho_0, \rho_2 \in Alt(n)$
1	0	0
2	0	0
3	0	0
4	3	1
5	3	1
6	9	2
7	9	2
8	21	7
9	21	7
10	39	10
11	39	10
12	67	21
13	67	21
14	105	28
15	105	28
16	158	48
17	158	48
18	226	61
19	226	61
20	315	93
30	1169	315
40	3105	855
50	6774	1795

Table A.3: Number of unordered pairs of commuting involutions in $Sym(n)$ and $Alt(n)$, up to conjugacy.

Bibliography

[1] W. W. R. Ball and H. S. M. Coxeter.
Mathematical recreations and essays.
St. Martin's Press Inc., New York, eleventh edition, 1956.
Cited on page 57.

[2] D. Bonheure, F. Buekenhout, and D. Leemans.
On the Petrials of thin rank 3 geometries.
J. Geom., 71(1-2):19–25, 2001.
Cited on pages 1 and 4.

[3] F. Buekenhout, editor.
Handbook of incidence geometry.
North-Holland, Amsterdam, 1995.
Buildings and foundations.
Cited on pages 1 and 4.

[4] W. Burnside.
Theory of groups of finite order.
Dover Publications Inc., New York, 1955.
2d ed.
Cited on pages 3 and 6.

[5] P. J. Cameron.
Permutation groups, volume 45 of *London Mathematical Society Student Texts*.
Cambridge University Press, Cambridge, 1999.
Cited on pages 3 and 6.

[6] M. E. Carrancho Fernandez and D. Leemans.
Abstract regular polytopes and symmetric groups.
in preparation.
Cited on page 70.

[7] M. Conder, P. Potočnik, and J. Širáň.
Regular hypermaps over projective linear groups.
J. Aust. Math. Soc., 85(2):155–175, 2008.
Cited on pages 1 and 4.

[8] R. L. Graham, M. Grötschel, and L. Lovász, editors.
Handbook of combinatorics. Vol. 1, 2.
Elsevier Science B.V., Amsterdam, 1995.
Cited on page 57.

[9] M. I. Hartley.
The atlas of small regular polytopes.
Periodoca Math. Hungar. (Special volume on discrete geometry), 2006, http://www.abstract-polytopes.com/atlas.
Cited on pages 2, 4, and 13.

[10] B. Huppert.
Endliche Gruppen. I.
Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.
Cited on pages 3, 6, and 18.

[11] A. Kiefer and D. Leemans.
On the number of abstract regular polytopes whose automorphism group is a suzuki simple group Sz(q).
Journal of Combinatorial Theory, Series A.
To appear. Published online doi:10.1016/j.jcta.2010.01.001.
Cited on pages 2, 4, 5, and 39.

[12] D. Leemans.
An atlas of regular thin geometries for small groups.
Math. Comp., 68(228):1631–1647, 1999.
Cited on pages 1 and 4.

[13] D. Leemans.
The Suzuki simple groups Sz(q) seen as automorphism groups of some geometric structures.
Havard Number Theory seminar, Octobre 2005.
Cited on pages 2 and 4.

[14] D. Leemans and E. Schulte.
Groups of type $L_2(q)$ acting on polytopes.
Adv. Geom., 7(4):529–539, 2007.
Cited on pages 2 and 4.

[15] D. Leemans and E. Schulte.
Polytopes with groups of type $PGL_2(q)$.
Ars Math. Contemp., 2(2):163–171, 2009.
Cited on pages 2 and 4.

[16] D. Leemans and L. Vauthier.
An atlas of abstract regular polytopes for small groups.
Aeq. Math., 72(3):313–320, 2006,
http://cso.ulb.ac.be/~dleemans/polytopes/.
Cited on pages 1, 2, 3, 4, 5, 6, 28, 33, 65, and 89.

[17] P. McMullen and E. Schulte.
Abstract regular polytopes, volume 92 of *Encyclopedia of Mathematics and its Applications*.
Cambridge University Press, Cambridge, 2002.
Cited on pages 1, 3, 4, 6, 7, 9, 10, 12, 13, 14, 15, 16, 26, and 30.

[18] D. Pellicer.
Gráficas CPR y Politopos Abstractos Regulares.
PhD thesis, Universidad Nacional Autónoma de México, 2007.
Cited on pages 3, 6, 23, 27, and 28.

[19] D. Pellicer.
CPR graphs and regular polytopes.
European J. Combin., 29(1):59–71, 2008.
Cited on pages 3, 6, 13, 23, 25, 27, 28, and 29.

[20] J. J. Rotman.
The theory of groups. An introduction.
Allyn and Bacon Inc., Boston, Mass., 1965.
Cited on pages 2, 3, 5, 6, 18, 23, and 41.

[21] E. Schulte and A. I. Weiss.
Problems on polytopes, their groups, and realizations.
Period. Math. Hungar., 53(1-2):231–255, 2006.
Cited on pages 2 and 5.

[22] D. Sjerve and M. Cherkassoff.
On groups generated by three involutions, two of which commute.
In *The Hilton Symposium 1993 (Montreal, PQ)*, volume 6 of *CRM Proc. Lecture Notes*, pages 169–185. Amer. Math. Soc., Providence, RI, 1994.
Cited on pages 30, 34, 35, 36, and 70.

[23] M. Suzuki.
Group theory. I, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*.
Springer-Verlag, Berlin, 1982.
Translated from the Japanese by the author.
Cited on pages 3, 6, 17, 18, 19, 20, and 45.

[24] M. Suzuki.
Group theory. II, volume 248 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*.
Springer-Verlag, New York, 1986.
Translated from the Japanese.
Not cited.

[25] J. Tits.
Généralisations des groupes projectifs basées sur leurs propriétés de transitivité.
Acad. Roy. Belgique. Cl. Sci. Mém. Coll. in 8°, 27(2):115, 1952.
Cited on page 20.

[26] H. van Maldeghem.
Generalized polygons, volume 93 of *Monographs in Mathematics*.
Birkhäuser Verlag, Basel, 1998.
Cited on pages 55, 56, and 59.

[27] L. Vauthier.
Construction algorithmique de polytopes réguliers abstraits, 2005.
Master's Thesis. Université Libre de Bruxelles.
Cited on pages 1 and 4.

[28] R. A. Wilson.
The finite simple groups, volume 251 of *Graduate Texts in Mathematics*.
Springer-Verlag London Ltd., London, 2009.
Cited on pages 3, 6, 17, 18, 19, 20, and 21.