

COLOUR-PERMUTING AUTOMORPHISMS OF CAYLEY GRAPHS

SHIRIN ALIMIRZAEI

**Master of Science, Institute for Advanced Studies in Basic Sciences,
Zanjan, Iran**

A thesis submitted
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in

MATHEMATICS

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

© Shirin Alimirzaei, 2026

COLOUR-PERMUTING AUTOMORPHISMS OF CAYLEY GRAPHS

SHIRIN ALIMIRZAEI

Date of Defence: July 10, 2026

Dr. Dave Morris	Professor	Ph.D.
Thesis Supervisor		

Dr. Andrew Fiori	Associate Professor	Ph.D.
Thesis Examination Committee Member		

Dr. Habiba Kadiri	Associate Professor	Ph.D.
Thesis Examination Committee Member		

Dr. Wendy Osborn	Associate Professor	Ph.D.
Chair, Thesis Examination Committee		

Dedication

I dedicate this thesis to my mother, who has believed in me at every step of my life.

To me, she is one of the strongest women in the world. For many people, being a strong woman may mean having a position, education, or the power to encourage others. But my mother showed me a deeper kind of strength. Even without knowing much about the world outside her home, she raised me to be a girl who could pursue her goals without giving up. She taught me that no matter what happens, I must
continue.

She sacrificed so much of her own life for us, with love, patience, and selflessness, so that we could grow and succeed. I am speechless when I think about everything she has endured and everything she has done for us. I know that I could not have
survived in her situation with the same grace and strength.

This dedication is only a small way to say: Mom, in every single step of my life, you have been with me. You are the person who taught me patience, resilience, and courage. Without the patience and resilience she taught me, I could not have continued through the most difficult moments of graduate study, especially when my
path felt heavier than others could see.

Thank you, Mom, for being my strong mother, my support, and my inspiration. I also dedicate this thesis to all of my family members who supported me during my
studies. I love you all.

Abstract

A Cayley graph is a certain graph constructed from a group and a generating set. It has a natural edge-colouring that specifies the generators corresponding to each edge. An automorphism of a Cayley graph is *colour-preserving* if it preserves each colour class of edges, and *colour-permuting* if it permutes the colour classes. A Cayley graph is called *CCA* if every colour-preserving automorphism is affine, and *strongly CCA* if every colour-permuting automorphism is affine. The main goal of this thesis is to study colour-preserving automorphisms and colour-permuting automorphisms of Cayley graphs, with particular emphasis on abelian groups and complete Cayley graphs.

For connected Cayley graphs on abelian groups, we prove that non-affine behaviour can occur only in the presence of a specific configuration of elements of order 4 in the connection set. Using local permutations induced by colour-permuting automorphisms, we obtain a complete characterization of connected abelian Cayley graphs that are CCA, and show that they are strongly CCA. Specifically, for a connected Cayley graph $\text{Cay}(G; S)$ on an abelian group G , the graph is strongly CCA if and only if

$$|G : \langle \{2s\} \cup \{t \in S \mid 2t \neq 2s\} \rangle| \leq 2$$

for every element $s \in S$ of order 4. As a consequence, we obtain a complete classification of non-CCA connected two-generator abelian Cayley graphs.

We also study graphical regular representations (GRRs), Cayley indices, and normal Cayley graphs. We give a proof of the known fact that elementary abelian 2-groups admit a GRR exactly when their rank is not 2, 3, or 4. We also verify the

Cayley indices of all finite groups and correct some previously published connection sets for certain generalized dicyclic groups. Using these results, we obtain an alternative proof of the classification of finite groups that admit a normal Cayley graph.

Finally, we prove that the complete Cayley graph K_G is strongly CCA unless $G \cong Q_8 \times B$, where Q_8 is the quaternion group of order 8, and B is an abelian group of exponent 2. We also prove that every colour-permuting automorphism of a complete Cayley graph is the composition of a group automorphism and a colour-preserving automorphism.

Acknowledgments

I would like to thank my supervisor, Professor Dave Witte Morris, for their guidance and support throughout this research.

I would also like to thank the members of the Department of Mathematics and Computer Science at the University of Lethbridge for their support during my studies.

Finally, I would like to thank my family and friends for their patience and support.

Contents

Dedication	iii
Abstract	iv
Acknowledgments	vi
List of Tables	ix
List of Figures	x
1 Introduction	1
1.1 Notation	2
1.2 Main Results On Abelian Groups	3
1.3 Main Results On GRR, MRR, and Normal	6
1.4 CCA and strongly CCA characterization	12
1.5 Proofs	15
1.5A Ideas of the proofs in the abelian case	15
1.5B Ideas of the proofs for complete Cayley graphs	18
2 Preliminaries	20
2.1 Preliminaries in Group Theory	20
2.2 Affine maps	24
2.3 Preliminaries on Cayley graphs	30
2.4 Preliminaries on colour-permuting automorphisms	31
2.5 Preliminaries on the permutation of the connection set	33
3 Literature Review	49
3.1 Automorphisms of Cayley Graphs	49
3.2 Graphical Regular Representations (GRRs)	55
3.3 The CCA Problem	60
4 Abelian groups	65
5 Finite groups that do not have a GRR	74
5.1 Elementary abelian 2-groups that have a GRR	76
5.2 Infinite families of groups that do not have a GRR	81
5.3 Groups given by generators and relations	82
5.3A The group H_1	82

5.3B	The group H_2	92
5.3C	The group H_3	94
5.3D	The group H_4	97
6	Cayley index of every finite group	100
7	Finite groups that do not have a normal Cayley graph	109
7.1	Preliminaries on normal Cayley graphs	110
7.2	Proof of Theorem 7.0.1	110
8	Colour-preserving automorphisms of complete Cayley graphs	112
8.1	Colour-preserving automorphisms of $\text{Cay}(G; G \setminus \{1\})$	113
8.2	Complete graphs that are not strongly CCA	121
8.3	Colour-permuting automorphisms of $\text{Cay}(G; G \setminus \{1\})$	125
	Bibliography	132
A	Computer programs	135
A.1	basic.sage	135
A.2	elementaryabelian.sage	138
A.3	exceptional13groups.sage	139
A.4	smalldicyclic.sage	144
A.5	table5.3.sage	146
A.6	table5.6.sage	147
A.7	table5.5elementaryabelian.sage	152
A.8	table5.5Hamiltonian2-group.sage	155
A.9	table5.5exceptionaldicyclic.sage	156
A.10	Z4xZ2.sage	157
A.11	table6.1.sage	158

List of Tables

1.1	Cayley indices of all finite groups	10
6.1	Order, Cayley index, and MRR connection set for each of the 13 groups in Theorem 5.0.1	101
6.2	Nonabelian generalized dicyclic groups for which no Cayley graph of index 2 was found.	103
6.3	Incorrect connection set in Table 4 of [28]	104
6.4	Correct connection sets yielding Cayley index 2	104
6.5	Cayley indices of all finite groups with connection sets for an MRR .	107
6.6	Corrected version of [28, Table 4]. The connection sets for $\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$ and $\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$ have been corrected. Some rows do not provide a connection set, because G has the same Cayley index as $G \times \mathbb{Z}_2$ unless G is $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_3^2$ [28, Corollary 4.5]. . . .	108
7.1	Connection set for a normal Cayley graph	111

List of Figures

3.1	Petersen graph	50
3.2	$J(4, 2)$	51
3.3	$\text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1, 0), \pm(1, 1)\})$	55
3.4	$\text{Cay}(\mathbb{Z}_4; \{\pm 1\})$	61
3.5	$\text{Cay}(D_4; \{r, s\})$	61
3.6	$\text{Cay}(S_3; \{(1\ 3), (1\ 2)\})$	62
5.1	The graph $\Gamma[S_1]$ with vertex set S_1 and edges $E = \{e_i e_j : e_i + e_j \in S_2 \cup S_3\}$	79
5.2	$\Gamma[S]$: The black vertex adjacent to e_i and e_j is $e_i + e_j$	81

Chapter 1

Introduction

A Cayley graph is a certain graph constructed from a group and a generating set, and it inherits a natural edge-colouring from the generators. (See Definitions 2.3.3 and 2.4.1.) Automorphisms of Cayley graphs that preserve this colouring reflect algebraic properties of the underlying group and play an important role in the study of graph symmetries. In particular, an automorphism of a Cayley graph is called *colour-preserving* if it preserves each colour class induced by the connection set, and *colour-permuting* if it permutes the colour classes.

A central problem in the theory of Cayley graphs is determining when every colour-preserving automorphism is induced by the algebraic structure of the group. A Cayley graph is called *CCA* if every colour-preserving automorphism is affine, that is, a composition of a left-translation and a group automorphism. Similarly, a Cayley graph is called *strongly CCA* if every colour-permuting automorphism is affine. These properties have been studied for many classes of groups, including abelian groups, generalized dihedral groups, generalized dicyclic groups, and groups of odd order.

The main goal of this thesis is to study colour-preserving automorphisms and colour-permuting automorphisms of Cayley graphs, with particular emphasis on connected abelian Cayley graphs (Chapter 4), complete Cayley graphs (Chapter 8), graphical regular representations (Chapter 5), Cayley indices (Chapter 6), and normal Cayley graphs (Chapter 7). One of the main results gives a complete characterization of connected abelian Cayley graphs that are CCA and shows that they are strongly

CCA. (See Theorem 1.2.3 for an overview, and Theorem 4.0.5 for the full proof.) Specifically, we show that non-affine behaviour occurs only in the presence of a specific configuration of elements of order 4 in the connection set. (See Theorems 1.2.1 and 4.0.1.)

We also study colour-permuting automorphisms of complete Cayley graphs. For a group G , let

$$K_G = \text{Cay}(G; G \setminus \{1\})$$

denote the complete Cayley graph on G . We prove that K_G is strongly CCA unless

$$G \cong Q_8 \times B,$$

where Q_8 is the quaternion group of order 8, and B is an abelian group of exponent 2. (See Theorems 1.4.1 and 8.0.1.) We further prove that every colour-permuting automorphism of K_G can be expressed as the composition of a group automorphism and a colour-preserving automorphism. (See Theorems 1.4.7 and 8.3.1.)

In addition, we investigate graphical regular representations, Cayley indices, and normal Cayley graphs. Using these results, we obtain an alternative proof of the classification of finite groups admitting a normal Cayley graph. (See Theorems 1.3.3 and 7.0.1.) The remaining sections of this introduction describe the main results of each chapter in more detail.

1.1 Notation

Notation 1.1.1. The following will hold for the remainder of the thesis:

- the identity element of the group G , will be denoted $\mathbf{1}$ or $\mathbf{1}_G$.
- The symbol S will denote an inverse-closed subset of $G \setminus \{\mathbf{1}\}$; that is, $S = S^{-1}$.
- The notation $\text{Cay}(G; S)$ will denote the simple undirected Cayley graph of the

group G with connection set S . (See Definition 2.3.3.)

Throughout this thesis, we study automorphisms of Cayley graphs that preserve the natural edge-colouring induced by the generating set.

Recall that a function $\varphi : G \rightarrow G$ is called *affine* if it is the composition of an automorphism of G with a left translation by an element of G (see Definition 2.2.2).

An automorphism of $\text{Cay}(G; S)$ is

- *colour-preserving* if it preserves each colour class, and
- *colour-permuting* if it permutes the colour classes.

A Cayley graph is said to be *CCA* if every colour-preserving automorphism is affine, and *strongly CCA* if every colour-permuting automorphism is affine. (See Section 2.4.) Understanding when a Cayley graph is CCA or strongly CCA is a central theme of this thesis.

1.2 Main Results On Abelian Groups

Throughout this section, all groups are abelian, and we use additive notation. Thus, the group operation is written as addition, the identity element is denoted by 0, and the inverse of s is denoted by $-s$. In particular, $2s = s + s$ for every $s \in G$. We also write $|g|$ for the order of an element $g \in G$.

Abelian groups provide a tractable setting for studying colour-preserving automorphisms and colour-permuting automorphisms of Cayley graphs. Because the group operation is commutative, one can compare the images of $g + s + t$ obtained by moving first along s and then t , or first along t and then s . This leads to strong restrictions on the local permutations induced by an automorphism.

Let φ be a colour-permuting automorphism of $\text{Cay}(G; S)$. For each vertex $g \in G$, φ induces a permutation π_g^φ of the connection set S , describing how the colours are

permuted locally at g . The formal definition of π_g^φ and its basic properties are given in Definition 2.5.1 and Lemma 2.5.2.

Our first structural result shows that if these local permutations are not constant from vertex to vertex, then this can occur only in a very restricted situation: there exist $s, t \in S$ such that

$$2s = 2t \quad \text{and} \quad |s| = |t| = 4.$$

Thus any obstruction to affine behaviour is forced by a specific configuration of elements of order 4 in the connection set.

Theorem 1.2.1 (see Theorem 4.0.1). *Assume G is abelian, φ is a colour-permuting automorphism of $\text{Cay}(G; S)$, $g \in G$, and $s, t \in S$. If $\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s)$, then*

$$\pi_{g+t}^\varphi(s) = -\pi_g^\varphi(s), \quad \pi_{g+s}^\varphi(t) = -\pi_g^\varphi(t),$$

and $t \notin \langle s \rangle$. Moreover,

$$2s = 2t \quad \text{and} \quad |s| = |t| = 4.$$

Theorem 1.2.1 shows that non-affine behaviour can occur only in the presence of elements of order 4, and even then only in a very restricted configuration.

To describe this obstruction more precisely, we introduce the following notation.

Definition 1.2.2. Let G be an abelian group and $S \subseteq G$. For $c \in G$, define

$$T(S, c) := \{c\} \cup \{t \in S \mid 2t \neq c\}.$$

Using this construction, we obtain a complete characterization of when a connected abelian Cayley graph is CCA (equivalently, strongly CCA).

Theorem 1.2.3 (Theorem 4.0.5). *Assume $\text{Cay}(G; S)$ is connected and G is abelian. Then the following are equivalent:*

1. $\text{Cay}(G; S)$ is strongly CCA;
2. $\text{Cay}(G; S)$ is CCA;
3. $|G : \langle T(S, 2s) \rangle| \leq 2$ for every $s \in S$ of order 4.

Theorem 1.2.3 shows that, for connected abelian Cayley graphs, the CCA property is governed entirely by a simple index condition determined by elements of order 4.

In §1.5A of this introduction we explain some of the main ideas behind the proof.

As an application, we obtain a sharp classification in the two-generator setting.

Corollary 1.2.4 (see Corollary 4.0.7). *Let G be an abelian group generated by two elements a and b . Then the Cayley graph*

$$\Gamma = \text{Cay}(G; \{\pm a, \pm b\})$$

is not CCA if and only if

$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \quad \text{and} \quad |\bar{a}| = |\bar{b}| = 4.$$

This provides a sharp and explicit description of the only obstruction in the two-generator abelian case.

Remark 1.2.5. Up to isomorphism, this yields a unique example. Indeed, by Corollary 4.0.7, the only possible group is $\mathbb{Z}_4 \times \mathbb{Z}_2$. The elements of order 4 in this group are $\{\pm(1, 0), \pm(1, 1)\}$ which form exactly two inverse pairs. Therefore, up to interchanging a and b and replacing either generator by its inverse, the unique connection set of the form $\{\pm a, \pm b\}$ with $|a| = |b| = 4$ is $\{\pm(1, 0), \pm(1, 1)\}$.

1.3 Main Results On GRR, MRR, and Normal

We now turn to several related notions that concern the full automorphism group of a Cayley graph. In particular, we study GRRs, MRRs, and normal Cayley graphs. These notions provide different ways of measuring how close a Cayley graph is to having the smallest possible automorphism group.

Understanding when Cayley graphs have these properties is closely related to the study of colour-preserving automorphisms and colour-permuting automorphisms discussed above.

Definition 1.3.1 (see Definition 3.2.2). A Cayley graph $\Gamma = \text{Cay}(G; S)$ is a *GRR* (*Graphical Regular Representation*) if every automorphism of Γ is a left translation by an element of G ; that is, $\text{Aut}(\Gamma) = L(G)$, where $L(G)$ denotes the group of all left translations by elements of G .

Godsil, Hetzel, Imrich, Nowitz, and Watkins showed that, apart from generalized dicyclic groups and abelian groups of exponent greater than 2, there are only thirteen additional finite groups that do not admit a GRR [14, pp. 222-223].

Theorem 1.3.2 (Godsil, Hetzel, Imrich, Nowitz, and Watkins; see Theorem 5.0.1). *The groups listed below are the only ones that are neither generalized dicyclic nor abelian with an exponent greater than 2, yet do not admit a GRR:*

- $\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4$;
- D_6, D_8, D_{10} , where D_n denotes the dihedral group of order n ;
- A_4 , the alternating group of degree 4;
- $H_1 = \langle a, b, c : a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle$;
- $H_2 = \langle a, b : a^8 = b^2 = 1, bab = a^5 \rangle$;
- $H_3 = \langle a, b, c : a^3 = b^3 = c^2 = 1, ab = ba, (ac)^2 = (bc)^2 = 1 \rangle$;

- $H_4 = \langle a, b, c : a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \rangle;$
- $Q_8 \times \mathbb{Z}_3$ and $Q_8 \times \mathbb{Z}_4$.

We briefly introduce the notion of Cayley index here; a formal definition is given in Definition 3.2.4. The Cayley index of a Cayley graph $\Gamma = \text{Cay}(G; S)$ is the ratio $|\text{Aut}(\Gamma)|/|L(G)|$, and the Cayley index $c(G)$ of a finite group G is the minimum of $c(\Gamma)$ over all Cayley graphs on G . A Cayley graph achieving this minimum is called a most rigid representation (MRR). In particular, a finite group G admits a GRR if and only if $c(G) = 1$.

In Corollary 6.0.2, we verify that none of these thirteen groups admits a GRR by computing its Cayley index and showing that $c(G) > 1$.

The full classification theorem of Godsil et al. is much deeper; rather than reproving it in full generality, we illustrate some of the methods involved by treating an important infinite family.

A key role is played by elementary abelian 2-groups. Imrich proved that such a group admits a GRR if and only if its rank is not 2, 3, or 4 [19, 20]. The construction for the case $n = 5$ was later corrected by Alspach, Hell, Hetzel, and Lim [22].

In Section 5.1, we give a complete proof of this characterization. We first show that the groups of ranks 2, 3, and 4 do not admit a GRR. (See Corollary 6.0.2.) We then verify computationally that GRRs exist for ranks 1, 5, 6, and 7. (See Theorem 5.1.4.) Finally, we prove that GRRs exist for all higher ranks $n \geq 8$. (See Theorem 5.1.5.)

This yields a full construction-based understanding of when an elementary abelian 2-group admits a GRR and illustrates the techniques used in the broader classification.

The main tool used in these constructions is a structural lemma that allows one to certify that a Cayley graph is a GRR by examining only the local structure around the identity element. (See Lemma 5.1.2.)

Specifically, if the induced subgraph on the neighbourhood of the identity element has no nontrivial automorphisms, then every automorphism of the Cayley graph fixing

the identity element must also be trivial. Since Cayley graphs are vertex-transitive, this forces the entire automorphism group to consist only of left translations, and hence the graph is a GRR.

Using an idea of Imrich [19], who constructed GRRs of $\mathbb{Z}_2^n$ by creating an asymmetric neighbourhood of a vertex, we reformulate this construction in terms of connection sets, using modern terminology and notation. Our formulation provides an algebraic description of Imrich’s graph-theoretic construction, expressed directly in the language of Cayley graphs. The proof proceeds by designing a generating set with carefully controlled combinatorial properties and showing that the induced subgraph on this set has no nontrivial symmetries. This reduces the problem of proving that a Cayley graph is a GRR to a purely local asymmetry argument.

Groups given by generators and relations are often difficult to interpret concretely. To make these groups more accessible, the end of Chapter 5 provides explicit descriptions of the groups H_1 , H_2 , H_3 , and H_4 . (See Sections 5.3A to 5.3D.)

The main outcome of Chapter 6 is a complete list of Cayley indices for all finite groups, summarized in Table 1.1; this table is a verification of the values reported in [28], together with the correction of two MRR connection sets for generalized dicyclic groups; see Remark 6.0.9.

The justification of Table 1.1 begins from the classical GRR classification: a finite group has Cayley index 1 unless it is abelian, generalized dicyclic, or one of the finitely many exceptional groups listed in Theorem 1.3.2. Thus the problem reduces to determining $c(G)$ for these three families.

For the exceptional groups, we compute $c(G)$ directly by explicit search: for each of the 13 groups in Theorem 1.3.2, a SageMath program produces a Cayley graph with the smallest automorphism group found, yielding the Cayley indices recorded in Table 1.1 (and, in particular, confirming that none of these 13 groups admits a GRR).

For abelian groups, we use the theorem of Imrich–Watkins [22, Thm. 2], which

implies that $c(G) \leq 2$ for every finite abelian group, except for seven explicitly listed groups. The remaining small cases (including the exceptional abelian groups) are verified computationally, and the elementary abelian 2-groups are handled separately in Chapter 5.

For generalized dicyclic groups, we separate the Hamiltonian 2-groups from the remaining cases. The Cayley indices for the Hamiltonian groups $Q_8 \times \mathbb{Z}_2^n$ follow from [28, Prop. 4.8]. For non-Hamiltonian generalized dicyclic groups of order $|G| > 96$, we invoke a theorem of Imrich–Watkins [22, Thm. 2(1b)] guaranteeing $c(G) = 2$. It therefore remains to treat only finitely many small generalized dicyclic groups; these are checked by computation, producing Cayley graphs of index 2 except for four explicit families, which have index 4 as recorded in Table 1.1.

During this verification we discovered two inaccuracies in [28, Table 4]: the connection sets listed there for $\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$ and $\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$ do not yield Cayley index 2. We give corrected MRR connection sets for both groups; for more details, see Remark 6.0.9.

One of the main structural results we obtain in Chapter 7 is the following classification of finite groups that admit a normal Cayley graph. This result was originally proved by Wang, Wang, and Xu [33]. Here we give an alternative proof that fits naturally into the framework of Cayley indices developed in Chapter 6.

Theorem 1.3.3 (see Theorem 7.0.1). *A finite group G has a normal Cayley graph if and only if*

$$G \not\cong \mathbb{Z}_4 \times \mathbb{Z}_2 \quad \text{and} \quad G \not\cong Q_8 \times \mathbb{Z}_2^r \text{ for any } r \geq 0.$$

The proof relies on the classification of Cayley indices established in Table 1.1. A Cayley graph is normal whenever its Cayley index is at most 2. Therefore, any group that does not admit a normal Cayley graph must have Cayley index greater than 2.

By the results of Table 1.1, the groups with Cayley index greater than 2 are very restricted. There is only one infinite family of such groups, namely the Hamiltonian

Group	Order	Cayley Index
Elementary abelian 2-groups		
$\mathbb{Z}_2$	2	1
$\mathbb{Z}_2^2$	4	2
$\mathbb{Z}_2^3$	8	6
$\mathbb{Z}_2^4$	16	8
$\mathbb{Z}_2^n, n \geq 5$	2^n	1
Other abelian groups		
$\mathbb{Z}_4 \times \mathbb{Z}_2$	8	6
$\mathbb{Z}_4^2$	16	4
$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	16	8
$\mathbb{Z}_3^2$	9	8
$\mathbb{Z}_3^3$	27	12
All other abelian groups		2
Hamiltonian 2-groups		
Q_8	8	16
$Q_8 \times \mathbb{Z}_2$	16	16
$Q_8 \times \mathbb{Z}_2^n, n \geq 2$	2^{n+3}	8
Other generalized dicyclic groups		
$\text{Dic}(\mathbb{Z}_6, 3)$	12	4
$\text{Dic}(\mathbb{Z}_8, 4)$	16	4
$\text{Dic}(\mathbb{Z}_{10}, 5)$	20	4
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$	16	4
All other generalized dicyclic groups		2
Exceptional groups		
D_6	6	2
D_8	8	2
D_{10}	10	2
A_4	12	2
$Q_8 \times \mathbb{Z}_3$	24	2
$Q_8 \times \mathbb{Z}_4$	32	2
H_1	16	2
H_2	16	2
H_3	18	2
H_4	27	2
Every finite group not listed above		1

Table 1.1: Cayley indices of all finite groups

2-groups

$$Q_8 \times \mathbb{Z}_2^r,$$

together with finitely many additional exceptional groups:

$$\begin{aligned} &\mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2^3, \quad \mathbb{Z}_2^4, \quad \mathbb{Z}_4^2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2^2, \quad \mathbb{Z}_3^2, \quad \mathbb{Z}_3^3, \\ &\text{Dic}(\mathbb{Z}_6, 3), \text{Dic}(\mathbb{Z}_8, 4), \text{Dic}(\mathbb{Z}_{10}, 5), \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1)). \end{aligned}$$

The finite exceptional groups are checked computationally, and each admits a normal Cayley graph except for $\mathbb{Z}_4 \times \mathbb{Z}_2$.

On the other hand, the infinite family $Q_8 \times \mathbb{Z}_2^r$ does not admit a normal Cayley graph. Indeed, inversion

$$\varphi(x) = x^{-1}$$

is a graph automorphism of every Cayley graph on these groups, but it fixes the identity and is not a group automorphism. Hence it is not affine, and so no Cayley graph on $Q_8 \times \mathbb{Z}_2^r$ can be normal.

Thus the only finite groups that do not admit a normal Cayley graph are $\mathbb{Z}_4 \times \mathbb{Z}_2$ and the Hamiltonian 2-groups $Q_8 \times \mathbb{Z}_2^r$.

This classification highlights the role of normal Cayley graphs as an intermediate notion of rigidity. GRRs represent the most rigid situation, in which the automorphism group consists only of translations, while non-normal Cayley graphs arise when additional symmetries are present.

The groups $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $Q_8 \times \mathbb{Z}_2^r$ emerge once again as exceptional cases. They appear not only in the study of GRRs and Cayley indices, but also in the analysis of normal Cayley graphs. In each setting, the inversion map

$$x \mapsto x^{-1}$$

acts as a non-affine graph automorphism and serves as a common source of additional symmetry. This recurring phenomenon links the results of Chapter 5, Chapter 6, and Chapter 7, and foreshadows their role in the study of colour-preserving automorphisms in later chapters.

1.4 Main Results on complete characterization of when a group admits a CCA or strongly CCA Cayley graph

Although many groups are CCA but not strongly CCA (the smallest example is the dihedral group of order 12 [18, Prop. 7.3]), this distinction behaves differently when one considers complete Cayley graphs (that is, the complete graph $\text{Cay}(G; G \setminus \{1\})$). In general, there exist groups G for which every connected Cayley graph is CCA, yet some connected Cayley graphs are not strongly CCA. However, our results show that this disappears when the complete Cayley graph is considered. More precisely, we prove that if a group admits even a single CCA Cayley graph, then its complete Cayley graph is automatically strongly CCA. Thus, for complete Cayley graphs, the CCA and strongly CCA properties coincide. This leads to the following equivalence theorem, which provides a complete characterization of when a group admits a CCA or strongly CCA Cayley graph.

Theorem 1.4.1 (see Theorem 8.0.1). *If G is a (finite or infinite) group, then the following are equivalent:*

1. G has a Cayley graph that is strongly CCA.
2. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is strongly CCA.
3. G has a Cayley graph that is CCA.
4. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is CCA.

5. G is not of the form $Q_8 \times B$, where Q_8 is the quaternion group of order 8, B is an abelian group of exponent 2.

Furthermore, if G is finite, then these are also equivalent to:

6. Either G has a Cayley graph that is normal, or $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

In the finite case, several implications in Theorem 1.4.1 follow from known classification results (see Note 1.4.5). In particular, results concerning GRRs and normal Cayley graphs play an essential role. However, the implication that passes from an arbitrary CCA Cayley graph to the complete Cayley graph requires new arguments and a careful analysis of colour-permuting automorphisms of complete Cayley graphs. For finitely generated infinite groups, a theorem of Leemann and de la Salle [24, Thm. 1] shows that every such group admits a normal Cayley graph (see Corollary 7.0.3). Consequently, all of the conditions in Theorem 1.4.1 hold automatically for these groups. This leads to the following corollary.

Corollary 1.4.2. *If G is an infinite group that has a finite generating set, then Conditions 1–6 in the statement of Theorem 1.4.1 are all true.*

For finitely generated groups, one is usually most interested in the Cayley graphs that come from finite generating sets, and we have the following standard definition:

Definition 1.4.3. A Cayley graph $\text{Cay}(G; S)$ is *locally finite* if S is finite.

The theorem of Leemann and de la Salle that was mentioned above provides a Cayley graph that is locally finite, in addition to being normal (see Corollary 7.0.3 again). Combining this with Theorem 1.4.1 yields the following result. (Note that the complete graph on an infinite group is never locally finite.)

Corollary 1.4.4. *If G is a (finite or infinite) group that has a finite generating set, then the following are equivalent:*

- 1'. G has a locally finite Cayley graph that is strongly CCA.
- 2. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is strongly CCA.
- 3'. G has a locally finite Cayley graph that is CCA.
- 4. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is CCA.
- 5. G is not of the form $Q_8 \times B$, where Q_8 is the quaternion group of order 8, B is an abelian group of exponent 2.
- 6'. Either G has a locally finite Cayley graph that is normal, or $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Note 1.4.5.

- 1. The following several implications of Theorem 1.4.1 are more-or-less obvious (see Lemma 8.0.2):

$$(6)$$

$$\Downarrow$$

$$(2) \Rightarrow (1) \Rightarrow (3) \Leftrightarrow (4) \Rightarrow (5)$$

- 2. The implication $(5 \Rightarrow 4)$ is also known (but it is not obvious). It was proved by D.P. Byrne, M.J. Donner, and T.Q. Sibley [6, cf. p. 324] for finite groups, and the general case was established by E. Dobson, A. Hujdurović, K. Kutnar, and J. Morris [9, Thm. 2.3].
- 3. For groups that are *finite*, the implication $(5 \Rightarrow 6)$ was established by C. Wang, D. Wang, and M. Xu [33]. The proof relies on the classification of finite groups that do not have a Graphical Regular Representation (GRR), which is a difficult theorem that was proved in a series of papers by several authors (see [14]).

Most of the implications in Theorem 1.4.1 for finite groups rely on previously established classification theorems. The principal new contribution in the finite setting is the passage from the existence of a CCA Cayley graph to the strongly CCA property

of the complete Cayley graph. For infinite groups that are not finitely generated, the argument requires additional work. In fact, we establish a stronger statement, namely that if G is not of the exceptional form $Q_8 \times B$ then the complete Cayley graph on G is strongly CCA (see Corollary 8.2.8). This result subsumes the key new implications in both the finite and infinite cases.

We also prove the following result (see Corollary 8.2.7), which was conjectured by Byrne, Donner, and Sibley in [6, cf. p. 332]. As a consequence of our proof of Theorem 1.4.7, this result shows that placing a natural restriction on the colour-preserving automorphisms of a Cayley graph can also restrict the colour-permuting automorphisms:

Proposition 1.4.6. *If every colour-preserving automorphism of $\text{Cay}(G; S)$ is a translation, then every colour-permuting automorphism of $\text{Cay}(G; S)$ is an affine map (i.e., $\text{Cay}(G; S)$ is strongly CCA).*

A second main result of Chapter 8, concerns colour-permuting automorphisms of complete Cayley graphs. Byrne–Donner–Sibley conjectured that every colour-permuting automorphism of a complete Cayley graph splits into a group automorphism and a colour-preserving automorphism; we prove this for all groups:

Theorem 1.4.7 (see Theorem 8.3.1). *If G is any group, then every colour-permuting automorphism of the complete graph $\text{Cay}(G; G \setminus \{1\})$ is the composition of a group automorphism and a colour-preserving graph automorphism.*

1.5 Proofs

1.5A Ideas of the proofs in the abelian case

Our analysis of CCA Cayley graphs and strongly CCA Cayley graphs on abelian groups is based on tracking how an automorphism acts on the coloured edges incident with each vertex.

To formalize this, let $\Gamma = \text{Cay}(G; S)$ and let $\varphi \in \text{Aut}(\Gamma)$. For each vertex $g \in G$, the automorphism φ induces a permutation

$$\pi_g^\varphi : S \rightarrow S$$

defined by the rule

$$\varphi(g + s) = \varphi(g) + \pi_g^\varphi(s) \quad (s \in S).$$

Thus π_g^φ records how φ permutes the colours of the edges incident with g .

Affine automorphisms act uniformly across the graph, so the maps π_g^φ are independent of the vertex g . Non-affine behaviour therefore manifests itself through variation in these local permutations.

The key observation is that such variation is highly constrained in the abelian setting. In fact, if the local permutations differ between two adjacent vertices, then strong algebraic restrictions must hold. This leads to the structural result stated in Theorem 1.2.1.

The basic properties of these local permutations are summarized in Lemma 1.5.1. In particular, Item 1 and item 2 translate the colour-preserving and colour-permuting conditions into simple constraints on the values $\pi_g^\varphi(s)$, and Item 3 shows that φ is affine exactly when the permutations π_g^φ do not depend on g .

Thus the central question becomes: *when can the local permutations vary from vertex to vertex?*

Lemma 1.5.1 (see Lemma 2.5.2). *Let $\Gamma = \text{Cay}(G; S)$ and let $\varphi \in \text{Aut}(\Gamma)$. For each $g \in G$, let π_g^φ be defined by*

$$\varphi(gs) = \varphi(g)\pi_g^\varphi(s).$$

The following rules will be used throughout the analysis:

1. φ is colour-preserving $\iff \pi_g^\varphi(s) \in \{s, s^{-1}\}$ for all $g \in G$ and $s \in S$.

2. φ is colour-permuting $\iff \pi_h^\varphi(s) \in \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\} \quad \forall g, h \in G, \forall s \in S$.
3. φ is affine $\iff \pi_g^\varphi(s)$ is independent of g for all $g \in G$.
4. π_g^φ is invariant along cosets of $\langle s \rangle$, meaning that $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$ for all $g \in G$, $s \in S$, and $k \in \mathbb{Z}$. Thus the image of s depends only on the coset $g\langle s \rangle$.
5. π_g^φ preserves the order of elements, so that $|\pi_g^\varphi(s)| = |s|$ for all $g \in G, s \in S$.

We repeatedly used these properties to translate global symmetry conditions into local algebraic constraints to prove Theorem 1.2.1. We are now going to explain the ideas of the proof of Theorem 1.2.3.

(1 $\Rightarrow$ 2). Assume that the Cayley graph $\text{Cay}(G; S)$ is strongly CCA. Then every colour-permuting automorphism of $\text{Cay}(G; S)$ is affine. Since every colour-preserving automorphism is, in particular, a colour-permuting automorphism, it follows that every colour-preserving automorphism is affine. Therefore $\text{Cay}(G; S)$ is CCA.

(2 $\Rightarrow$ 3). We prove the contrapositive. Suppose there exists $s \in S$ with $|s| = 4$ such that $|G : \langle T(S, 2s) \rangle| > 2$. Let $c = 2s$, so c has order 2. Define a map $\varphi_c^S : G \rightarrow G$ by translating elements of the coset $\langle T(S, c) \rangle$ by c , and fixing all other elements.

Since the coset $\langle T(S, c) \rangle$ has size less than $|G|/2$, the map φ_c^S fixes more than half of the elements of G , so it is not affine (see Lemma 2.2.5). One checks that φ_c^S is colour-preserving on $\text{Cay}(G; S)$. Thus $\text{Cay}(G; S)$ admits a colour-preserving automorphism that is not affine, so it is not CCA. This proves the contrapositive.

(3 $\Rightarrow$ 1). A key consequence of Theorem 1.2.1 is that if $\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s)$ for some $g \in G$ and $s, t \in S$, then $|s| = 4$ and $s \notin \langle T(S, 2s) \rangle$.

Suppose φ is a colour-permuting automorphism of $\text{Cay}(G; S)$. If φ were not affine, then for some $g \in G$ and $s, t \in S$ we would have

$$\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s).$$

By the observation above, this forces

$$s \notin \langle T(S, 2s) \rangle.$$

Hence, whenever $\langle T(S, 2s) \rangle = G$, such a discrepancy cannot occur. This is the essential idea behind the proof. The full argument shows that the same conclusion still holds under the weaker assumption $|G : \langle T(S, 2s) \rangle| \leq 2$. Therefore $\text{Cay}(G; S)$ is strongly CCA.

1.5B Ideas of the proofs for complete Cayley graphs

The analysis of complete Cayley graphs relies on the fact that every pair of vertices is adjacent. This provides much stronger constraints on automorphisms than in the general case, since every group element appears as a generator.

Let $\Gamma = \text{Cay}(G; G \setminus \{1\})$. As in the abelian case, we study automorphisms by tracking how they act on edges. However, in the complete setting, the situation simplifies significantly: every element of G appears as a colour, so the behaviour of an automorphism is determined by its action on the group.

The first key step is the classification of colour-preserving automorphisms. A result of Byrne, Donner, and Sibley [6, p. 324], extended to infinite groups by Leemann and de la Salle [24, Thm. 2], shows that any nontrivial colour-preserving automorphism that fixes the identity forces the group to have a very restricted structure: it must be either abelian or generalized dicyclic. Thus, except for these special cases, the group of colour-preserving automorphisms is extremely small.

This structural restriction allows us to control the CCA and strongly CCA properties. In particular, if G is not of the form $Q_8 \times B$, then the set of elements that are not fixed by any nontrivial colour-preserving automorphism generates the entire group. This forces all colour-permuting automorphisms to act uniformly, and hence to be affine. Therefore, the complete Cayley graph is strongly CCA.

On the other hand, when $G = Q_8 \times B$, there exist additional colour-preserving automorphisms coming from the quaternion structure, and these give rise to non-affine behaviour. This explains why these groups form the unique obstruction in the equivalence theorem.

The proof of Theorem 1.4.7 uses a different idea. Given a colour-permuting automorphism φ , one first reduces to the case $\varphi(\mathbf{1}) = \mathbf{1}$ by composing with a translation. If the graph is strongly CCA, then φ is already a group automorphism. Otherwise, the group must be of the form $Q_8 \times B$.

In this case, one analyzes the action of φ on the central subgroup of elements of order 2, showing that φ behaves like a group automorphism on this part. One then reconstructs an actual group automorphism β that agrees with φ on both the quaternion component and the central subgroup. The remaining map $\psi = \beta^{-1}\varphi$ is then shown to be colour-preserving.

Thus every colour-permuting automorphism decomposes as

$$\varphi = \beta \circ \psi,$$

where $\beta \in \text{Aut}(G)$ and ψ is colour-preserving. This shows that all colour-permuting automorphisms are obtained by combining group structure with the limited set of colour-preserving symmetries.

Chapter 2

Preliminaries

This chapter presents basic definitions and results that will be used in the following chapters.

Assumption 2.0.1. Graphs in this thesis are simple and undirected, but they may be infinite.

Remark 2.0.2. In the statements of our main results, it does not matter whether graphs are allowed to have loops. This is because all of our main results concern automorphisms of Cayley graphs, and adding a loop to every vertex of a graph does not affect its automorphism group. (For a Cayley graph $\text{Cay}(G; S)$, adding a loop at all vertices is achieved by replacing S with $S \cup \{\mathbf{1}\}$.)

2.1 Preliminaries in Group Theory

Contents of this section are based on [8, 31]. In this thesis, G always denotes a group (which may be infinite) and $\mathbf{1}$ is the identity element of G .

Theorem 2.1.1 (Orbit-Stabilizer Theorem, [8, Theorem 1.4]). *Let G be a group acting on a set X , and let $x \in X$. Then*

$$|Gx| = [G : \text{Stab}_G(x)],$$

where $Gx = \{g \cdot x \mid g \in G\}$ is the orbit of x , and

$$\text{Stab}_G(x) := G_x = \{g \in G \mid g \cdot x = x\}$$

is the stabilizer of x in G .

Definition 2.1.2 ([31, Definition, p. 42]). An *elementary abelian 2-group* is an abelian group G such that:

- G is abelian, i.e., for all $x, y \in G$, $xy = yx$, and
- every non-identity element in G has order 2, i.e., for all $g \in G$, we have $g^2 = \mathbf{1}$.

Definition 2.1.3 (cf. [18, Definition 2.6]). A group G is *generalized dicyclic* if it has an abelian subgroup A of index 2, an element z of order 2 that is in A , and an element $q \notin A$, such that $q^2 = z$, and every element of A is inverted by q (in the action by conjugation). We write

$$\text{Dic}(A, z) = \langle A, q \mid q^2 = z, q^{-1}aq = a^{-1} \forall a \in A \rangle.$$

Notation 2.1.4 ([11, §1.5, p. 36]). We let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8, where -1 is central, $i^2 = j^2 = k^2 = -1$, and $ij = -ji = k$.

Definition 2.1.5 (cf. [39]). A group G is *Hamiltonian* if it is nonabelian, and every subgroup of G is normal. It can be shown that G is Hamiltonian if and only if it is isomorphic to $Q_8 \times A \times B$, for some abelian groups A and B , such that every element of A has odd order, and every element of B has order 1 or 2.

Lemma 2.1.6. *If H is a proper subgroup of a group G , then $\langle G \setminus H \rangle = G$, where $G \setminus H = \{g \in G \mid g \notin H\}$.*

Proof. Since $G \setminus H$ is obviously contained in $\langle G \setminus H \rangle$, it suffices to show that $H \subseteq \langle G \setminus H \rangle$. Since H is proper, there is some $g \in G \setminus H$. Then, for any $h \in H$, we have

$g^{-1}h \in G \setminus H$, so

$$h = g(g^{-1}h) \in (G \setminus H)(G \setminus H) \subseteq \langle G \setminus H \rangle. \quad \square$$

Lemma 2.1.7 (internal direct product [11, Theorem 9, p. 171]). *If H and K are normal subgroups of G , such that $HK = G$ and $H \cap K = \{1\}$, then G is isomorphic to the direct product of H and K , and we write $G = H \times K$.*

Lemma 2.1.8 ([11, Proposition 14, p. 94]). *Assume H and K are subgroups of G . The product HK is a subgroup of G if and only if $HK = KH$.*

Corollary 2.1.9 (cf. [11, Proposition 14, p. 94]). *Assume H and K are subgroups of G . If $G = HK$, then $G = KH$.*

The following definition can be generalized to allow any group in the place of $\mathbb{Z}_n$ (see [8, §2.5, p. 44]), but this special case is simpler, and suffices for our purposes.

Definition 2.1.10. Let H be a group, let $n \in \mathbb{Z}_{>0}$, and let $\varphi \in \text{Aut}(H)$ be an automorphism of H such that $\varphi^n = \text{id}$. Then the *semidirect product of H by the cyclic group of order n* , denoted by $H \rtimes_{\varphi} \mathbb{Z}_n$, is the group defined on the set

$$H \times \mathbb{Z}_n = \{(h, i) \mid h \in H, i \in \mathbb{Z}_n\}$$

with multiplication given by

$$(h, i)(h', j) = (h \cdot \varphi^i(h'), i + j),$$

for all $h, h' \in H$, and $i, j \in \mathbb{Z}_n$. Here, the action of $\mathbb{Z}_n$ on H is determined by powers of the automorphism φ , so that the generator $1 \in \mathbb{Z}_n$ acts as φ , and in general, $i \in \mathbb{Z}_n$ acts as φ^i .

Remark 2.1.11. The identity element of the group $H \rtimes_{\varphi} \mathbb{Z}_n$ is $(\mathbf{1}_H, 0)$, and the inverse of the element (h, i) is the element $(\varphi^{-i}(h^{-1}), -i)$.

Definition 2.1.12 ([11, pp. 23–26]). The *dihedral group* of order $2n$, denoted by D_{2n} , is the group of symmetries of a regular n -gon, consisting of rotations and reflections. This group can be generated by a clockwise rotation r about the origin through an angle of $2\pi/n$ radians, and a reflection s about a line of symmetry passing through a vertex. All rotations $(\mathbf{1}, r, r^2, \dots, r^{n-1})$ are orientation-preserving. Any reflection s is orientation-reversing. Then the elements of D_{2n} are

$$D_{2n} = \{\mathbf{1}, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

Additionally, the elements of D_{2n} satisfy the relations $r^n = \mathbf{1}$, $s^2 = \mathbf{1}$, and $srs = r^{-1}$. Thus, the dihedral group D_{2n} can be presented by generators and relations as:

$$D_{2n} = \langle r, s \mid r^n = s^2 = \mathbf{1}, srs = r^{-1} \rangle.$$

Proposition 2.1.13. $D_{2n} \cong \mathbb{Z}_n \rtimes_{\iota} \mathbb{Z}_2$, where $\iota \in \text{Aut}(\mathbb{Z}_n)$ is the inversion map defined by $\iota(x) = -x$.

Theorem 2.1.14 (Von Dyck's Theorem, [31, p. 346], or [26, Theorem 4.1.8]). Assume

- $G = \langle x_1, \dots, x_n \mid R_1, R_2, \dots, R_m \rangle$ is a group defined by generators and relations.
- $\hat{x}_1, \dots, \hat{x}_n$ are elements of a group H , and
- the relations $\hat{R}_1, \dots, \hat{R}_m$ are satisfied in H , where $\hat{R}_j$ is obtained by replacing the symbols $x_1, \dots, x_n$ in R_j with $\hat{x}_1, \dots, \hat{x}_n$.

Then there is a homomorphism $\varphi: G \rightarrow H$ such that $\varphi(x_i) = \hat{x}_i$ for all i .

Here is a useful consequence for finite groups:

Corollary 2.1.15 ([26, Theorem 4.1.11]). *Suppose*

- $G = \langle x_1, \dots, x_n \mid R_1, R_2, \dots, R_\ell \rangle$ is a group defined by generators and relations,
- $H = \langle \hat{x}_1, \dots, \hat{x}_n \rangle$ is a finite group that is generated by n elements, such that the relations $\hat{R}_1, \hat{R}_2, \dots, \hat{R}_\ell$ are satisfied, and
- $|G| \leq |H|$.

Then $G \cong H$.

2.2 Affine maps

Throughout this section, let G be a group.

Definition 2.2.1 (cf. [18, p. 190]). Let G be a group. For each $g \in G$, the *left translation* by g is the map

$$\ell_g: G \rightarrow G, \quad \ell_g(x) = gx \quad \text{for all } x \in G.$$

The set of all left translations, $L(G) = \{\ell_g \mid g \in G\}$, forms a group under function composition, isomorphic to G .

Definition 2.2.2 ([18, Definition 1.2]). A function $\varphi: G \rightarrow G$ is said to be *affine* if it is the composition of an automorphism of G with left translation by an element of G . This means $\varphi(x) = \alpha(gx)$, for some $\alpha \in \text{Aut}(G)$ and $g \in G$ (or, equivalently, that $\varphi(x) = h\alpha(x)$ for some $\alpha \in \text{Aut } G$ and $h \in G$).

In this thesis, affine maps are required to be bijections, but most authors do not have this restriction, because they allow α to be a homomorphism, rather than requiring it to be an automorphism. We use this more restrictive convention because all affine maps considered in this thesis arise in the study of automorphisms of Cayley graphs, and hence are bijections. Thus, allowing arbitrary homomorphisms would introduce maps that are not needed in our setting.

Lemma 2.2.3 ([15, 2.1. Lemma]). *Let $\varphi: G \rightarrow G$ be a bijection. Then the following are equivalent:*

1. φ is affine.
2. φ normalizes $L(G)$.
3. φ normalizes $R(G)$, where $R(G)$ is the group of right translations.

Proof. $1 \Rightarrow 2$. Suppose $\varphi = \ell_h \circ \alpha$ with $\alpha \in \text{Aut}(G)$, $h \in G$. Then $\varphi^{-1} = \alpha^{-1} \circ \ell_{h^{-1}}$.

For any $g \in G$:

$$\varphi \ell_g \varphi^{-1} = (\ell_h \alpha) \ell_g (\alpha^{-1} \ell_{h^{-1}}) = \ell_h (\alpha \ell_g \alpha^{-1}) \ell_{h^{-1}}.$$

Since $\alpha \ell_g \alpha^{-1} = \ell_{\alpha(g)}$ we have $((\alpha \ell_g \alpha^{-1})(x) = \alpha(g \alpha^{-1}(x)) = \alpha(g)x)$, so

$$\varphi \ell_g \varphi^{-1} = \ell_h \ell_{\alpha(g)} \ell_{h^{-1}} = \ell_{h \alpha(g) h^{-1}} \in L(G).$$

Thus $\varphi L(G) \varphi^{-1} \subseteq L(G)$. Since φ^{-1} is also affine, the inclusion is equality. So φ normalizes $L(G)$.

$1 \Rightarrow 3$. Again $\varphi = \ell_h \alpha$. For any $g \in G$:

$$\varphi r_g \varphi^{-1} = (\ell_h \alpha) r_g (\alpha^{-1} \ell_{h^{-1}}) = \ell_h (\alpha r_g \alpha^{-1}) \ell_{h^{-1}}.$$

Since $\alpha r_g \alpha^{-1} = r_{\alpha(g)}$ (as $(\alpha r_g \alpha^{-1})(x) = \alpha(\alpha^{-1}(x)g) = x\alpha(g)$), we get:

$$\varphi r_g \varphi^{-1} = \ell_h r_{\alpha(g)} \ell_{h^{-1}}.$$

Now compute action on $x \in G$:

$$\begin{aligned}
 (\ell_h r_{\alpha(g)} \ell_{h^{-1}})(x) &= \ell_h(r_{\alpha(g)}(h^{-1}x)) \\
 &= \ell_h((h^{-1}x)\alpha(g)) \\
 &= h(h^{-1}x)\alpha(g) \\
 &= x\alpha(g) \\
 &= r_{\alpha(g)}(x).
 \end{aligned}$$

So $\varphi r_g \varphi^{-1} = r_{\alpha(g)} \in R(G)$. Hence φ normalizes $R(G)$.

2 $\Rightarrow$ 1. Assume φ normalizes $L(G)$. Then for each $g \in G$, $\varphi \ell_g \varphi^{-1} = \ell_{f(g)}$ for some $f(g) \in G$. The map $f: G \rightarrow G$ is a bijection. Also:

$$\ell_{f(gh)} = \varphi \ell_{gh} \varphi^{-1} = \varphi \ell_g \ell_h \varphi^{-1} = (\varphi \ell_g \varphi^{-1})(\varphi \ell_h \varphi^{-1}) = \ell_{f(g)} \ell_{f(h)} = \ell_{f(g)f(h)},$$

so $f(gh) = f(g)f(h)$, hence $f \in \text{Aut}(G)$. The relation $\varphi \ell_g = \ell_{f(g)} \varphi$ applied to e gives:

$$\varphi(g) = \varphi(\ell_g(e)) = \ell_{f(g)}(\varphi(e)) = f(g)\varphi(e).$$

Let $h = \varphi(e)$. We can define $\alpha(g) = h^{-1}f(g)h$. Then $\varphi(g) = h\alpha(g) = \ell_h \circ \alpha$, so $\varphi = \ell_h \circ \alpha$ with $\alpha \in \text{Aut}(G)$, hence affine.

3 $\Rightarrow$ 1. Assume φ normalizes $R(G)$. Then for each $g \in G$, $\varphi r_g \varphi^{-1} = r_{f(g)}$ for some $f(g) \in G$, and $f \in \text{Aut}(G)$. The relation $\varphi r_g = r_{f(g)} \varphi$ applied to e gives:

$$\varphi(g) = \varphi(r_g(e)) = r_{f(g)}(\varphi(e)) = \varphi(e)f(g).$$

Let $k = \varphi(e)$. Then $\varphi(g) = kf(g) = \ell_k(f(g))$, so $\varphi = \ell_k \circ f$ with $f \in \text{Aut}(G)$, hence affine. $\square$

The equivalence (1 $\Leftrightarrow$ 3) of Lemma 2.2.3 can be expressed in the following well-

known equivalent form:

Corollary 2.2.4. *A bijection $\varphi: G \rightarrow G$ is affine if and only if for all $g \in G$, there exists $h \in G$, such that $\varphi(xg) = \varphi(x)h$ for all $x \in G$.*

Proof. ($\Rightarrow$). Assume φ is affine, so by Lemma 2.2.3(3), for every $g \in G$ we have $\varphi r_g \varphi^{-1} = r_h$ for some $h \in G$. Then

$$\varphi(xg) = \varphi(r_g(x)) = r_h \varphi(x) = \varphi(x)h.$$

($\Leftarrow$). Suppose for all $g \in G$, there exists $h \in G$ such that $\varphi(xg) = \varphi(x)h$ for all $x \in G$. It means $\varphi(r_g(x)) = r_h \varphi(x)$ so $\varphi r_g \varphi^{-1} = r_h$. Thus φ normalizes $R(G)$. By Lemma 2.2.3(1), φ is affine. $\square$

Lemma 2.2.5. *Assume $\varphi: G \rightarrow G$ fixes more than half of the elements of G , but is not the identity map. Then φ is not affine.*

Proof. Assume, for a contradiction, that φ is affine.

Let

$$F = \{x \in G \mid \varphi(x) = x\}.$$

By hypothesis, we have $|F| > |G|/2$.

Let h be an arbitrary element in F , so that $\varphi(h) = h$. Define the affine map $\psi: G \rightarrow G$ by

$$\psi(x) = h^{-1} \varphi(hx).$$

Then ψ fixes the identity element:

$$\psi(\mathbf{1}) = h^{-1} \varphi(h) = h^{-1}h = \mathbf{1},$$

and ψ has the same number of fixed points as φ . Indeed,

$$\psi(y) = y \iff h^{-1}\varphi(hy) = y \iff \varphi(hy) = hy,$$

so y is fixed by ψ if and only if hy is fixed by φ . Thus $|\text{Fix}(\psi)| = |\text{Fix}(\varphi)| > |G|/2$.

Also, ψ is affine, since $\psi = L_{h^{-1}} \circ \varphi \circ L_h$ and the set of affine maps is closed under composition.

Since ψ is affine, there exist $\alpha' \in \text{Aut}(G)$ and $g \in G$ such that

$$\psi(x) = g\alpha'(x) \quad \text{for all } x \in G.$$

Because $\psi(\mathbf{1}) = \mathbf{1}$, we have

$$\mathbf{1} = \psi(\mathbf{1}) = g\alpha'(\mathbf{1}) = g,$$

and therefore

$$\psi(x) = \alpha'(x) \quad \text{for all } x \in G.$$

Hence, $\psi \in \text{Aut}(G)$.

Next, note that $\text{Fix}(\psi)$ is a subgroup of G . Indeed, if $\psi(x) = x$ and $\psi(y) = y$, then

$$\psi(xy^{-1}) = \psi(x)\psi(y)^{-1} = xy^{-1}.$$

We already know that

$$|\text{Fix}(\psi)| > \frac{|G|}{2}.$$

In a finite group, the only subgroup whose order is strictly larger than $|G|/2$ is the whole group itself. Hence $\text{Fix}(\psi) = G$, so $\psi = \text{id}_G$.

Finally, since

$$\psi = L_{h^{-1}} \circ \varphi \circ L_h,$$

conjugating by L_h preserves the identity map, so $\varphi = \text{id}_G$, contradicting the hypothesis that φ is not the identity map.

Therefore, φ is not affine. $\square$

Lemma 2.2.6. *Let $H \leq G$ and let $h_1, h_2 \in H$. Define a map $\varphi: G \rightarrow G$ by*

$$\varphi(g) = \begin{cases} h_1g, & g \in H, \\ h_2g, & g \notin H. \end{cases}$$

Then φ is a bijection.

Proof. (Injectivity) Suppose $\varphi(g_1) = \varphi(g_2)$.

- If $g_1, g_2 \in H$, then $\varphi(g_i) = h_1g_i$ for $i = 1, 2$, so $h_1g_1 = h_1g_2$, this implies that $g_1 = g_2$.
- If $g_1, g_2 \notin H$, then $\varphi(g_i) = h_2g_i$ for $i = 1, 2$, so $h_2g_1 = h_2g_2$, this implies that $g_1 = g_2$.
- If $g_1 \in H$ and $g_2 \notin H$ (or vice versa), then $\varphi(g_1) = h_1g_1 \in H$, since H is a subgroup. But $\varphi(g_2) = h_2g_2 \in Hg_2$ which is a different coset of H . So $\varphi(g_1) \neq \varphi(g_2)$. This is a contradiction, so this case cannot occur.

(Surjectivity) Let y be an arbitrary element in G . We will find $x \in G$ such that $\varphi(x) = y$.

- If $y \in H$, we may let $x = h_1^{-1}y$. Since $h_1^{-1} \in H$ and H is a subgroup, so $x \in H$. Then

$$\varphi(x) = h_1x = h_1(h_1^{-1}y) = y.$$

- If $y \notin H$, we may let $x = h_2^{-1}y$. Then $x \notin H$ so

$$\varphi(x) = h_2x = h_2(h_2^{-1}y) = y. \quad \square$$

2.3 Preliminaries on Cayley graphs

Basic graph-theoretic terminology not defined here can be found in [16].

Definition 2.3.1 ([16, Chapter 1]). Let $\Gamma = (V, E)$ be a graph. Then a permutation $\alpha \in \text{Sym}(V)$ is an automorphism of Γ if and only if it preserves the adjacency in Γ . The set of all automorphisms of a graph Γ is called the automorphism group of the graph Γ and is denoted by $\text{Aut}(\Gamma)$.

Remark 2.3.2. The definition and notation for Cayley graphs used here differ from those in [16]. We write $\text{Cay}(G; S)$, whereas the notation $X(G, C)$ was common in the older literature. The notation $\text{Cay}(G; S)$ is now also widely used.

We join g to gs , whereas [16] joins g to sg . However, these two conventions give isomorphic undirected graphs. Indeed, the inversion map

$$\iota: G \rightarrow G, \quad \iota(g) = g^{-1},$$

sends an edge $\{g, gs\}$ to

$$\{g^{-1}, (gs)^{-1}\} = \{g^{-1}, s^{-1}g^{-1}\}.$$

Since $S = S^{-1}$, this is an edge under the convention using left multiplication. Therefore, the choice between gs and sg does not affect the graph up to isomorphism, and hence does not cause any essential difference in the results.

Definition 2.3.3 (cf. [16, p. 34]). Let G be a group and S be a subset of G , such that $S = S^{-1}$ (inverse-closed) and $\mathbf{1} \notin S$. The (simple undirected) Cayley graph on G with connection set S , denoted by $\text{Cay}(G; S)$, is the graph with the vertex set G and the edge set $\{\{g, gs\} \mid g \in G, s \in S\}$. Equivalently, two vertices $u, v \in G$ are adjacent if and only if $u^{-1}v \in S$.

Remark 2.3.4. We assume $1 \notin S$, in order to ensure that the Cayley graph $\text{Cay}(G; S)$ has no loops.

It is easy to see that the Cayley graph $\text{Cay}(G; S)$ is a $|S|$ -regular graph because each vertex $g \in G$ is connected by an edge to gs for each $s \in S$. Therefore, every vertex g is incident to exactly $|S|$ edges, confirming that $\text{Cay}(G; S)$ is $|S|$ -regular.

Lemma 2.3.5. *Let $\Gamma = \text{Cay}(G; S)$ be a Cayley graph on the group G . The left regular representation of G , defined by the set of automorphisms $L(G) = \{\ell_g \mid g \in G\}$ where $\ell_g(h) = gh$ for all $h \in G$, is a subgroup of $\text{Aut}(\Gamma)$.*

Proof. For every $g \in G$, the left translation $\ell_g: G \rightarrow G$ defined by $\ell_g(x) = gx$ maps vertices of Γ to vertices such that if there is an edge between x and xs for $s \in S$, then there is also an edge between gx and gxs . Hence, ℓ_g is an automorphism of Γ . Therefore, $L(G) = \{\ell_g \mid g \in G\}$ forms a subgroup of $\text{Aut}(\Gamma)$. $\square$

Proposition 2.3.6 ([16, Lemma 3.7.4]). *The Cayley graph $\text{Cay}(G; S)$ is connected if and only if S generates G .*

Lemma 2.3.7 ([16, Lemma 3.7.3]; see also Section 3.7). *Assume α is an automorphism of G and $S = S^{-1}$ is a subset of G .*

1. α is an isomorphism from $\text{Cay}(G; S)$ to $\text{Cay}(G; \alpha(S))$.
2. $\alpha \in \text{Aut}(\text{Cay}(G; S))$ if and only if $\alpha(S) = S$.

Definition 2.3.8 (cf. [33, Definition 1] and [15, Lemma 2.1]). A Cayley graph $\Gamma = \text{Cay}(G; S)$ is *normal* if every automorphism of the Cayley graph is affine.

2.4 Preliminaries on colour-permuting automorphisms

Definition 2.4.1 (Edge-Colouring [18, Definition 1.1]). By the definition of Cayley graphs, there is a *natural edge colouring* for the edges of a Cayley graph $\text{Cay}(G; S)$, such that the edge $\{g, gs\}$ is coloured by $\{s, s^{-1}\}$.

Since the Cayley graph is undirected, the edge between a group element g and gs is the same as the edge between gs and g . But these two directions correspond to multiplying by s and by its inverse s^{-1} , respectively. To make sure the colouring doesn't depend on which direction we are looking at, we assign the edge the colour $\{s, s^{-1}\}$, treating both elements as part of the same, symmetric label. This way, the colouring is well-defined for undirected edges.

Definition 2.4.2 ([18, p. 190]). An automorphism φ of $\text{Cay}(G; S)$ is *colour-preserving* if for every edge $\{x, xs\}$ coloured $\{s, s^{-1}\}$, the image edge $\{\varphi(x), \varphi(xs)\}$ is also coloured $\{s, s^{-1}\}$.

Definition 2.4.3 ([18, Definition 1.4]). An automorphism φ of a Cayley graph $\text{Cay}(G; S)$ is *colour-permuting* if it respects the colour classes; if two edges have the same colour, then their images under φ must also have the same colour. More precisely, there is a permutation π of the set of colours, such that if the colour of an edge e is c , then the colour of the edge $\varphi(e)$ is $\pi(c)$.

Definition 2.4.4 ([18, Definition 1.2]). A Cayley graph $\text{Cay}(G; S)$ is *CCA* if all of its colour-preserving automorphisms are affine functions on G . (CCA is an abbreviation for the *Cayley Colour Automorphism* property.)

Definition 2.4.5 ([18, Definition 1.2]). We say that G is *CCA* if every connected Cayley graph of G is CCA.

Definition 2.4.6 ([18, Definition 1.4]). $\text{Cay}(G; S)$ is *strongly CCA* if all of its colour-permuting automorphisms are affine functions.

Definition 2.4.7 ([18, Definition 1.4]). We say that G is *strongly CCA* if every connected Cayley graph of G is strongly CCA.

The following result gives several elementary properties of colour-permuting automorphisms. Although all are well known, we list them here for future reference.

Lemma 2.4.8.

1. A permutation φ of G is a colour-preserving automorphism of $\text{Cay}(G; S)$ if and only if, for all $g \in G$ and $s \in S$, we have $\varphi(gs) \in \{\varphi(g)s^{\pm 1}\}$. [18, p. 190]
2. An automorphism φ of a Cayley graph $\text{Cay}(G; S)$ is colour-permuting if and only if there is a permutation π of S , such that $\varphi(gs) \in \{\varphi(g)\pi(s)^{\pm 1}\}$ for all $g \in G$ and $s \in S$ (and $\pi(s^{-1}) = \pi(s)^{-1}$). [18, Definition 1.4]
3. For each $g \in G$, the left translation $\ell_g: x \mapsto gx$ is a colour-preserving automorphism of $\text{Cay}(G; S)$. [18, p. 190]
4. If α is an automorphism of the group G , such that $\alpha(s) \in \{s^{\pm 1}\}$ for all $s \in S$, then α is a colour-preserving automorphism of $\text{Cay}(G; S)$. [18, p. 190]
5. Every strongly CCA Cayley graph is CCA. So every strongly CCA group is CCA. [18, p. 191]
6. Every normal Cayley graph is strongly CCA. [18, Remark 1.6 (3)]
7. Assume $S \subseteq S' \subseteq G$. If $\text{Cay}(G; S)$ is CCA, then $\text{Cay}(G; S')$ is CCA. (cf. [13, Lemma. 3.1])

2.5 Preliminaries on the permutation of the connection set

Definition 2.5.1. Assume φ is an automorphism of $\text{Cay}(G; S)$. For each $g, h \in G$, define $\tilde{\pi}_g^\varphi(h) \in G$ by

$$\varphi(gh) = \varphi(g)\tilde{\pi}_g^\varphi(h).$$

So, for each $g \in G$, $\tilde{\pi}_g^\varphi: G \rightarrow G$.

We are most interested in the case where $h \in S$, so we let π_g^φ be the restriction of $\tilde{\pi}_g^\varphi$ to S . Therefore

$$\varphi(gs) = \varphi(g)\pi_g^\varphi(s)$$

for all $g \in G$ and $s \in S$.

We list the following well-known observations for future reference.

Lemma 2.5.2. *Assume that $\text{Cay}(G; S)$ is connected and $\varphi \in \text{Aut}(\text{Cay}(G; S))$. Then*

1. π_g^φ is a permutation of S for each $g \in G$.
2. $\pi_{gs}^\varphi(s^{-1}) = \pi_g^\varphi(s)^{-1}$ for all $g \in G$ and $s \in S$.
3. φ is colour-preserving if and only if $\pi_g^\varphi(s) \in \{s, s^{-1}\}$ for all $g \in G$ and $s \in S$.
4. φ is colour-permuting if and only if $\pi_h^\varphi(s) \in \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\}$ for all $g, h \in G$ and all $s \in S$.
5. φ is affine if and only if π_g^φ is independent of g : i.e., $\pi_g^\varphi(s) = \pi_h^\varphi(s)$ for all $g, h \in G$ and $s \in S$.
6. If φ is colour-permuting, then for all $g \in G$, $s \in S$, and $k \in \mathbb{Z}$, we have
 - (a) $|\pi_g^\varphi(s)| = |s|$. In particular, if $s^2 = \mathbf{1}$, then $\pi_g^\varphi(s)^2 = \mathbf{1}$,
 - (b) $\pi_g^\varphi(s^{-1}) = \pi_g^\varphi(s)^{-1}$,
 - (c) $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$, and
 - (d) $\tilde{\pi}_g^\varphi(s^k) = \pi_g^\varphi(s)^k$.

Proof. 1. We show that $\pi_g^\varphi: S \rightarrow S$ is a bijection for each $g \in G$.

We know $\varphi \in \text{Aut}(\text{Cay}(G; S))$, so it preserves adjacency. For any $s \in S$, we have:

$$\varphi(gs) = \varphi(g)t \quad \text{for some } t \in S.$$

By definition, $\pi_g^\varphi(s) = t$, so π_g^φ maps S to S .

We show π_g^φ is injective. If $\pi_g^\varphi(s_1) = \pi_g^\varphi(s_2)$, then:

$$\varphi(gs_1) = \varphi(g)\pi_g^\varphi(s_1) = \varphi(g)\pi_g^\varphi(s_2) = \varphi(gs_2).$$

Since φ is injective, $gs_1 = gs_2$ and thus $s_1 = s_2$.

Let $t \in S$. Since φ is a bijection on G , we know it is onto, so there exists a $x \in G$ such that $\varphi(x) = \varphi(g)t$. Because φ preserves adjacency, x is adjacent to g in $\text{Cay}(G; S)$, so $x = gs$ for some $s \in S$. Then

$$\varphi(gs) = \varphi(x) = \varphi(g)t,$$

and by the definition of π_g^φ we have $\pi_g^\varphi(s) = t$. Thus, for every $t \in S$, there is some $s \in S$ such that $\pi_g^\varphi(s) = t$. Thus π_g^φ is surjective.

2. By using definition of π_g^φ we have

$$\varphi(g) = \varphi(gss^{-1}) = \varphi(gs)\pi_{gs}^\varphi(s^{-1}) = \varphi(g)\pi_g^\varphi(s)\pi_{gs}^\varphi(s^{-1}),$$

so $\pi_{gs}^\varphi(s^{-1}) = \pi_g^\varphi(s)^{-1}$ for all $g \in G$ and $s \in S$.

3. By the definition of $\pi_g^\varphi(s)$, we have

$$\varphi(gs) = \varphi(g)\pi_g^\varphi(s).$$

Therefore, for all $g \in G$ and $s \in S$,

$$\begin{aligned} \varphi(gs) \in \{\varphi(g)s, \varphi(g)s^{-1}\} &\iff \varphi(g)\pi_g^\varphi(s) \in \{\varphi(g)s, \varphi(g)s^{-1}\} \\ &\iff \pi_g^\varphi(s) \in \{s, s^{-1}\}. \end{aligned}$$

Hence, by Lemma 2.4.8(1), φ is colour-preserving if and only if

$$\pi_g^\varphi(s) \in \{s, s^{-1}\}$$

for all $g \in G$ and $s \in S$.

4. ($\Rightarrow$). Assume φ is colour-permuting. By Definition 2.4.3, there exists a per-

mutation π of the set of colours, such that for every edge $\{x, xs\}$ with edge colour $\{s, s^{-1}\}$ its image $\{\varphi(x), \varphi(xs)\}$ has colour $\pi(\{s, s^{-1}\})$.

For any $x \in G$ we have

$$\varphi(xs) = \varphi(x) \pi_x^\varphi(s),$$

so the image edge $\{\varphi(x), \varphi(xs)\}$ has edge colour $\{\pi_x^\varphi(s), \pi_x^\varphi(s)^{-1}\}$. By the colour-permuting property this equals $\pi(\{s, s^{-1}\})$. Hence for every $x \in G$,

$$\{\pi_x^\varphi(s), \pi_x^\varphi(s)^{-1}\} = \pi(\{s, s^{-1}\}).$$

Plugging in $x = g$ and $x = h$ yields

$$\{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\} = \pi(\{s, s^{-1}\}) = \{\pi_h^\varphi(s), \pi_h^\varphi(s)^{-1}\}.$$

Therefore $\pi_h^\varphi(s)$ is either $\pi_g^\varphi(s)$ or $\pi_g^\varphi(s)^{-1}$, i.e.

$$\pi_h^\varphi(s) \in \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\},$$

as required.

($\Leftarrow$). We wish to show that if two edges $e_1 = (g, gs)$ and $e_2 = (h, hs)$ have the same colour $\{s, s^{-1}\}$, then the colour of $\varphi(e_1)$ is the same as the colour of $\varphi(e_2)$. Since

$$\varphi(e_1) = (\varphi(g), \varphi(gs)) = (\varphi(g), \varphi(g) \pi_g^\varphi(s))$$

so its colour is $\{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\}$. Similarly, the colour of $\varphi(e_2)$ is $\{\pi_h^\varphi(s), \pi_h^\varphi(s)^{-1}\}$. Also, by assumption, we know that $\pi_h^\varphi(s) \in \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\}$, so these two sets are equal. Hence $\varphi(e_1)$ and $\varphi(e_2)$ have the same colour.

5. ($\Rightarrow$). Suppose φ is affine, so $\varphi(x) = g'\alpha(x)$ for some $g' \in G$ and $\alpha \in \text{Aut}(G)$.

Then for any $g \in G$ and $s \in S$ we have

$$\varphi(gs) = g'\alpha(gs) = g'\alpha(g)\alpha(s)$$

and

$$\varphi(g) = g'\alpha(g).$$

From the definition of π_g^φ we know $\varphi(gs) = \varphi(g)\pi_g^\varphi(s)$. So this implies that

$$g'\alpha(g)\alpha(s) = g'\alpha(g)\pi_g^\varphi(s).$$

Multiplying both sides by $(g'\alpha(g))^{-1}$ gives

$$\alpha(s) = \pi_g^\varphi(s).$$

Since $\alpha(s)$ is independent of g , we conclude that $\pi_g^\varphi(s) = \pi_h^\varphi(s)$ for all $g, h \in G$.

($\Leftarrow$). Suppose π_g^φ is independent of g , so $\pi_g^\varphi(s) = \pi(s)$ for some function $\pi: S \rightarrow S$.

We will show that φ is affine by using Corollary 2.2.4.

Let $g \in G$ be arbitrary. Since $g \in G$ we can write $g = s_1 \cdots s_k$ where $s_i \in S$. We let $h = \pi(s_1) \cdots \pi(s_k)$.

We prove by induction on i

$$\varphi(xs_1s_2 \cdots s_i) = \varphi(x)\pi(s_1)\pi(s_2) \cdots \pi(s_i) \text{ for all } x \in G.$$

Base case: $i = 0$ is obvious (since $\varphi(x) = \varphi(x)$).

Inductive step: Assume the claim holds for $i - 1$. Then

$$\begin{aligned}
 \varphi(xs_1s_2 \cdots s_i) &= \varphi(xs_1 \cdots s_{i-1}s_i) \\
 &= \varphi(xs_1 \cdots s_{i-1})\pi_{xs_1 \cdots s_{i-1}}^\varphi(s_i) && \text{(definition of } \pi_{xs_1 \cdots s_{i-1}}^\varphi) \\
 &= \varphi(xs_1 \cdots s_{i-1})\pi(s_i) && (\pi_g^\varphi \text{ is independent of } g) \\
 &= \varphi(x)\pi(s_1) \cdots \pi(s_{i-1})\pi(s_i) && \text{(inductive hypothesis).}
 \end{aligned}$$

Then, for any $x \in G$, by letting $i = k$, we have

$$\varphi(xg) = \varphi(x)h.$$

Then by Corollary 2.2.4, φ is affine.

6a. Let $\Gamma = \text{Cay}(G; S)$. Fix $s \in S$. The edges of colour $\{s, s^{-1}\}$ form a subgraph Γ_s of Γ , which is a disjoint union of components. Each of these components has exactly $|s|$ vertices. In the special case where $|s| = 2$, each component is a perfect matching.

Now, if $\varphi \in \text{Aut}(\Gamma)$ is colour-permuting, then φ maps Γ_s onto $\Gamma_{\pi_g^\varphi(s)}$ for some $\pi_g^\varphi(s) \in S$ and $g \in G$. Since φ is a graph isomorphism, it preserves the number of vertices in each component. Therefore,

$$|\pi_g^\varphi(s)| = |s|.$$

6b. For any $g \in G$ and $s \in S$, we have

$$\varphi(gs^{-1}) = \varphi(g)\pi_g^\varphi(s^{-1}).$$

The colour of the edge from g to gs^{-1} is $\{s, s^{-1}\}$. Another edge with the same colour is the edge from g to gs , so the edge from $\varphi(g)$ to $\varphi(gs^{-1})$ must have the same colour

as the edge from $\varphi(g)$ to $\varphi(gs)$. In other words,

$$\{\pi_g^\varphi(s^{-1}), \pi_g^\varphi(s^{-1})^{-1}\} = \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\}.$$

So $\pi_g^\varphi(s^{-1})$ is either $\pi_g^\varphi(s)$ or $\pi_g^\varphi(s)^{-1}$.

If $\pi_g^\varphi(s^{-1}) = \pi_g^\varphi(s)^{-1}$, we are done.

Otherwise, $\pi_g^\varphi(s^{-1}) = \pi_g^\varphi(s)$. Since π_g^φ is injective, this forces $s^{-1} = s$, i.e. $s^2 = \mathbf{1}$.

In this case by Lemma 2.5.2(6a), $\pi_g^\varphi(s)^2 = \mathbf{1}$, so

$$\pi_g^\varphi(s^{-1}) = \pi_g^\varphi(s) = \pi_g^\varphi(s)^{-1},$$

which is what we wanted to prove.

6c. We prove by induction $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$, for $k \geq 0$.

Base case: $k = 0$ is trivially true.

Inductive step for $k \geq 1$: Assume $\pi_{gs^m}^\varphi(s) = \pi_g^\varphi(s)$ holds for all integers $m \in \{0, 1, 2, \dots, k-1\}$. We want to show that $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$.

Since φ is a colour-permuting, $\pi_{gs^k}^\varphi(s) \in \{\pi_g^\varphi(s), \pi_g^\varphi(s)^{-1}\}$. If $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$ we are done. So suppose instead $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)^{-1}$. Then

$$\begin{aligned} \varphi(gs^{k+1}) &= \varphi(gs^k) \pi_{gs^k}^\varphi(s) && \text{(definition of } \pi_{gs^k}^\varphi) \\ &= \varphi(gs^k) \pi_g^\varphi(s)^{-1} && (\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)^{-1}) \\ &= (\varphi(gs^{k-1}) \pi_{gs^{k-1}}^\varphi(s)) \pi_g^\varphi(s)^{-1} && \text{(definition of } \pi_{gs^{k-1}}^\varphi) \\ &= \varphi(gs^{k-1}) \pi_g^\varphi(s) \pi_g^\varphi(s)^{-1} && \text{(Inductive hypothesis)} \\ &= \varphi(gs^{k-1}). \end{aligned}$$

Since φ is injective, this implies $gs^{k+1} = gs^{k-1}$, i.e. $s^2 = \mathbf{1}$.

But then, by Lemma 2.5.2(6a), $\pi_g^\varphi(s)^2 = \mathbf{1}$, $\pi_g^\varphi(s)^{-1} = \pi_g^\varphi(s)$. Thus

$$\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)^{-1} = \pi_g^\varphi(s),$$

which is the desired equality.

Thus in all cases we have $\pi_{gs^k}^\varphi(s) = \pi_g^\varphi(s)$, which completes the induction for $k \geq 0$.

Also, by replacing s with s^{-1} , we have

$$\pi_{gs^{-k}}^\varphi(s^{-1}) = \pi_g^\varphi(s^{-1})$$

so by Lemma 2.5.2(6b)

$$\pi_{gs^{-k}}^\varphi(s)^{-1} = \pi_g^\varphi(s)^{-1},$$

so

$$\pi_{gs^{-k}}^\varphi(s) = \pi_g^\varphi(s).$$

Hence, the desired is also true for $k < 0$.

6d. We first prove the claim for $k \geq 0$ by induction.

Base case: It is true for $k = 0$ trivially.

Inductive step for $k \geq 1$: Suppose the equality holds for $k - 1$. By definition of π_g^φ ,

$$\varphi(gs^k) = \varphi(g)\tilde{\pi}_g^\varphi(s^k).$$

Also,

$$\begin{aligned}
 \varphi(gs^k) &= \varphi(gs^{k-1}s) \\
 &= \varphi(gs^{k-1})\pi_{gs^{k-1}}^\varphi(s) && \text{(definition of } \pi_{gs^{k-1}}^\varphi \text{)} \\
 &= \varphi(g)\tilde{\pi}_g^\varphi(s^{k-1})\pi_g^\varphi(s) && \text{(by definition of } \tilde{\pi}_g^\varphi \text{ and 6c)} \\
 &= \varphi(g)\pi_g^\varphi(s)^{k-1}\pi_g^\varphi(s) && \text{(Induction hypothesis)} \\
 &= \varphi(g)\pi_g^\varphi(s)^k.
 \end{aligned}$$

By equating the two expressions we have

$$\tilde{\pi}_g^\varphi(s^k) = \pi_g^\varphi(s)^k.$$

This completes the induction for $k \geq 0$.

Also,

$$\tilde{\pi}_g^\varphi(s^{-k}) = \tilde{\pi}_g^\varphi((s^{-1})^k) = \pi_g^\varphi(s^{-1})^k = (\pi_g^\varphi(s)^{-1})^k = \pi_g^\varphi(s)^{-k}.$$

Hence, the desired equality is true for $k < 0$. Thus the equality holds for all integers k . $\square$

For ease of reference we restate a few parts of lemma 2.5.2.

Corollary 2.5.3. *Assume φ is a colour-permuting automorphism of $\text{Cay}(G; S)$. Then the following hold.*

1. *If $g \in G$ and $s, t \in S$ satisfy $\varphi(gs) = \varphi(g)t$, then $\varphi(gs^n) = \varphi(g)t^n$ for all $n \in \mathbb{Z}$.*
2. *If $\varphi(\mathbf{1}) = \mathbf{1}$, then, for all $g \in G$, $s \in S$, and $n \in \mathbb{Z}$, we have*

$$\varphi(gs^n) \in \{\varphi(g)\varphi(s)^{\pm n}\}.$$

Proof. 1 By the definition of π_g^φ , the assumption $\varphi(gs) = \varphi(g)t$ means that

$$\pi_g^\varphi(s) = t.$$

Therefore, by Lemma 2.5.2(6d), we have

$$\tilde{\pi}_g^\varphi(s^n) = \pi_g^\varphi(s)^n = t^n$$

for all $n \in \mathbb{Z}$. Hence

$$\varphi(gs^n) = \varphi(g)\tilde{\pi}_g^\varphi(s^n) = \varphi(g)t^n,$$

as required.

2 since $\varphi(\mathbf{1}) = \mathbf{1}$, we have

$$\pi_{\mathbf{1}}^\varphi(s) = \varphi(s).$$

By Lemma 2.5.2(4), applied with $h = \mathbf{1}$, we obtain

$$\pi_g^\varphi(s) \in \{ \pi_{\mathbf{1}}^\varphi(s), \pi_{\mathbf{1}}^\varphi(s)^{-1} \} = \{ \varphi(s), \varphi(s)^{-1} \}.$$

Now Lemma 2.5.2(6d) gives

$$\varphi(gs^n) = \varphi(g)\tilde{\pi}_g^\varphi(s^n) = \varphi(g)\pi_g^\varphi(s)^n.$$

Therefore

$$\varphi(gs^n) \in \{ \varphi(g)\varphi(s)^n, \varphi(g)\varphi(s)^{-n} \},$$

as required. □

Corollary 2.5.4. *If $\text{Cay}(G; S)$ is connected, and $\pi_g^\varphi = \pi_{gt}^\varphi$ for all $g \in G$ and $t \in S$, then φ is affine.*

Proof. Let g and h be arbitrary elements of G . Since $\text{Cay}(G; S)$ is connected, h can

be written as a product $h = gt_1t_2\cdots t_n$ for some $t_1, \dots, t_n \in S$. We will show by induction on k that

$$\pi_{gt_1t_2\cdots t_k}^\varphi = \pi_g^\varphi.$$

Base case: If $k = 0$, then $gt_1t_2\cdots t_k = g$ and trivially $\pi_{gt_1t_2\cdots t_k}^\varphi = \pi_g^\varphi$.

Inductive step: Suppose that for some $k \geq 0$, we have $\pi_{h'}^\varphi = \pi_g^\varphi$, where $h' = gt_1\cdots t_{k-1}$.

Since $t_k \in S$, from the assumption we have

$$\pi_{h'}^\varphi = \pi_{h't_k}^\varphi = \pi_{gt_1\cdots t_{k-1}\cdot t_k}^\varphi = \pi_{gt_1\cdots t_k}^\varphi.$$

Thus, by induction,

$$\pi_g^\varphi = \pi_{gt_1\cdots t_n}^\varphi = \pi_h^\varphi$$

Therefore, π_g^φ is independent of g , and by Lemma 2.5.2(5), φ is affine. $\square$

In a 2015 talk, Joy Morris asked whether Cayley graphs of small valency must be CCA, even when the underlying group is not CCA [27]. Here, the valency of a graph is the number of edges incident with each vertex; for a Cayley graph $\text{Cay}(G; S)$, this is $|S|$. Thus, the question asks whether restricting attention to generating sets of small size can prevent the existence of non-affine colour-preserving automorphisms.

The following new result shows that this is not the case. Indeed, it establishes that non-CCA behaviour is already visible at the level of two generators: whenever a Cayley graph $\text{Cay}(G; S)$ is not CCA, this failure is witnessed by a 2-generated Cayley subgraph.

Theorem 2.5.5. *If $\text{Cay}(G; S)$ is not CCA, then there is a 2-element subset $\{s, t\}$ of S , such that $\text{Cay}(\langle s, t \rangle; \{s^{\pm 1}, t^{\pm 1}\})$ is not CCA.*

Proof. Since $\text{Cay}(G; S)$ is not CCA, there exists a non-affine, colour-preserving automorphism φ . By Corollary 2.5.4, there exist $g \in G$ and $s, t \in S$ with

$$\pi_g^\varphi(s) \neq \pi_{gt}^\varphi(s). \quad (2.5.6)$$

We define the colour-preserving automorphism

$$\varphi'(x) = \varphi(g)^{-1}\varphi(gx).$$

(Since left translations are colour-preserving automorphisms of Cayley graphs, and φ is colour-preserving, it follows that φ' is also a colour-preserving automorphism.)

Also, let $H = \langle s, t \rangle$ with generators s, t from the inequality and define $\varphi_H = \varphi'|_H$.

Then φ_H has these properties:

1. $\varphi_H(\mathbf{1}) = \mathbf{1}$, because

$$\varphi_H(\mathbf{1}) = \varphi'(\mathbf{1}) = \mathbf{1}.$$

2. $\pi_h^{\varphi_H} = \pi_{gh}^\varphi$ for all $h \in H$, because:

$$\varphi_H(hs) = \varphi_H(h)\pi_h^{\varphi_H}(s) \quad (\text{by definition of } \pi)$$

so

$$\varphi(g)^{-1}\varphi(ghs) = \varphi(g)^{-1}\varphi(gh)\pi_h^{\varphi_H}(s) \quad (\text{definitions of } \varphi_H \text{ and } \varphi')$$

so

$$\varphi(gh)^{-1}\varphi(ghs) = \pi_h^{\varphi_H}(s) \quad (\text{solving for } \pi_h^{\varphi_H}(s))$$

But from the definition of π_{gh}^φ , we know

$$\varphi(ghs) = \varphi(gh)\pi_{gh}^\varphi(s)$$

Substituting this in:

$$\varphi(gh)^{-1}\varphi(gh)\pi_{gh}^\varphi(s) = \pi_h^{\varphi_H}(s)$$

Thus $\pi_h^{\varphi_H}(s) = \pi_{gh}^\varphi(s)$. This holds for all generators $s \in S$ and all $h \in H$.

Therefore $\pi_h^{\varphi_H} = \pi_{gh}^\varphi$.

3. $\pi_1^{\varphi_H}(s) \neq \pi_t^{\varphi_H}(s)$.

Let $h = 1$ and $h = t$ in 2, so we have $\pi_1^{\varphi_H}(s) = \pi_g^\varphi(s)$, and $\pi_t^{\varphi_H}(s) = \pi_{gt}^\varphi(s)$. By (2.5.6), we know that the right sides of these two equations are not equal, so the left sides are not equal too. I.e., $\pi_1^{\varphi_H}(s) \neq \pi_t^{\varphi_H}(s)$.

We claim that φ_H is a colour-preserving automorphism of $\text{Cay}(H; \{s^{\pm 1}, t^{\pm 1}\})$. First, note that $\varphi_H(H) = H$. For any $h \in H$ and $u \in \{s, t\}$:

$$\varphi_H(hu) = \varphi'(hu) = \varphi'(h)\pi_h^{\varphi'}(u) = \varphi_H(h)\pi_h^{\varphi'}(u).$$

So $\pi_h^{\varphi_H}(u) = \pi_h^{\varphi'}(u)$. Since H is a subgroup and φ' preserves the colours of the edges in G , it preserves the colours of edges in H . We have

$$\pi_h^{\varphi_H}(u) = \pi_h^{\varphi'}(u) \in \{u, u^{-1}\} \quad (\text{by Lemma 2.5.2(3)})$$

This completes the proof of the claim.

However, by (3), we have

$$\pi_1^{\varphi_H}(s) \neq \pi_t^{\varphi_H}(s)$$

Thus φ_H cannot be affine by Lemma 2.5.2(5).

Therefore $\text{Cay}(H; \{s^{\pm 1}, t^{\pm 1}\})$ admits a non-affine colour-preserving automorphism φ_H , making it non-CCA. □

Corollary 2.5.7. *Let G be a group. Suppose that, for every 2-element subset $\{s, t\}$*

of G , the Cayley graph

$$\text{Cay}(\langle s, t \rangle; \{s^{\pm 1}, t^{\pm 1}\})$$

is CCA. Then every connected Cayley graph on G is CCA.

Proof. Immediate from Theorem 2.5.5. $\square$

We record the following well-known elementary facts for future reference.

Lemma 2.5.8. *Assume φ is a colour-permuting automorphism of $\text{Cay}(G; S)$, such that $\varphi(\mathbf{1}) = \mathbf{1}$, and let $H = \langle s \in S \mid s^2 = \mathbf{1} \rangle$. Then $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g \in G$ and $h \in H$.*

Proof. Let S_2 be the set of all elements of order 2 in S . From the definition of π_g^φ we have

$$\varphi(gs) = \varphi(g)\pi_g^\varphi(s). \quad (2.5.9)$$

plugging $g = 1$, and using $\varphi(\mathbf{1}) = \mathbf{1}$, it follows that $\pi_1^\varphi(s) = \varphi(s)$.

Since φ is a colour-permuting automorphism, by Lemma 2.5.2(4) we have

$$\pi_g^\varphi(s) \in \{\pi_{g'}^\varphi(s), \pi_{g'}^\varphi(s)^{-1}\} \quad \text{for all } g, g' \in G. \quad (2.5.10)$$

On the other hand, since $s^2 = \mathbf{1}$, Lemma 2.5.2(6a) implies $(\pi_{g'}^\varphi(s))^2 = \mathbf{1}$ for all $g' \in G$. So $\pi_{g'}^\varphi(s)^{-1} = \pi_{g'}^\varphi(s)$. Therefore in (2.5.10) $\pi_g^\varphi(s) = \pi_{g'}^\varphi(s)$. Taking $g' = 1$, we obtain $\pi_g^\varphi(s) = \pi_1^\varphi(s) = \varphi(s)$. Substituting into (2.5.9) yields

$$\varphi(gs) = \varphi(g)\pi_g^\varphi(s) = \varphi(g)\pi_1^\varphi(s) = \varphi(g)\varphi(s).$$

Let $h \in H$, so $h = s_1 s_2 \cdots s_n$ for some $s_1, \dots, s_n \in S_2$.

We prove by induction on n that

$$\varphi(gs_1 \cdots s_n) = \varphi(g)\varphi(s_1) \cdots \varphi(s_n) \quad \text{for all } g \in G.$$

Base case $n = 1$: We already showed $\varphi(gs_1) = \varphi(g)\varphi(s_1)$.

Inductive step: Assume the statement holds for $n - 1$. Then

$$\varphi(gs_1 \cdots s_n) = \varphi((gs_1 \cdots s_{n-1})s_n).$$

By the base case (with $gs_1 \cdots s_{n-1}$ in place of g and s_n in place of s):

$$\varphi((gs_1 \cdots s_{n-1})s_n) = \varphi(gs_1 \cdots s_{n-1})\varphi(s_n).$$

By the inductive hypothesis (with g):

$$\varphi(gs_1 \cdots s_{n-1}) = \varphi(g)\varphi(s_1) \cdots \varphi(s_{n-1}).$$

Thus:

$$\varphi(gs_1 \cdots s_n) = \varphi(g)\varphi(s_1) \cdots \varphi(s_{n-1})\varphi(s_n).$$

This completes the induction.

In particular, taking $g = \mathbf{1}$, we get

$$\varphi(h) = \varphi(s_1) \cdots \varphi(s_n).$$

Therefore,

$$\varphi(gh) = \varphi(g)\varphi(s_1) \cdots \varphi(s_n) = \varphi(g)\varphi(h). \quad \square$$

Lemma 2.5.11. *Assume φ is a colour-preserving automorphism of $\text{Cay}(G; S)$, and let $H = \langle s \in S \mid s^2 = \mathbf{1} \rangle$. Then:*

1. $\varphi(gh) = \varphi(g)h$, for all $g \in G$ and $h \in H$.
2. In particular, if $\varphi(\mathbf{1}) = \mathbf{1}$, then $\varphi(h) = h$ for all $h \in H$.

Proof. Let φ be a colour-preserving automorphism of $\text{Cay}(G; S)$, by Lemma 2.5.2(3)

$$\pi_g^\varphi(s) \in \{s, s^{-1}\} \quad \text{for all } g \in G, s \in S.$$

Now, if $s \in S$ with $s^2 = \mathbf{1}$, then $s^{-1} = s$, so

$$\pi_g^\varphi(s) = s \quad \text{for all } g \in G.$$

By the definition of π_g^φ , this implies

$$\varphi(gs) = \varphi(g) \pi_g^\varphi(s) = \varphi(g) s.$$

This establishes the claim for generators of H .

Let $h \in H$, so $h = s_1 s_2 \cdots s_k$ with each $s_i^2 = \mathbf{1}$. We prove by induction on k that

$$\varphi(gh) = \varphi(g)h.$$

Base case: for $k = 1$ established above.

By the inductive hypothesis, $\varphi(gh) = \varphi(g)h$, and let $h' = hs_{k+1}$. So

$$\varphi(gh') = \varphi((gh)s_{k+1}) = \varphi(gh)s_{k+1} = \varphi(g)hs_{k+1} = \varphi(g)(hs_{k+1}) = \varphi(g)h'.$$

Thus the claim holds for k , completing the induction.

This proves part (1). For part (2), if $\varphi(\mathbf{1}) = \mathbf{1}$, then for any $h \in H$ we have

$$\varphi(h) = \varphi(\mathbf{1} \cdot h) = \varphi(\mathbf{1})h = h. \quad \square$$

Chapter 3

Literature Review

Arthur Cayley introduced the definition of the Cayley graph in 1878 to illustrate abstract groups defined by a set of generators. Over the past 50 years, the study of Cayley graphs has become a significant branch of algebraic graph theory. Cayley graphs are connected to classical problems in pure mathematics, such as the classification, isomorphism, and enumeration of Cayley graphs. Notable surveys by Xu [40], Li [25], and the handbook by Babai [4] delve into these mathematical aspects. Additionally, Cayley graphs relate to practical problems studied by professionals in graph theory, group theory, networks, molecular biology, coding theory, and other areas (see, for example, [1, 12]).

3.1 Automorphisms of Cayley Graphs

In this section, we introduce the key ideas we need to understand the relationship between automorphisms, vertex-transitivity, and Cayley graphs. We start by defining an automorphism, which is a way to describe the symmetries of a graph, and the set of all these symmetries forms the automorphism group, $\text{Aut}(\Gamma)$. For any group G , a natural question to ask is what is the automorphism group for a Cayley graph on G .

We then show that for Cayley graphs, the left regular representation of the group forms a subgroup of the automorphism group. This tells us that the group's structure directly influences the graph's symmetries.

Next, we explain the concept of vertex-transitivity, it means any of a graph's

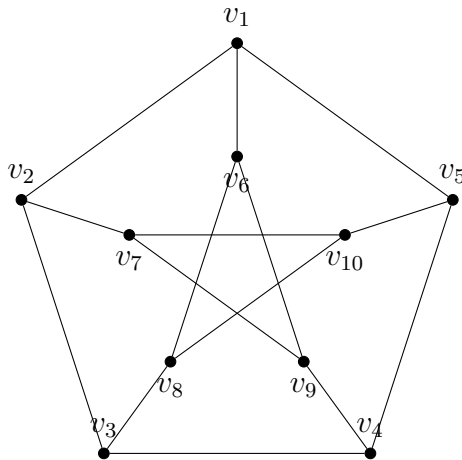


Figure 3.1: Petersen graph

vertices can be mapped to any other by one of its automorphisms. We prove that all Cayley graphs have this property.

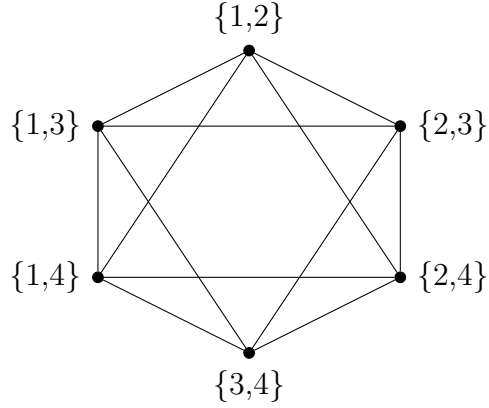
Finally, we introduce a result that shows when a graph is actually a Cayley graph based on how its automorphism group acts on its vertices. This helps us understand which graphs fit into the Cayley graph structure and which do not.

Definition 3.1.1 ([5, Chapter 16]). A graph Γ is called *vertex-transitive* if for every pair of its vertices x and y , there is an automorphism $\alpha \in \text{Aut}(\Gamma)$ such that $\alpha(x) = y$.

Corollary 3.1.2 ([16, Chapter 3]). *All Cayley graphs are vertex-transitive.*

Proof. As a result of Lemma 2.3.5, for all $x, y \in G$, the automorphism $\ell_{yx^{-1}} \in L(G)$ maps x to y . Therefore, Γ is a vertex-transitive graph. $\square$

Example 3.1.3. Let $\Omega = \{1, 2, \dots, n\}$ and let k and i be two positive integers such that $n \geq k \geq i$. The Johnson graph $J(n, k, i)$ is a graph with the vertex set as k -subsets of Ω and two vertices A and B are adjacent when $|A \cap B| = i$. In [16, Chapter 3] it is shown that the Johnson graphs are vertex-transitive. $J(n, k, 0)$ is called the Kneser graph $K(n, k)$, and $J(5, 2, 0)$ is called the Petersen graph, shown in Figure 3.1. Also, $J(n, k, k - 1)$ is denoted by $J(n, k)$ (see Figure 3.2).


 Figure 3.2: $J(4, 2)$

We see that all Cayley graphs are vertex-transitive, but the converse is not true. There are some classes of vertex-transitive graphs that are not Cayley graphs. For example, consider the following theorem.

Theorem 3.1.4 ([29, Theorem 2.1]). *Let n, k be integers, $n > k$, $2 \leq k \leq \frac{n}{2}$, and $\binom{n}{k}$ is an even integer. Then the Kneser graph $K(n, k)$ is a vertex-transitive non-Cayley graph if one of the following conditions holds:*

- n is an odd integer;
- n and k are even integers.

Definition 3.1.5. A group G is said to *act regularly* on a set X if each point in X has a unique group element mapping it to any other point in X , and no non-identity element of G leaves any point in X fixed.

Lemma 3.1.6 ([5, Lemma 16.3]). *Let Γ be a connected graph such that $G = \text{Aut}(\Gamma)$. Then the subgroup H of G acts regularly on the vertex set of Γ if and only if Γ is isomorphic to a Cayley graph $\text{Cay}(H; \Omega)$ for some subset $\Omega \subseteq H$.*

Proof. Let $\Gamma = \text{Cay}(H; \Omega)$. Let $h \in H$ and $L_H = \{\ell_h \mid h \in H\}$, define $\ell_h : H \rightarrow H$ by $\ell_h(g) = hg$. We know $\ell_h \in \text{Aut}(\Gamma)$. (It acts transitively on Γ since for all $h_1, h_2 \in H$, we have $\ell_{h_2 h_1^{-1}}(h_1) = h_2 h_1^{-1}(h_1) = h_2$.)

Let $g \in H$ and $\ell_h(g) = g$ then we have $hg = g$, which implies $h = \mathbf{1}$. Therefore, $\ell_h = \ell_{\mathbf{1}}$. Notice $\ell_{\mathbf{1}} = id$. Thus, L_H acts regularly.

Conversely, Let $V(\Gamma) = \{v_1, \dots, v_n\}$ be the vertex set of Γ . Let H be a subgroup of $\text{Aut}(\Gamma)$ acting regularly on $V(\Gamma)$.

Then for each $i \in \{1, \dots, n\}$, there is a unique $h_i \in H$ such that $h_i(v_1) = v_i$. For contradiction, let $h_i \neq h'_i$ and $h_i(v_1) = h'_i(v_1) = v_i$. Then $h_i^{-1}h'_i(v_1) = v_1$, so $h_i^{-1}h'_i \in H_{v_1} = \{\mathbf{1}\}$ so $h_i^{-1}h'_i = \mathbf{1}$ then $h_i = h'_i$, it is a contradiction.

Let $\Omega = \{h_i \in H \mid v_i \text{ is adjacent to } v_1 \text{ in } \Gamma\}$. Then $\Omega \subseteq H$, and $\mathbf{1} \notin \Omega$. Let $h_i(v_1) = v_i$ and $h_i^{-1}(v_1) = v_j$. Since H is a group and $h_i^{-1} \in H$ then $H \subseteq \text{Aut}(\Gamma)$ and we have $h_i^{-1}(v_1)$ adjacent to $h_i^{-1}(v_i)$. On the other hand, $h_i^{-1}(v_1) = v_j$ and $h_i^{-1}(v_i) = v_1$. The vertex v_1 is adjacent to v_j , which implies that $h_i^{-1} \in \Omega$. Therefore, $\Omega = \Omega^{-1}$. Thus, we can define the Cayley graph $\text{Cay}(H; \Omega)$.

Let $\varphi : \Gamma \rightarrow \text{Cay}(H; \Omega)$ be a map defined by $\varphi(v_i) = h_i$. We show φ is injective. Let $\varphi(v_i) = \varphi(v_j)$ so $h_i = h_j$ so $h_i(v_1) = h_j(v_1)$ so $v_i = v_j$.

We now show that φ is surjective. Let $h \in H$. Since h is an automorphism of Γ , we have

$$h(v_1) \in V(\Gamma).$$

Therefore, there is some $i \in 1, \dots, n$ such that

$$h(v_1) = v_i.$$

By the definition of h_i , it is the unique element of H satisfying

$$h_i(v_1) = v_i.$$

Since $h(v_1) = v_i$, the uniqueness of h_i implies that $h = h_i$. Hence,

$$\varphi(v_i) = h_i = h.$$

Therefore, every element of H lies in the image of φ , so φ is surjective.

Let v_i be adjacent to v_j in Γ . Since $h_i^{-1} \in \text{Aut}(\Gamma)$ so $h_i^{-1}(v_i) \sim h_i^{-1}(v_j)$ so $v_1 \sim h_i^{-1}(v_j)$ which is equal to $h_i^{-1}h_j(v_1) = h_i^{-1}(v_j) \sim v_1$. Then $h_i^{-1}h_j \in \Omega$, meaning h_i is adjacent to h_j , so $\varphi(v_i) \sim \varphi(v_j)$.

On the other hand, let $\varphi(v_i) \sim \varphi(v_j)$ then h_i is adjacent to h_j . It means $h_i^{-1}(h_j) \in \Omega$. Now we have $h_i^{-1}h_j(v_1) = h_i^{-1}(v_j)$. So $h_i^{-1}(v_j)$ is adjacent to v_1 , and therefore $h_i^{-1}(v_j)$ is adjacent to $h_i(v_i)$. Then we can conclude that $v_i \sim v_j$.

Therefore, φ is an isomorphism, implying $\Gamma \cong \text{Cay}(H; \Omega)$. $\square$

Next, we define a specific subset of the automorphism group of G that will play a crucial role in the structure of the automorphism group of the corresponding Cayley graph.

Let G be a group and $S \subset G$. The set of all automorphisms of G which preserves S is a group denoted by $\text{Aut}(G; S)$. In other words:

$$\text{Aut}(G; S) = \{\varphi \in \text{Aut}(G) \mid \varphi(S) = S\},$$

where for $C \subseteq G$ and $\varphi \in \text{Aut}(G)$, we define

$$\varphi(C) = \{\varphi(g) \mid g \in C\}.$$

There are some things we can always say about automorphism groups of Cayley graphs. We have already shown that every left-translation ℓ_g is always in the automorphism group. Now we will show that the elements of $\text{Aut}(G; S)$ are also always in the automorphism group of $\text{Cay}(G; S)$.

To see this, let $\Gamma = \text{Cay}(G; S)$ and $\alpha \in \text{Aut}(G)$ such that $\alpha(S) = S$. Then for two

adjacent vertices $g, h \in G$ we have $g^{-1}h \in S$. So

$$(\alpha(g))^{-1}\alpha(h) = \alpha(g^{-1})\alpha(h) = \alpha(g^{-1}h) \in \alpha(S) = S.$$

So α is an automorphism of the Cayley graph $\text{Cay}(G; S)$.

We have just shown that $\text{Aut}(G; S) \leq \text{Aut}(\Gamma)$. The observation about $\text{Aut}(G; S)$ was first made by Godsil in [15], where he proved the following group-theoretic characterization of this subgroup.

Lemma 3.1.7 ([15, Lemma 2.1]). *Let $\Gamma = \text{Cay}(G; S)$ and $A = \text{Aut}(\Gamma)$. Then $N_A(L(G)) \cap A_1 = \text{Aut}(G; S)$, where $S \subseteq G$. Note that $N_A(L(G))$ is the normalizer of $L(G)$ in A ; and A_1 is the subgroup of A that fixes the identity vertex.*

Proof. Observe that $\text{Aut}(G; S) \leq A_1$, since every group automorphism fixes the identity. Let $g \in G$. Then it is easy to see that $\varphi^{-1}\ell_g\varphi = \ell_{\varphi^{-1}g\varphi}$ for all $\varphi \in \text{Aut}(G)$, so $\text{Aut}(G; S) \subseteq N_A(L(G))$. On the other hand, it is not difficult to see that every permutation of G that normalizes $L(G)$ and fixes $\mathbf{1}$ is an automorphism of G , since conjugation on $L(G)$ is a homomorphism. Therefore, $N_A(L(G)) \cap A_1 \subseteq \text{Aut}(G; S)$. $\square$

Putting what we have seen together, it is always the case that

$$L(G) \rtimes \text{Aut}(G; S) \leq \text{Aut}(\text{Cay}(G; S)).$$

Indeed, the semidirect product is taken with respect to the conjugation action of $\text{Aut}(G; S)$ on $L(G)$, and it is identified with the subgroup

$$\{\ell_g\alpha \mid g \in G, \alpha \in \text{Aut}(G; S)\}$$

of $\text{Aut}(\text{Cay}(G; S))$, where $(\ell_g\alpha)(x) = g\alpha(x)$ for all $x \in G$.

Chris Godsil has conducted significant research on the automorphism groups of Cayley graphs. One of his notable contributions is in the characterization of Graphical

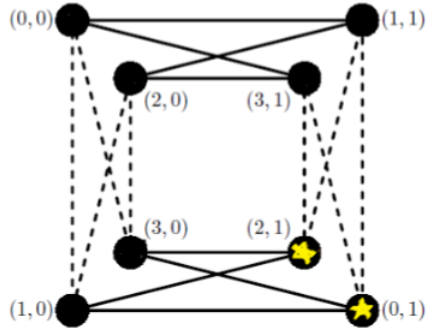

 FIGURE 3. $\text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1,0), \pm(1,1)\})$.

 Figure 3.3: $\text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1,0), \pm(1,1)\})$

Regular Representations (GRRs), where he showed that, most groups have a Cayley graph whose full automorphism group is equal to the regular action of G .

3.2 Graphical Regular Representations (GRRs)

In this thesis, we focus on automorphisms of Cayley graphs that are affine maps, which we will discuss in more detail in Chapter 5.

Definition 3.2.1 ([18, Definition 1.2]). A function $\varphi: G \rightarrow G$ is said to be *affine* if it is the composition of an automorphism of G with left translation by an element of G . This means $\varphi(x) = \alpha(gx)$, for some $\alpha \in \text{Aut}(G)$ and $g \in G$.

We already saw that $L(G) \rtimes \text{Aut}(G; S)$ is exactly the subgroup of affine functions in $\text{Aut}(\text{Cay}(G; S))$.

As we mentioned before, sometimes graphs have other automorphisms that are not easy to detect just by analyzing G and S . For example, consider $\text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1,0), \pm(1,1)\})$. There is a graph automorphism φ that swaps the positions of the vertices $(0,1)$ and $(2,1)$ while leaving all other vertices unchanged, see Figure 3.3. It is important to note that although φ is a graph automorphism, it is not affine.

Definition 3.2.2 ([22, pp. 243-244]). A *Graphical Regular Representation (GRR)* of a group G is a Cayley graph $\Gamma = \text{Cay}(G; S)$ such that the automorphism group of the graph, $\text{Aut}(\Gamma)$, is exactly equal to the left regular representation of G . (A group G admits a GRR if there is a graph Γ such that $G \cong \text{Aut}(\Gamma)$ and $\text{Aut}(\Gamma)$ acts regularly on the vertex set of Γ . [5, Definition 16.4])

In other words, a GRR just has no other symmetries. As we saw in the previous section the left regular representation of G is always a subgroup of $\text{Aut}(\Gamma)$ and those are the only things that we always know are in the automorphism group of Cayley graph. Additionally, since

$$L(G) \rtimes \text{Aut}(G; S) \leq \text{Aut}(\text{Cay}(G; S)),$$

for the Cayley graph to be a GRR, the group $\text{Aut}(G; S)$ has to be the identity map.

The study of GRRs involved contributions from many researchers. We can find some of them in [20, 21].

Chao in [7] and independently, Sabidussi in [32] showed that abelian groups, except for elementary abelian 2-groups (which are direct products of cyclic groups of order 2), cannot admit GRRs. This is because Chao proved that no connected graph can have an abelian automorphism group acting regularly unless the group consists entirely of elements of order 2, which corresponds to elementary abelian 2-groups. Thus, any abelian group that is not of this form (i.e., not entirely made up of elements of order 2) cannot act regularly as the automorphism group of a graph, ruling out GRRs for such groups.

The investigation of groups continued by Imrich in [20] led to the classification of elementary abelian 2-groups, identifying exactly three groups that do not have a GRR. Specifically, he showed that there is a GRR for $\mathbb{Z}_2^n$ if and only if $n \neq 2, 3$, or 4. However, it was later discovered that the construction provided in [20] was incorrect for $n = 5$. This error was identified by B. Alspach, P. Hell, D. Hetzel, and Chong-

Keang Lim, who, along with R. Frucht and M. H. McAndrew, subsequently provided a correct construction for the case $n = 5$. See, for example, the construction in [22].

Watkins, [34], began by exploring whether finite non-abelian groups can have regular representations as automorphism groups of graphs. He introduced two classes of groups: Class I consists of groups that admit GRRs, while Class II consists of groups that do not admit GRRs. He showed that generalized dicyclic groups do not have GRRs.

Through a series of papers, Watkins, along with coauthor Nowitz in some instances [30, 34, 35, 36], identified ten other nonabelian groups lacking a GRR. Hetzel [17] demonstrated that apart from the one infinite family previously described by Watkins, along with the thirteen small solvable groups (of order at most 32) identified by Imrich, Nowitz, and Watkins, all solvable groups possess a GRR. Godsil, in [15], completed the classification for nonsolvable groups, showing that every nonsolvable group admits a GRR.

Theorem 3.2.3 (Godsil, Hetzel, Imrich, Nowitz, and Wakis; see [14]). *The groups listed below are the only ones that are neither generalized dicyclic nor abelian with an exponent greater than 2, yet do not admit a GRR:*

- $\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4$;
- D_6, D_8, D_{10} , where D_n denotes the dihedral group of order n ;
- A_4 , the alternating group of degree 4;
- $H_1 = \langle a, b, c : a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle$;
- $H_2 = \langle a, b : a^8 = b^2 = 1, bab = a^5 \rangle$;
- $H_3 = \langle a, b, c : a^3 = b^3 = c^2 = 1, ab = ba, (ac)^2 = (bc)^2 = 1 \rangle$;
- $H_4 = \langle a, b, c : a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \rangle$;

- $Q_8 \times \mathbb{Z}_3$ and $Q_8 \times \mathbb{Z}_4$.

In this thesis, we focus on Cayley graphs on groups that have only affine automorphisms. One situation where this is definitely true is when the group has a GRR, which we explore further in Chapter 5. Thus, we do not need to worry about those groups. Instead, we focus on groups that do not have a GRR, which we will discuss in Chapter 6.

We now give the formal definition of the Cayley index, which was introduced briefly in Chapter 1.

Definition 3.2.4 ([28, Definition 1.1]). The *Cayley index* $c(\Gamma)$ of a Cayley graph Γ is defined as $|\text{Aut}(\Gamma) : L(G)|$, where $L(G)$ is the left regular representation of G . The Cayley index of a group G is denoted by $c(G)$ and equal to

$$\min_{S \subseteq G \setminus \{1\}, S=S^{-1}} \{c(\text{Cay}(G; S))\}.$$

So a Cayley graph Γ is a GRR if and only if its Cayley index $c(\Gamma) = 1$.

Definition 3.2.5 ([28, Definition 1.4]). Let G be a group and $\Gamma = \text{Cay}(G; S)$ be a Cayley graph on G then a Cayley graph with the smallest Cayley index is called an MRR (Most Rigid Representation) for G .

For groups that do not admit a GRR, we consider an MRR, which is a Cayley graph with the smallest possible automorphism group. The study of MRRs has been further developed by several researchers: Imrich and Watkins explored the structure of Cayley graphs and identified the significance of MRRs for groups that do not admit GRRs. They provided initial results on the minimal automorphism groups of these Cayley graphs and established early classification results for specific families of groups.

More recently, in [28], Morris and Tymurski extended the work on MRRs by providing a comprehensive classification of groups based on their Cayley indices. They

determined an MRR for various finite groups, completing the classification for those that do not admit GRRs.

In Chapter 6, we check some of the finite groups in Table 6.5, which is based on a similar table from [28], to confirm their Cayley index. First, we describe these groups, including their specific permutation representations and what they are isomorphic to. Then, we use Sage to find a generating set and show that using that generating set as a connection set produces an MRR.

We know that the automorphism group of every GRR consists only of affine maps. Now, consider the definition of a normal Cayley graph.

Definition 3.2.6 (cf. [33, Definition 1] and [15, Lemma 2.1]). A Cayley graph $\Gamma = \text{Cay}(G; S)$ is said to be *normal* if $L(G) \triangleleft \text{Aut}(\Gamma)$, where $L(G)$ is the left regular representation of G . A group G is said to have a normal Cayley graph if G has a subset S such that the Cayley graph $\Gamma = \text{Cay}(G; S)$ is normal.

Remark 3.2.7. A Cayley graph $\Gamma = \text{Cay}(G; S)$ is a normal Cayley graph if and only if every automorphism of the Cayley graph is affine [33, Lemma A].

Thus, every GRR corresponds to a normal Cayley graph.

In Table 6.5, we can see the Cayley index for each group. Our goal is to find Cayley graphs where all the automorphisms are affine, which is equivalent to identifying groups that have normal graphs. If a group has a GRR, its Cayley index is 1, and we are done. If the group has a Cayley index of 2, the left regular representation is a normal subgroup of index 2 in the automorphism group, so we are also done.

Thus, it is sufficient to focus on groups with a Cayley index greater than 2, excluding the infinite families $(Q_8 \times \mathbb{Z}_2^n)$. These groups are:

$\mathbb{Z}_2^3$	$\mathbb{Z}_2^4$
$\mathbb{Z}_4 \times \mathbb{Z}_2$	$\mathbb{Z}_4^2$
$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	$\mathbb{Z}_3^2$
$\mathbb{Z}_3^3$	$\text{Dic}(\mathbb{Z}_6, 3)$
$\text{Dic}(\mathbb{Z}_8, 4)$	$\text{Dic}(\mathbb{Z}_{10}, 5)$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$	

We ran a program in Sage for these groups and verified that they indeed have normal Cayley graphs, which we will discuss in more detail in Chapter 7.

Example 3.2.8. The Cayley index of the group $\mathbb{Z}_4 \times \mathbb{Z}_2$ is 6. Using Sage code in Appendix A.10, we determined that this group does not admit a normal Cayley graph.

Everything we have set up to this point provides an alternative proof of the following theorem.

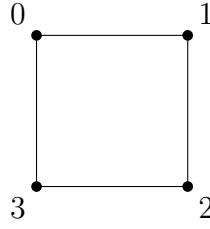
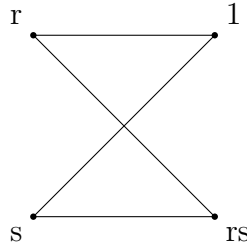
Theorem 3.2.9 (Wang, Wang, and Xu [33, Thm. 1]). *G has a Cayley graph that is normal Cayley graph if and only if G is not isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $Q_8 \times \mathbb{Z}_2^r$ for $r \geq 0$.*

3.3 The CCA Problem

Recall from Section 2.4 that every Cayley graph $\text{Cay}(G; S)$ has a natural edge-colouring in which the edge $\{g, gs\}$ has colour $\{s, s^{-1}\}$.

An automorphism is colour-preserving if it preserves each colour class, and colour-permuting if it permutes the colour classes. A Cayley graph is CCA if all of its colour-preserving automorphisms are affine, and it is strongly CCA if all of its colour-permuting automorphisms are affine.

Similarly, a group G is CCA, respectively strongly CCA, if every connected Cayley graph on G is CCA, respectively strongly CCA.


 Figure 3.4: $\text{Cay}(\mathbb{Z}_4; \{\pm 1\})$

 Figure 3.5: $\text{Cay}(D_4; \{r, s\})$

As noted in Lemma 2.4.8, every left translation is colour-preserving. Furthermore, if $\alpha \in \text{Aut}(G)$ satisfies $\alpha(s) \in \{s, s^{-1}\}$ for every $s \in S$, then α is also a colour-preserving automorphism of $\text{Cay}(G; S)$.

The CCA problem asks when these obvious affine colour-preserving automorphisms account for all colour-preserving automorphisms of a Cayley graph.

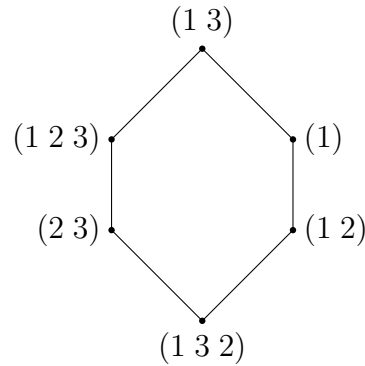
Remark 3.3.1. Since disconnected Cayley graphs will almost never be CCA-graphs, connectedness is important in this definition.

Next we are going to present some examples of CCA graphs and groups.

Example 3.3.2. • The Cayley graph $\text{Cay}(\mathbb{Z}_4; \{\pm 1\})$, which is a cycle of length 4, is CCA (see Figure 3.4).

• The Cayley graph $\text{Cay}(D_4; \{r, s\})$ where r is rotation and s is reflection is CCA (see Figure 3.5).

• The Cayley graph $\text{Cay}(S_3; \{(1\ 3), (1\ 2)\})$ is also CCA (see Figure 3.6).


 Figure 3.6: $\text{Cay}(S_3; \{(1\ 3), (1\ 2)\})$

- It is known that Q_8 and $\mathbb{Z}_4 \times \mathbb{Z}_2$ are not CCA groups [18, Example 2.2]; see also Figure 3.3.

$$\text{Cay}(Q_8; \{\pm i, \pm j\}) \cong \text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1, 0), \pm(1, 1)\}) \cong K_{4,4}$$

The colour-preserving and colour-permuting automorphisms of $\text{Cay}(G; S)$ are the automorphisms that respect the colour classes of $\text{Cay}(G; S)$.

A directed Cayley graph $\text{Cay}(G; S)$ has vertex set G and a directed edge (g, gs) for each $g \in G$ and $s \in S$. The edge (g, gs) is assigned the color s , which represents the group element that generates the edge.

By [37, Theorem 4-8], every colour-preserving automorphism of a directed Cayley graph $\text{Cay}(G; S)$ is a left translation.

In contrast, for undirected Cayley graphs, where edge colors are assigned as unordered pairs $\{s, s^{-1}\}$, the symmetry in coloring introduces the possibility of additional automorphisms that are not left translations. Thus, the theorem for directed Cayley graphs contrasts with the more complex situation of undirected graphs.

In [2], the authors explore the structure and properties of automorphisms in Cayley graphs, particularly focusing on those that permute the colors assigned to the edges. Hujdurović et al. [18] identifies several classes of groups that have the colour-preserving automorphism (CCA) property, meaning every colour-preserving automor-

phism is an affine map. They also determine the orders of all groups that do not have the CCA property. They provide examples of non-CCA groups and a general construction to generate more examples.

In a normal Cayley graph, we already know that $L(G) \triangleleft \text{Aut}(\Gamma)$. Consequently, they have only affine automorphisms, making them strongly CCA and therefore CCA.

In the following theorem you can find some main results of [18] about CCA groups.

Theorem 3.3.3 ([18, Theorem 1.3]). • *(Existence of Non-CCA Groups) There is a non-CCA group of order n if and only if $n \geq 8$ and n is divisible by either 4, 21, or a number of the form $p^q \cdot q$ where p, q are prime.*

- *(Abelian Groups) An abelian group is not CCA if and only if it has a direct factor that is isomorphic to either $\mathbb{Z}_4 \times \mathbb{Z}_2$ or a group of the form $\mathbb{Z}_{2^k} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with $k \geq 2$.*
- *(Odd Order Groups) Every non-CCA group of odd order has a section that is isomorphic to either the non-abelian group of order 21 or a certain generalization of a wreath product. (A section of a group G is a group that can be obtained as a quotient of a subgroup of G .)*
- *(Product Groups) For two groups G and H , if $G \times H$ is CCA then G and H are CCA. The converse is true when we have $\gcd(|G|, |H|) = 1$.*

Note that any strongly CCA group is CCA, since each colour-preserving automorphism is a colour-permuting automorphism. For converse we have the following theorem. (Conditions for a CCA group to also be strongly CCA.)

Theorem 3.3.4 ([18, Theorem 1.5]). *A CCA group is strongly CCA if either:*

- *it is abelian; or*
- *it has odd order.*

The abelian case is particularly important in the study of CCA Cayley graphs. For abelian groups, the obstruction to being CCA is closely related to elements of order 4. Hujdurović et al. [18, Theorem 1.3] proved that an abelian group is not CCA if and only if it has a direct factor isomorphic to either $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_{2^k} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, where $k \geq 2$. They also proved that, for abelian groups, the CCA property and the strongly CCA property are equivalent.

Chapter 4

Abelian groups

This chapter studies colour-preserving and colour-permuting automorphisms of Cayley graphs on abelian groups. Throughout the chapter, all groups are written additively. Thus, the identity element of a group is denoted by 0, the inverse of an element s is denoted by $-s$, and the group operation is written as addition.

We begin by showing that any change in the local permutation induced by a colour-permuting automorphism can occur only in a very restricted situation involving elements of order 4. More precisely, we prove that if

$$\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s), \text{ then } 2s = 2t \text{ and } |s| = |t| = 4.$$

We then use this result to characterize the connected abelian Cayley graphs that are CCA and strongly CCA. This characterization is expressed in terms of the subgroup generated by the set $T(S, 2s)$. Finally, we apply the characterization to Cayley graphs arising from two generators and determine precisely when such a graph is not CCA.

Theorem 4.0.1. *Assume G is abelian, φ is a colour-permuting automorphism of $\text{Cay}(G; S)$, $g \in G$ and $s, t \in S$. If $\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s)$, then $\pi_{g+t}^\varphi(s) = -\pi_g^\varphi(s)$, $\pi_{g+s}^\varphi(t) = -\pi_g^\varphi(t)$, and $t \notin \langle s \rangle$. Also, $2s = 2t$ and $|s| = |t| = 4$.*

Proof. We first show that $t \notin \langle s \rangle$. Suppose, for a contradiction, that $t \in \langle s \rangle$. Then $g+t \in g + \langle s \rangle$. By Lemma 2.5.2(6c), the value $\pi_h^\varphi(s)$ is constant on the coset $g + \langle s \rangle$, and hence

$$\pi_{g+t}^\varphi(s) = \pi_g^\varphi(s),$$

contradicting the assumption that $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$. Therefore $t \notin \langle s \rangle$.

For simplicity, let $\hat{s} = \pi_g^\varphi(s)$ and $\hat{t} = \pi_g^\varphi(t)$, so

$$\varphi(g + s) = \varphi(g) + \hat{s} \text{ and } \varphi(g + t) = \varphi(g) + \hat{t}.$$

Since φ is colour-permuting, by Lemma 2.5.2(4), we know

$$\pi_{g+t}^\varphi(s) \in \{\pi_g^\varphi(s), -\pi_g^\varphi(s)\} = \{\hat{s}, -\hat{s}\}.$$

Given $\pi_{g+t}^\varphi(s) \neq \hat{s}$, it follows that

$$\pi_{g+t}^\varphi(s) = -\hat{s}.$$

Therefore

$$\varphi(g + s + t) = \varphi(g + t + s) = \varphi(g + t) + \pi_{g+t}^\varphi(s) = \varphi(g + t) - \hat{s} = \varphi(g) + \hat{t} - \hat{s}.$$

Also,

$$\varphi(g + s + t) = \varphi(g + s) + \pi_{g+s}^\varphi(t) = \varphi(g) + \hat{s} + \pi_{g+s}^\varphi(t).$$

Furthermore, $\pi_{g+s}^\varphi(t) \in \{\pi_g^\varphi(t), -\pi_g^\varphi(t)\} = \{\hat{t}, -\hat{t}\}$.

Case 1. Assume $\pi_{g+s}^\varphi(t) = \hat{t}$. Then $\hat{t} - \hat{s} = \hat{s} + \hat{t}$, so $2\hat{s} = 0$. On the other hand, because of our assumption $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$, so $\hat{s} \neq -\hat{s}$. It means $2\hat{s} \neq 0$. This is a contradiction. So this case is impossible.

Case 2. Assume $\pi_{g+s}^\varphi(t) = -\hat{t}$. Then $\hat{t} - \hat{s} = \hat{s} - \hat{t}$, so $2\hat{s} = 2\hat{t}$. From this, we can show $2s = 2t$. To do that, we calculate

$$\begin{aligned}
\varphi(g + 2s) &= \varphi(g) + \tilde{\pi}_g^\varphi(2s) && (\text{definition of } \tilde{\pi}_g^\varphi) \\
&= \varphi(g) + 2\pi_g^\varphi(s) && (\varphi \in \mathcal{A}^0(\Gamma), \text{ Lemma 2.5.2(6d)}) \\
&= \varphi(g) + 2\hat{s} && (\pi_g^\varphi(s) = \hat{s}) \\
&= \varphi(g) + 2\hat{t} && (2\hat{s} = 2\hat{t}) \\
&= \varphi(g) + 2\pi_g^\varphi(t) && (\pi_g^\varphi(t) = \hat{t}) \\
&= \varphi(g) + \tilde{\pi}_g^\varphi(2t) && (\varphi \in \mathcal{A}^0(\Gamma), \text{ Lemma 2.5.2(6d)}) \\
&= \varphi(g + 2t) && (\text{definition of } \tilde{\pi}_g^\varphi).
\end{aligned}$$

So, we get $\varphi(g + 2s) = \varphi(g + 2t)$ by injectivity of φ , $2s = 2t$.

Now we calculate $\varphi(g - t)$ in 2 ways by using the fact that $-t = t - 2t$.

$$\varphi(g - t) = \varphi(g) + \pi_g^\varphi(-t) = \varphi(g) - \pi_g^\varphi(t) = \varphi(g) - \hat{t}.$$

Also,

$$\begin{aligned}
\varphi(g - t) &= \varphi(g + t - 2t) \\
&= \varphi(g + t - 2s) && (2t = 2s) \\
&= \varphi(g + t) + \tilde{\pi}_{g+t}^\varphi(-2s) && (\text{definition of } \tilde{\pi}_{g+t}^\varphi) \\
&= \varphi(g + t) + 2\pi_{g+t}^\varphi(-s) && (\varphi \in \mathcal{A}^0(\Gamma), \text{ Lemma 2.5.2(6d)}) \\
&= \varphi(g + t) - 2\pi_{g+t}^\varphi(s) && (\varphi \in \mathcal{A}^0(\Gamma), \text{ Lemma 2.5.2(6b)}) \\
&= \varphi(g + t) - 2(-\hat{s}) && (\pi_{g+t}^\varphi(s) = -\hat{s}) \\
&= \varphi(g + t) + 2\hat{s} \\
&= \varphi(g) + \pi_g^\varphi(t) + 2\hat{s} && (\text{definition of } \pi_g^\varphi) \\
&= \varphi(g) + \hat{t} + 2\hat{s}.
\end{aligned}$$

Therefore, from them we have $-\hat{t} = \hat{t} + 2\hat{s}$, so $-2\hat{t} = 2\hat{s}$. We had $2\hat{t} = 2\hat{s}$, then $4\hat{s} = 0$ and $4\hat{t} = 0$.

Now we show $4s = 0$ (then $4t = 2(2t) = 2(2s) = 4s = 0$).

$$\begin{aligned}
 \varphi(g + 4s) &= \varphi(g) + \tilde{\pi}_g^\varphi(4s) && \text{(definition of } \tilde{\pi}_g^\varphi) \\
 &= \varphi(g) + 4\pi_g^\varphi(s) && (\varphi \in \mathcal{A}^0(\Gamma), \text{ Lemma 2.5.2(6d)}) \\
 &= \varphi(g) + 4\hat{s} && (\hat{s} = \pi_g^\varphi(s)) \\
 &= \varphi(g) && (4\hat{s} = 0).
 \end{aligned}$$

So we get $\varphi(g + 4s) = \varphi(g)$ by injectivity of φ , $4s = 0$. We got $2s = 2t$, $4s = 4t = 0$.

Since $4s = 0$, then $|s| \in \{1, 2, 4\}$. Also, as mentioned above because of our assumption $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$, so $\hat{s} \neq -\hat{s}$. It means $2\hat{s} \neq 0$. Therefore, $|\hat{s}| > 2$. So $|s| > 2$, by Lemma 2.5.2(6a). So $|s| = 4$. Similarly, $|t| = 4$. $\square$

Corollary 4.0.2. *Assume φ is a colour-preserving automorphism of $\text{Cay}(G; S)$ (and S generates G), and suppose G is abelian. If $g \in G$ and $s, t \in S$, such that $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$, then $2s = 2t$ and $|s| = |t| = 4$, but $t \notin \langle s \rangle$. Also, $\pi_{g+t}^\varphi(s) = -\pi_g^\varphi(s)$ and $\pi_{g+s}^\varphi(t) = -\pi_g^\varphi(t)$.*

Proof. Since every colour-preserving automorphism is colour-permuting, the result follows from Theorem 4.0.1. $\square$

We will work on abelian Cayley graphs that are not strongly CCA.

Definition 4.0.3. Let G be an abelian group and $S \subseteq G$. For $c \in G$, define

$$T(S, c) := \{c\} \cup \{t \in S \mid 2t \neq c\}.$$

Lemma 4.0.4. *Assume $\Gamma = \text{Cay}(G; S)$ is connected, and G is abelian. Let φ be a colour-permuting automorphism of Γ and the letters s and t always represent elements of S .*

1. If $|s| = 4$, then $\pi_{g+t}^\varphi(s) = \pi_g^\varphi(s)$ for all $g \in G$ and all $t \in \{s\} \cup T(S, 2s)$.
2. If $|s| = 4$ and $\langle s, T(S, 2s) \rangle = G$, then $\pi_g^\varphi(s)$ is independent of g .

Proof. 1. Suppose, on the contrary, that $\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s)$ for some

$$t \in \{s\} \cup T(S, 2s) = \{s, 2s\} \cup \{t \in S \mid 2t \neq 2s\}.$$

By Lemma 2.5.2(6c), we have $t \notin \langle s \rangle$, so $t \notin \{s, 2s\}$. Therefore, $t \in S$ with $2t \neq 2s$.

This contradicts the fact that Theorem 4.0.1 says $2t = 2s$.

2. Let g, h be arbitrary elements of G . Since $\langle s, T(S, 2s) \rangle = G$, we have

$$h = g + s_1 + s_2 + \cdots + s_n$$

where $s_i \in \{s\} \cup T(S, 2s)$ for all i .

Since $|s| = 4$, we know from part 1, that for all $x \in G$ and all $t \in \{s\} \cup T(S, 2s)$, we have $\pi_{x+t}^\varphi(s) = \pi_x^\varphi(s)$. Then we have

$$\pi_h^\varphi(s) = \pi_{g+s_1+s_2+\cdots+s_n}^\varphi(s) = \pi_{g+s_1+s_2+\cdots+s_{n-1}}^\varphi(s) = \cdots = \pi_{g+s_1}^\varphi(s) = \pi_g^\varphi(s). \quad \square$$

Theorem 4.0.5. Assume $\text{Cay}(G; S)$ is connected. If G is abelian, then the following are equivalent:

1. $\text{Cay}(G; S)$ is strongly CCA.
2. $\text{Cay}(G; S)$ is CCA.
3. $|G : \langle T(S, 2s) \rangle| \leq 2$ for all $s \in S$ with $|s| = 4$.

Proof. (1 $\Rightarrow$ 2). It is obvious.

(2 $\Rightarrow$ 3). This implication is a special case of [18, Proposition 2.5]. For completeness, we provide a direct proof. We prove the contrapositive. Suppose that there is

$s \in S$ with $|s| = 4$ such that $|G : \langle T(S, 2s) \rangle| > 2$. Set $c = 2s$, so c has order 2. Since $|G : \langle T(S, c) \rangle| > 2$, we have $G \neq \langle T(S, c) \rangle$.

Define $\varphi_c^S : G \rightarrow G$ by

$$\varphi_c^S(x) = \begin{cases} x + c & \text{if } x \in \langle T(S, c) \rangle, \\ x & \text{otherwise.} \end{cases}$$

By Lemma 2.2.6, φ_c^S is a bijection. Also, since $|G : \langle T(S, c) \rangle| > 2$, the coset $\langle T(S, c) \rangle$ has size less than $|G|/2$, so φ_c^S fixes more than half of the elements of G , and it is not the identity map. So, by Lemma 2.2.5, φ_c^S is not affine. Therefore, it suffices to show φ_c^S is colour-preserving. Then $\text{Cay}(G; S)$ has a colour-preserving automorphism that is not affine, and hence $\text{Cay}(G; S)$ is not CCA, a contradiction.

To complete the proof we now show that φ_c^S is colour-preserving on $\text{Cay}(G; S)$. So we need to show that for all $x \in G$ and $s \in S$,

$$\varphi_c^S(x + s) = \varphi_c^S(x) \pm s$$

We have the following cases:

Case 1. Assume $x \notin \langle T(S, c) \rangle$ and $x + s \notin \langle T(S, c) \rangle$.

Then $\varphi_c^S(x) = x$ and $\varphi_c^S(x + s) = x + s$, so

$$\varphi_c^S(x + s) = x + s = \varphi_c^S(x) + s.$$

Case 2. Assume $x \in \langle T(S, c) \rangle$ and $x + s \in \langle T(S, c) \rangle$.

Then $\varphi_c^S(x) = x + c$ and $\varphi_c^S(x + s) = x + s + c$. Hence

$$\varphi_c^S(x + s) = x + s + c = x + c + s = \varphi_c^S(x) + s.$$

Case 3. Assume $x \in \langle T(S, c) \rangle$ but $x + s \notin \langle T(S, c) \rangle$.

Since $x \in \langle T(S, c) \rangle$, if $s \in \langle T(S, c) \rangle$, then $x + s \in \langle T(S, c) \rangle$, since $\langle T(S, c) \rangle$ is a subgroup. This contradicts our assumption. Hence $s \notin \langle T(S, c) \rangle$.

Now if $2s \neq c$, then $s \in T(S, c) \subseteq \langle T(S, c) \rangle$, a contradiction. Hence we must have $2s = c$.

Now $\varphi_c^S(x) = x + c$ and $\varphi_c^S(x + s) = x + s$, so using $2s = c$ we obtain

$$\varphi_c^S(x + s) = x + s = x + 2s - s = x + c - s = \varphi_c^S(x) - s.$$

Case 4. Assume $x \notin \langle T(S, c) \rangle$ but $x + s \in \langle T(S, c) \rangle$.

Since $x + s \in \langle T(S, c) \rangle$, if $s \in \langle T(S, c) \rangle$, then

$$x = (x + s) - s \in \langle T(S, c) \rangle,$$

since $\langle T(S, c) \rangle$ is a subgroup. This contradicts our assumption. Hence $s \notin \langle T(S, c) \rangle$.

Now if $2s \neq c$, then $s \in T(S, c) \subseteq \langle T(S, c) \rangle$, a contradiction. Hence we must have $2s = c$.

Now $\varphi_c^S(x) = x$ and $\varphi_c^S(x + s) = x + s + c$, so using $2s = c$ and $|s| = 4$, we obtain

$$\varphi_c^S(x + s) = x + s + c = x + s + 2s = x + 3s = x - s = \varphi_c^S(x) - s.$$

(3 $\Rightarrow$ 1). We prove by contradiction. Suppose $\text{Cay}(G; S)$ is not strongly CCA. Then there is a colour-permuting automorphism φ that is not affine. By Corollary 2.5.4, since $\text{Cay}(G; S)$ is connected and φ is not affine, there exist $g \in G$ and $s, t \in S$, such that $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$. Then by Theorem 4.0.1, we must have $|s| = 4$.

We claim that when $|s| = 4$ and $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$ then $s \notin \langle T(S, 2s) \rangle$.

Suppose on the contrary that $s \in \langle T(S, 2s) \rangle$ and $\pi_{g+t}^\varphi(s) \neq \pi_g^\varphi(s)$. By Theo-

rem 4.0.1 we have

$$\pi_{g+s}^\varphi(t) = -\pi_g^\varphi(t) \text{ and } |s| = |t| = 4 \quad (4.0.6)$$

and $2t = 2s$. Thus, $T(S, 2s) = T(S, 2t)$. Applying Lemma 4.0.4(1) for t , we have for all $u \in \{t\} \cup T(S, 2t)$,

$$\pi_{g+u}^\varphi(t) = \pi_g^\varphi(t).$$

Since $s \in \langle T(S, 2s) \rangle = \langle T(S, 2t) \rangle$, there are $u_1, u_2, \dots, u_k \in T(S, 2t)$, such that

$$s = u_1 + u_2 + \dots + u_k.$$

Thus,

$$\begin{aligned} \pi_{g+s}^\varphi(t) &= \pi_{g+u_1+u_2+\dots+u_{k-1}+u_k}^\varphi(t) \\ &= \pi_{g+u_1+u_2+\dots+u_{k-1}}^\varphi(t) \\ &\vdots \\ &= \pi_{g+u_1}^\varphi(t) \\ &= \pi_g^\varphi(t). \end{aligned}$$

Therefore,

$$\pi_g^\varphi(t) = \pi_{g+s}^\varphi(t) = -\pi_g^\varphi(t) \quad \text{by (4.0.6)}$$

Then by Lemma 2.5.2(6b) $\pi_g^\varphi(t) = -\pi_g^\varphi(t) = \pi_g^\varphi(-t)$. Since π_g^φ is a bijection, we must have $t = -t$, or equivalently, $2t = 0$, a contradiction since $|t| = 4$.

Since $s \notin \langle T(S, 2s) \rangle$ and $|G : \langle T(S, 2s) \rangle| \leq 2$, this implies that $|G : \langle T(S, 2s) \rangle| = 2$.

Since $|G : \langle T(S, 2s) \rangle| = 2$ and $s \notin \langle T(S, 2s) \rangle$, then we have two cosets: $\langle T(S, 2s) \rangle$ and $s + \langle T(S, 2s) \rangle$ therefore,

$$G = \langle T(S, 2s) \rangle \cup (s + \langle T(S, 2s) \rangle) \subseteq \langle s, T(S, 2s) \rangle.$$

Thus $\langle s, T(S, 2s) \rangle = G$.

Therefore by Lemma 4.0.4(2), $\pi_g^\varphi(s)$ is independent of g . This contradicts the assumption that $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$.

Therefore, $\text{Cay}(G; S)$ is strongly CCA. $\square$

Corollary 4.0.7. *Let G be abelian group with two generators a and b . Then the Cayley graph $\Gamma = \text{Cay}(G; \{\pm a, \pm b\})$ is not CCA if and only if $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ and $|\bar{a}| = |\bar{b}| = 4$.*

Proof. ($\Rightarrow$). Let $\Gamma = \text{Cay}(G; \{\pm a, \pm b\})$ be non-CCA. Then there exists a colour-preserving automorphism φ that is not affine. By Corollary 2.5.4, there exists $s, t \in \{\pm a, \pm b\}$ and $g \in G$ with $\pi_g^\varphi(s) \neq \pi_{g+t}^\varphi(s)$. So, Corollary 4.0.2 implies that $2a = 2b$, $|a| = |b| = 4$, and $a \notin \langle b \rangle$. The only abelian group with two generators satisfying these conditions is $\mathbb{Z}_4 \times \mathbb{Z}_2$.

($\Leftarrow$). Let $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. The elements of order 4 in G are $\{\pm(1, 0), \pm(1, 1)\}$. There is only one generating set $\{\pm a, \pm b\}$ with $|a| = |b| = 4$ that needs to be considered. We show that the Cayley graph $\Gamma = \text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; \{\pm(1, 0), \pm(1, 1)\})$ is not CCA.

For every $t \in S$ we have $2t = (2, 0)$, since

$$2(1, 0) = (2, 0), \quad 2(3, 0) = (2, 0), \quad 2(1, 1) = (2, 0), \quad 2(3, 1) = (2, 0).$$

Hence

$$T(S, 2s) = \{2s\} \cup \{t \in S \mid 2t \neq 2s\} = \{(2, 0)\}.$$

Therefore $\langle T(S, 2s) \rangle = \langle (2, 0) \rangle = \{(0, 0), (2, 0)\}$ has order 2, so

$$|G : \langle T(S, 2s) \rangle| = \frac{|G|}{2} = \frac{8}{2} = 4 > 2.$$

So, by Theorem 4.0.5, Γ is not CCA. $\square$

Chapter 5

Finite groups that do not have a GRR

Recall (see Definition 3.2.2). A Cayley graph $\text{Cay}(G; S)$ is a *GRR* (*Graphical Regular Representation*) if every automorphism of $\text{Cay}(G; S)$ is a left translation by an element of G ; that is, $\text{Aut}(\text{Cay}(G; S)) = L(G)$.

We will see in Example 5.2.2 and Example 5.2.3 that certain abelian groups and certain generalized dicyclic groups do not have a GRR. The following theorem, which was already mentioned in Theorem 3.2.3 shows there are only 13 other finite groups that do not have a GRR.

Theorem 5.0.1 (Godsil, Hetzel, Imrich, Nowitz, and Watkins; see [14, pp. 222-223]). *The following are the only finite groups that are neither generalized dicyclic nor abelian of exponent greater than 2, yet admit no GRR:*

- $\mathbb{Z}_2^2, \mathbb{Z}_2^3, \mathbb{Z}_2^4$;
- D_6, D_8, D_{10} where these represent the dihedral groups of orders 6, 8, and 10 (respectively);
- A_4 the alternating group of degree 4;
- $H_1 = \langle a, b, c : a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle$;
- $H_2 = \langle a, b : a^8 = b^2 = 1, bab = a^5 \rangle$;

- $H_3 = \langle a, b, c : a^3 = b^3 = c^2 = 1, ab = ba, (ac)^2 = (bc)^2 = e \rangle;$
- $H_4 = \langle a, b, c : a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \rangle;$
- $Q_8 \times \mathbb{Z}_3, Q_8 \times \mathbb{Z}_4$ where Q_8 is the quaternion group of order 8.

We will prove only one direction of Theorem 5.0.1: we will verify in Chapter 6 that none of the 13 groups have a GRR (see Corollary 6.0.2). The proof of the other direction is much longer. As an illustration of the methods used to prove this other direction, we will prove in Section 5.1 that $\mathbb{Z}_2^n$ has a GRR if and only if $n \notin \{2, 3, 4\}$.

Groups given by generators and relations are hard to understand, so the end of this chapter will give a concrete description of the groups H_1 , H_2 , H_3 , and H_4 . (See sections 5.3A to 5.3D.)

Lemma 5.0.2 ([23, Lemma 5.2]). *A Cayley graph $\text{Cay}(G; S)$ is a GRR if and only if every automorphism φ of $\text{Cay}(G; S)$ that fixes the identity element satisfies $\varphi(g) = g$ for all $g \in G$.*

Proof. Let $\Gamma = \text{Cay}(G; S)$.

($\Rightarrow$). Suppose that Γ is a GRR. Then every automorphism of Γ is a left translation; that is, $\text{Aut}(\Gamma) = \{\ell_g \mid g \in G\}$, where $\ell_g(h) = gh$ for all $h \in G$.

Now suppose $\varphi \in \text{Aut}(\Gamma)$ and $\varphi(\mathbf{1}) = \mathbf{1}$. Since all automorphisms are of the form ℓ_g , we must have $\varphi = \ell_g$ for some $g \in G$. But then

$$\mathbf{1} = \varphi(\mathbf{1}) = \ell_g(\mathbf{1}) = g,$$

so $g = \mathbf{1}$ and $\varphi = \ell_{\mathbf{1}} = \text{id}$. Therefore, $\varphi(g) = g$ for all $g \in G$.

($\Leftarrow$). Conversely, suppose that every automorphism $\varphi \in \text{Aut}(\Gamma)$ with $\varphi(\mathbf{1}) = \mathbf{1}$ is the identity.

Let $\varphi \in \text{Aut}(\Gamma)$ be arbitrary, and define $g := \varphi(\mathbf{1})$. Consider the composition

$\psi := \ell_{g^{-1}} \circ \varphi$. Then

$$\psi(\mathbf{1}) = \ell_{g^{-1}}(\varphi(\mathbf{1})) = \ell_{g^{-1}}(g) = g^{-1}g = \mathbf{1},$$

so $\psi \in \text{Aut}(\Gamma)$ and $\psi(\mathbf{1}) = \mathbf{1}$. By hypothesis, $\psi = \text{id}$, so

$$\varphi = \ell_g.$$

Hence, every automorphism of Γ is a left translation, and so Γ is a GRR. $\square$

Proposition 5.0.3. *Every Cayley graph that is a GRR is also normal.*

Proof. Let $\Gamma = \text{Cay}(G; S)$ be a Cayley graph that is a GRR, i.e., $\text{Aut}(\Gamma) = L(G)$. So all automorphisms of Γ are left translations. Since left translations are affine maps (we can assume $\alpha = \text{id}_G$ in the definition of affine map) it follows that every automorphism of Γ is affine, so Γ is normal by definition. $\square$

5.1 Elementary abelian 2-groups that have a GRR

We will prove a complete characterization of elementary abelian 2-groups that have a GRR in this section.

Theorem 5.1.1 (Imrich [19, 20]; corrected by Alspach et al. in [22]). *$\mathbb{Z}_2^n$ has a GRR if and only if $n \notin \{2, 3, 4\}$.*

(The construction in [20] for $n = 5$ was later shown to be incorrect. A corrected construction appears in [22].)

Our proof of this theorem has three different parts. First, we show that the groups $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, and $\mathbb{Z}_2^4$ do not admit a GRR. This is known by Theorem 5.0.1, and we provide a proof in Corollary 6.0.2.

In Theorem 5.1.4 we verify by using a computer that $\mathbb{Z}_2^n$ admits a GRR for $n = 1, 5, 6$, and 7 . In Theorem 5.1.5, we prove that $\mathbb{Z}_2^n$ admits a GRR for every $n \geq 8$.

Lemma 5.1.2 (cf. Imrich [19, proof of Satz 3]). *Let $\Gamma = \text{Cay}(G; S)$ be connected. If the induced subgraph $\Gamma[S]$ has no nontrivial automorphism, then Γ is a GRR. ($\Gamma[S]$ denotes the graph whose vertex set is S , where two elements $s, t \in S$ are adjacent in $\Gamma[S]$ exactly when they are adjacent in Γ .)*

Proof. Let $A = \text{Aut}(\Gamma)$. Consider the action $A \times G \rightarrow G$. Let

$$A_1 = \text{Stab}_A(\mathbf{1}_G) = \{\varphi \in A \mid \varphi(\mathbf{1}_G) = \mathbf{1}_G\}$$

be the stabilizer of the identity.

In a Cayley graph $\Gamma = \text{Cay}(G; S)$ the neighbors of $\mathbf{1}_G$ are exactly the elements of S . Thus, $\Gamma[S]$ is the subgraph induced by the neighborhood of $\mathbf{1}_G$. Any $\varphi \in A_1$ must map neighbors of $\mathbf{1}_G$ to neighbors of $\mathbf{1}_G$, so φ induces an automorphism of $\Gamma[S]$. Therefore, we get a homomorphism $\theta : A_1 \rightarrow \text{Aut}(\Gamma[S])$ by $\theta(\varphi) = \varphi|_S$.

By hypothesis $\text{Aut}(\Gamma[S])$ is trivial, hence $\theta(\varphi)$ is the identity for every $\varphi \in A_1$. In particular,

$$\varphi(s) = s \quad \text{for all } s \in S \text{ and all } \varphi \in A_1.$$

We now prove that this forces φ to be the identity on the entire group G , which implies $A_1 = \{\text{id}\}$ then Γ is a GRR by Lemma 5.0.2. Assume, for contradiction, that φ is not the identity on G . So there is a $g \in G$ such that $\varphi(g) \neq g$. Since Γ is connected then there is a path from $\mathbf{1}$ to g in the Cayley graph:

$$\mathbf{1} \sim s_1 \sim s_1 s_2 \sim \cdots \sim s_1 s_2 \dots s_k = g.$$

Since $\varphi(g) \neq g$ we have $\varphi(s_1 s_2 \dots s_k) \neq s_1 s_2 \dots s_k$, so we may let i be the smallest positive integer for which

$$\varphi(s_1 s_2 \dots s_i) \neq s_1 s_2 \dots s_i \tag{5.1.3}$$

Define $h = s_1 s_2 \dots s_{i-1}$. By the minimality of i and $\varphi(\mathbf{1}) = \mathbf{1}$, we have $\varphi(h) = h$.

Consider the composition

$$\psi = \ell_{h^{-1}} \circ \varphi \circ \ell_h.$$

Then $\psi \in \text{Aut}(\Gamma)$ and

$$\psi(\mathbf{1}) = \ell_{h^{-1}} \circ \varphi \circ \ell_h(\mathbf{1}) = (\ell_{h^{-1}} \circ \varphi)(h) = \ell_{h^{-1}}(\varphi(h)) = h^{-1}h = \mathbf{1},$$

so $\psi \in A_1$. Therefore, we know from above $\psi(s) = s$ for all $s \in S$. In particular, $\psi(s_i) = s_i$. Therefore,

$$s_1 s_2 \cdots s_{i-1} s_i = h s_i = h \psi(s_i) = h \ell_{h^{-1}} \circ \varphi \circ \ell_h(s_i) = \varphi(h s_i) = \varphi(s_1 s_2 \cdots s_{i-1} s_i).$$

this contradicts (5.1.3).

Therefore, A_1 contains only the identity automorphism. So by Lemma 5.0.2, Γ is a GRR. $\square$

Theorem 5.1.4 ([20]). $\mathbb{Z}_2^n$ for $n = 1, 5, 6$, and 7 has a GRR.

Proof. The program in Appendix A.2 computes the Cayley index of Cayley graphs $\text{Cay}(\mathbb{Z}_2^n; S)$ for randomly generated nonempty connection sets $S \subseteq \mathbb{Z}_2^n \setminus \{0\}$, where $n = 1, 5, 6$, and 7 . In each case, the program finds a set S for which the Cayley index is 1. The corresponding connection sets have sizes 1, 18, 32, and 52, respectively. Since these sets are quite large, we do not list them explicitly. $\square$

Theorem 5.1.5 (Imrich [19, Satz 3]). $\mathbb{Z}_2^n$ for $n \geq 8$ has a GRR.

Proof (cf. [19]). Let $S_1 = \{e_1, e_2, \dots, e_n\}$ be the set of standard generators of $\mathbb{Z}_2^n$,

$$S_2 = \{e_4 + e_1, e_4 + e_n, e_3 + e_6\},$$

and

$$S_3 = \{e_1 + e_2, e_2 + e_3, \dots, e_{n-1} + e_n\}.$$

Now let

$$S = S_1 \cup S_2 \cup S_3.$$

Consider $\Gamma = \text{Cay}(\mathbb{Z}_2^n; S)$. We show that $\Gamma[S]$ the induced subgraph of Γ by S , is asymmetric, that is $\text{Aut}(\Gamma[S])$ is trivial, and so by Lemma 5.1.2, Γ is a GRR.

Since $e_i + e_j \notin S_1$ we have $e_i \sim e_j$ if and only if $e_i + e_j \in S_2 \cup S_3$, so $\Gamma[S_1]$ is the graph in Figure 5.1 with vertex set S_1 and edge set $E = \{e_i e_j \mid e_i + e_j \in S_2 \cup S_3\}$.

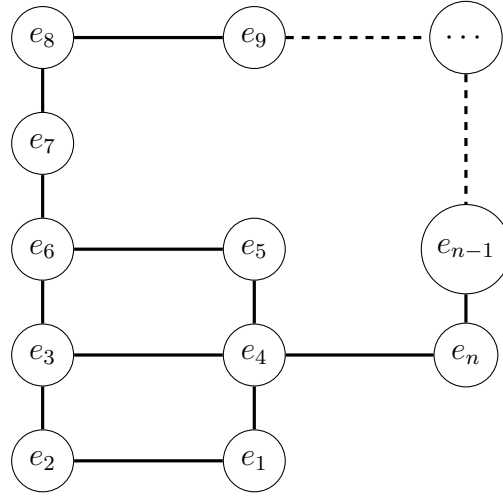


Figure 5.1: The graph $\Gamma[S_1]$ with vertex set S_1 and edges $E = \{e_i e_j : e_i + e_j \in S_2 \cup S_3\}$

We claim that $\Gamma[S_1]$ is asymmetric. Let $\varphi \in \text{Aut}(\Gamma[S_1])$. We will show that φ fixes every vertex of $\Gamma[S_1]$.

- e_4 is the only vertex in the graph that has degree 4.
- e_3 is the only neighbor of e_4 that has degree 3 (the rest have degree 2).
- e_6 is the only neighbor of e_3 that has degree 3.
- e_2 is the only neighbor of e_3 that has degree 2.
- e_5 is the only common neighbor of e_4 and e_6 that has degree 2.
- e_1 is the only common neighbor of e_2 and e_4 that has degree 2.

- finally, for $i = 7, 8, \dots, n$ we see by induction that e_i is fixed, because it is the only neighbor of e_{i-1} that is not already known to be fixed.

Thus, every vertex of $\Gamma[S_1]$ is fixed by φ , and therefore φ is the identity automorphism. Therefore, $\Gamma[S_1]$ does not have any non-trivial automorphisms.

Now we will show $\Gamma[S]$ is the graph in Figure 5.2, where the black vertices represent elements of $S_2 \cup S_3$.

1. We already know $\Gamma[S_1]$ is the graph in the Figure 5.1.
2. We prove each black vertex $e_i + e_j \in S_2 \cup S_3$ is adjacent to the endpoints e_i and e_j of the edge $e_i e_j$, and to no other vertices of $\Gamma[S_1]$.
 - We have $(e_i + e_j) + e_i = e_j \in S$ and $(e_i + e_j) + e_j = e_i \in S$. So $(e_i + e_j) \sim e_i$ and $(e_i + e_j) \sim e_j$.
 - Conversely, if $(e_i + e_j) \sim e_k$ then $e_i + e_j + e_k \in S$. Since $\text{Cay}(\mathbb{Z}_2^n; S_1)$ is bipartite it is clear from the definition of S_1 , S_2 , and S_3 that $e_i + e_j + e_k \notin S_2 \cup S_3$, so $e_i + e_j + e_k \in S_1$. This implies that $i = k$ or $j = k$.
3. Finally, we prove there are no edges between black vertices. If $(e_i + e_j) \sim (e_k + e_\ell)$ then $(e_i + e_j) + (e_k + e_\ell) \in S$. Since $\text{Cay}(\mathbb{Z}_2^n; S_1)$ is bipartite it is clear from the definition of S_1 , S_2 , and S_3 that $e_i + e_j + e_k + e_\ell \notin S_1$, so $e_i + e_j + e_k + e_\ell \in S_2 \cup S_3$. This implies that $\{i, j\} \cap \{k, \ell\} \neq \emptyset$. Without loss of generality we may assume that $j = \ell$. This means $e_i + e_k \in S_2 \cup S_3$, so $e_i \sim e_k \in \Gamma[S_1]$. But also since $e_i + e_j \in S$ and $e_k + e_j = e_k + e_\ell \in S$ we know $e_i \sim e_j$ and $e_k \sim e_j$. This contradicts the fact that the graph in Figure 5.1, does not have a triangle.

We now know $\Gamma[S]$ is the graph in Figure 5.2. Let φ be an arbitrary automorphism of $\Gamma[S]$, we have that $\varphi(S_1) = S_1$ because S_1 consists of precisely the vertices that have degree bigger than 2. Therefore, $\varphi|_{S_1}$ is an automorphism of $\Gamma[S_1]$, so $\varphi|_{S_1} = id$ since $\Gamma[S_1]$ is asymmetric.

Also for $e_i + e_j \in S_2 \cup S_3$, we have $\varphi(e_i + e_j) = e_i + e_j$ because $e_i + e_j$ is the only common neighbor of e_i and e_j and both e_i and e_j are fixed by φ . Thus, φ is the identity. Consequently, $\text{Aut}(\Gamma[S]) = \{\text{id}\}$. $\square$

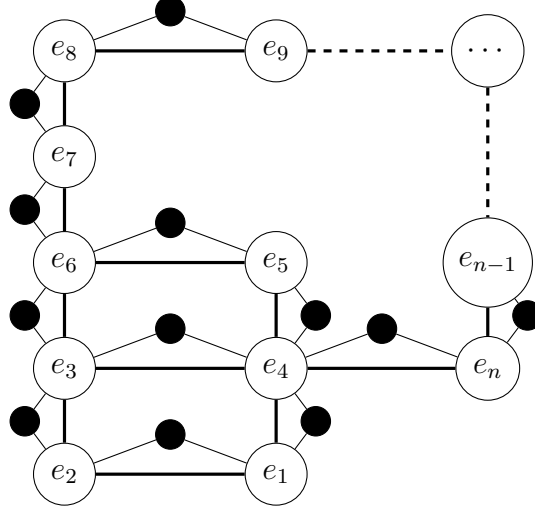


Figure 5.2: $\Gamma[S]$: The black vertex adjacent to e_i and e_j is $e_i + e_j$

5.2 Infinite families of groups that do not have a GRR

Lemma 5.2.1 ([10, p. 372]). *Let G be an abelian group. Then $\varphi(x) = x^{-1}$ is an automorphism of the Cayley graph $\Gamma = \text{Cay}(G; S)$.*

Proof. Suppose $g, h \in V(\Gamma)$ such that $g \sim h$. Then $g^{-1}h \in S$. We now compute:

$$\varphi(g)^{-1}\varphi(h) = (g^{-1})^{-1}h^{-1} = gh^{-1} = h^{-1}g = (g^{-1}h)^{-1} \in S^{-1} = S.$$

Thus, $\varphi(g) \sim \varphi(h)$, and therefore φ is an automorphism of Γ . $\square$

Example 5.2.2 ([10, p. 372]). If G is an abelian group and the exponent of G is greater than 2 (i.e., G is not an elementary abelian 2-group), then G does not have a GRR.

Proof. Suppose $\Gamma = \text{Cay}(G; S)$ is a GRR. (This will lead to a contradiction.) Let $\varphi(x) = x^{-1}$ for all $x \in G$. By Lemma 5.2.1, we know that $\varphi \in \text{Aut}(\Gamma)$, and it is obvious that $\varphi(\mathbf{1}) = \mathbf{1}$.

Now, since Γ is a GRR, we know $\varphi = \text{id}$ (the identity automorphism). Then for every $x \in G$ we have $\varphi(x) = \text{id}(x)$, which means $x^{-1} = x$. Therefore, $|x| \leq 2$, but the exponent of G is greater than 2, which is a contradiction.

Hence, G does not have a GRR. $\square$

Example 5.2.3 ([10, p. 372]). If $G = \text{Dic}(A, z)$ is a generalized dicyclic group, then G does not have a GRR.

Proof. Suppose, for contradiction, that G admits a GRR. Then there exists a subset $S \subseteq G \setminus \{\mathbf{1}\}$ such that $\Gamma = \text{Cay}(G; S)$ is a GRR. By Proposition 5.0.3, every GRR is CCA, so Γ is CCA.

Since $S \subseteq G \setminus \{\mathbf{1}\}$, we know from Lemma 2.4.8(7) that the complete Cayley graph $\text{Cay}(G; G \setminus \{\mathbf{1}\})$ is also CCA.

However, by Theorem 8.1.2, if G is generalized dicyclic, then the complete Cayley graph $\text{Cay}(G; G \setminus \{\mathbf{1}\})$ admits a nontrivial colour-preserving automorphism fixing the identity, and hence is not CCA. This is a contradiction.

Therefore G does not admit a GRR. $\square$

5.3 Groups given by generators and relations

5.3A The group H_1

In order to provide an explicit description of H_1 , we first establish some facts related to the group Q_8 .

Lemma 5.3.1. *In Q_8 , if $i^{m_1}j^{n_1} = i^{m_2}j^{n_2}$, then*

$$m_1 \equiv m_2 \pmod{2} \quad \text{and} \quad n_1 \equiv n_2 \pmod{2}.$$

Proof. We know

$$Z(Q_8) = \langle -1 \rangle = \{1, -1\}.$$

Since $Z(G)$ is a normal subgroup in any group, we conclude that:

$$\langle -1 \rangle \triangleleft Q_8.$$

So we can consider the quotient $\overline{Q_8} = Q_8 / \langle -1 \rangle = \{\bar{1}, \bar{i}, \bar{j}, \bar{k}\}$.

Since $\overline{Q_8}$ is a group of order 4 and is generated by two elements of order two $\bar{i}$ and $\bar{j}$ so it is an abelian group so we have

$$\overline{Q_8} = \langle \bar{i} \rangle \times \langle \bar{j} \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Now assume that $i^{m_1} j^{n_1} = i^{m_2} j^{n_2}$ in Q_8 . So the equality is true in $\overline{Q_8}$:

$$\bar{i}^{m_1} \bar{j}^{n_1} = \bar{i}^{m_2} \bar{j}^{n_2}.$$

Since $\overline{Q_8}$ is abelian, we can rearrange the terms:

$$\bar{i}^{m_1 - m_2} = \bar{j}^{n_1 - n_2}.$$

Since $\overline{Q_8} = \langle \bar{i} \rangle \times \langle \bar{j} \rangle$, we must have:

$$\bar{i}^{m_1 - m_2} = \bar{1} \quad \text{and} \quad \bar{j}^{n_1 - n_2} = \bar{1}.$$

Since the order of $\bar{i}$ is 2, we must have $m_1 - m_2$ even, and since the order of $\bar{j}$ is 2, we must have $n_1 - n_2$ even. This gives the desired congruences:

$$m_1 \equiv m_2 \pmod{2}, \quad n_1 \equiv n_2 \pmod{2}.$$

□

Lemma 5.3.2. *Define $\zeta : Q_8 \rightarrow \{\pm 1\}$ by $\zeta(i^m j^n) = (-1)^{m+n}$. Then*

1. ζ is a well-defined homomorphism, and
2. $\zeta(z) = 1$ for all $z \in Z(Q_8)$.

Proof. (1) We show that ζ is (a) well-defined and (b) a homomorphism.

(a) We need to show that if $i^{m_1} j^{n_1} = i^{m_2} j^{n_2}$ in Q_8 , then $\zeta(i^{m_1} j^{n_1}) = \zeta(i^{m_2} j^{n_2})$.

By Lemma 5.3.1, equality in Q_8 implies that:

$$m_1 + n_1 \equiv m_2 + n_2 \pmod{2}. \quad (5.3.3)$$

Therefore,

$$\begin{aligned} \zeta(i^{m_1} j^{n_1}) &= (-1)^{m_1+n_1} && \text{(definition of } \zeta) \\ &= (-1)^{m_2+n_2} && \text{(by Equation 5.3.3)} \\ &= \zeta(i^{m_2} j^{n_2}) && \text{(definition of } \zeta) \end{aligned}$$

This proves that ζ is well-defined.

For any two elements $i^{m_1} j^{n_1}$ and $i^{m_2} j^{n_2}$ in Q_8 , we have:

$$\begin{aligned} (i^{m_1} j^{n_1})(i^{m_2} j^{n_2}) &= i^{m_1} j^{n_1} i^{m_2} j^{n_2} \\ &= i^{m_1} (-1)^{m_2 n_1} i^{m_2} j^{n_1+n_2} && \text{(Using the relations } j^n i^m = (-1)^{mn} i^m j^n) \\ &= (-1)^{m_2 n_1} i^{m_1+m_2} j^{n_1+n_2} \\ &= i^{2m_2 n_1} i^{m_1+m_2} j^{n_1+n_2} && \text{(since } -1 = i^2) \\ &= i^{2m_2 n_1 + m_1 + m_2} j^{n_1+n_2} \end{aligned}$$

Applying ζ , we get:

$$\begin{aligned}
 \zeta(i^{m_1} j^{n_1} i^{m_2} j^{n_2}) &= \zeta(i^{2m_2n_1+m_1+m_2} j^{n_1+n_2}) \\
 &= (-1)^{2m_2n_1+m_1+m_2+n_1+n_2} && \text{(definition of } \zeta) \\
 &= (-1)^{m_1+m_2+n_1+n_2} && \text{(since } (-1)^{2m_2n_1} = 1) \\
 &= (-1)^{m_1+n_1} (-1)^{m_2+n_2} \\
 &= \zeta(i^{m_1} j^{n_1}) \zeta(i^{m_2} j^{n_2})
 \end{aligned}$$

Hence, ζ is a homomorphism.

2. We have

$$\zeta(-1) = \zeta(i^2 j^0) = (-1)^{2+0} = 1.$$

Since the center of Q_8 is $Z(Q_8) = \langle -1 \rangle$, this implies $\zeta(z) = 1$ for all $z \in Z(Q_8)$. $\square$

Lemma 5.3.4. *Suppose G is finite and $\zeta : G \rightarrow Z(G)$ is a homomorphism, such that $\zeta(z) = \mathbf{1}_G$ for all $z \in Z(G)$. If we define $\alpha : G \rightarrow G$ by $\alpha(g) = g \cdot \zeta(g)$, then*

1. α is an automorphism of G , and

2. $\alpha^n = \mathbf{1}$, where $n = |Z(G)|$.

Proof. (1) We first verify that α preserves the group operation. For any $g, h \in G$, we compute:

$$\begin{aligned}
 \alpha(gh) &= (gh) \cdot \zeta(gh) && \text{(by definition of } \alpha) \\
 &= (gh) \cdot \zeta(g)\zeta(h) && \text{(since } \zeta \text{ is a homomorphism)} \\
 &= g\zeta(g)h\zeta(h) && \text{(since } \zeta(g) \in Z(G), \text{ it commutes with } h) \\
 &= \alpha(g)\alpha(h) && \text{(by definition of } \alpha)
 \end{aligned}$$

Now, we show that α is injective. Let $g \in G$ such that $\alpha(g) = \mathbf{1}_G$. This implies:

$g\zeta(g) = \mathbf{1}_G$. Rearranging this equation, we get:

$$g = \zeta(g)^{-1}.$$

Since $\zeta(g) \in Z(G)$, it follows that $\zeta(g)^{-1} \in Z(G)$. Because $\zeta(g)^{-1} \in Z(G)$ by assumption $\zeta(\zeta(g)^{-1}) = \mathbf{1}_G$. Therefore, $\zeta(g) = \mathbf{1}_G$. Substituting this back into $g = \zeta(g)^{-1}$, we get $g = (\mathbf{1}_G)^{-1} = \mathbf{1}_G$. Hence, we conclude that:

$$\ker(\alpha) = \{\mathbf{1}_G\}.$$

We now know that α is injective, and since α is a homomorphism from finite group G to itself, injectivity implies surjectivity. Hence, α is an automorphism.

2. First let us prove by induction on k that

$$\alpha^k(g) = gz^k \text{ where } z = \zeta(g). \tag{5.3.5}$$

By the definition of α , we have:

$$\alpha(g) = g\zeta(g) = gz.$$

which establishes the base case where $k = 1$.

Assume that for some $k \geq 1$, we have $\alpha^k(g) = gz^k$. Then

$$\begin{aligned}
 \alpha^{k+1}(g) &= \alpha(\alpha^k(g)) \\
 &= \alpha(gz^k) && \text{(by the induction hypothesis)} \\
 &= (gz^k)\zeta(gz^k) && \text{(definition of } \alpha) \\
 &= (gz^k)\zeta(g)\zeta(z^k) && \text{(since } \zeta \text{ is a homomorphism)} \\
 &= (gz^k)\zeta(g)\zeta(z)^k && \text{(since } \zeta \text{ is a homomorphism)} \\
 &= (gz^k)z1_G && \text{(since } z = \zeta(g) \in Z(G), \text{ so } \zeta(z) = \mathbf{1}_G) \\
 &= gz^{k+1}
 \end{aligned}$$

We can now show $\alpha^n = \mathbf{1}$ where $n = |Z(G)|$:

$$\begin{aligned}
 \alpha^n(g) &= gz^n && \text{(by Equation 5.3.5)} \\
 &= g\zeta(g)^n && \text{(since } z = \zeta(g)) \\
 &= g\mathbf{1} && \text{(since } \zeta(g) \in Z(G), \text{ and } |Z(G)| = n \text{ then } \zeta(g)^n = \mathbf{1}) \\
 &= g.
 \end{aligned}$$

□

Lemma 5.3.6. *Define $\alpha: Q_8 \rightarrow Q_8$ by*

$$\alpha(i^m j^n) = (-1)^{m+n} i^m j^n,$$

for $m, n \in \mathbb{Z}$. Then α is a well-defined automorphism of Q_8 , and α^2 is the identity.

Proof. By using Lemma 5.3.2 and Lemma 5.3.4, α is a well-defined automorphism of Q_8 , and since $|Z(Q_8)| = 2$ so by part 2 of Lemma 5.3.4, $\alpha^2 = \mathbf{1}$. □

Theorem 5.3.7.

$$H_1 = \langle a, b, c \mid a^2 = b^2 = c^2 = 1, abc = bca = cab \rangle \cong Q_8 \rtimes_{\alpha} \mathbb{Z}_2,$$

where α is the automorphism of Q_8 defined in Lemma 5.3.6.

Proof. Let $H = Q_8 \rtimes_{\alpha} \mathbb{Z}_2$, and define $\hat{a} = (1, 1)$, $\hat{b} = (i, 1)$, and $\hat{c} = (j, 1)$. We claim that $H = \langle \hat{a}, \hat{b}, \hat{c} \rangle$.

We will show that $Q_8 \times \{0\} \subseteq H$.

Since $\hat{a} = (1, 1)$, we compute:

$$\hat{a}^2 = (1, 1)(1, 1) = (1 \cdot \alpha^1(1), 1 + 1) = (1 \cdot 1, 0) = (1, 0),$$

which is the identity in the $\mathbb{Z}_2$ -component.

Next, observe that $\hat{a}^{-1} = (\alpha^{-1}(1^{-1}), -1) = (1, 1)$, since $\alpha(1) = 1$ and $1^{-1} = 1$.

Thus:

$$\hat{b}\hat{a}^{-1} = (i, 1)(1, 1) = (i \cdot \alpha(1), 1 + 1) = (i, 0).$$

Similarly,

$$\hat{c}\hat{a}^{-1} = (j, 1)(1, 1) = (j \cdot \alpha(1), 1 + 1) = (j, 0).$$

Since $Q_8 = \langle i, j \rangle$, it follows that:

$$Q_8 \times \{0\} = \{(q, 0) \mid q \in Q_8\} \subseteq H.$$

We show that H contains all elements with second coordinate 1.

By definition, $\hat{a} = (1, 1)$, $\hat{b} = (i, 1)$, and $\hat{c} = (j, 1)$ are in H . Since $Q_8 \times \{0\} \subseteq H$, for any $q \in Q_8$, we have:

$$(q, 0)(1, 1) = (q \cdot \alpha^0(1), 0 + 1) = (q, 1).$$

Thus, H contains all elements of the form $(q, 1)$.

The group $Q_8 \rtimes_{\alpha} \mathbb{Z}_2$ has order $|Q_8| \cdot |\mathbb{Z}_2| = 16$. Since H contains:

- All 8 elements of $Q_8 \times \{0\}$,

- All 8 elements of $Q_8 \times \{1\}$,

it follows that $|H| \geq 16$. Therefore, $H = Q_8 \rtimes_{\alpha} \mathbb{Z}_2$.

Now let us verify that H satisfies the relations of H_1 :

- we check $\hat{a}^2 = \hat{b}^2 = \hat{c}^2 = \mathbf{1}_{Q_8 \rtimes \mathbb{Z}_2}$.

$$\hat{b}^2 = (i, 1)(i, 1) = (i \cdot \alpha^1(i), 1 + 1) = (i \cdot (-i), 0) = (1, 0).$$

$$\hat{c}^2 = (j, 1)(j, 1) = (j \cdot \alpha^1(j), 1 + 1) = (j \cdot (-j), 0) = (1, 0).$$

- To check $\hat{a}\hat{b}\hat{c} = \hat{b}\hat{c}\hat{a} = \hat{c}\hat{a}\hat{b}$, compute:

$$\begin{aligned} \hat{a}\hat{b}\hat{c} &= (1, 1)(i, 1)(j, 1) \\ &= (1 \cdot \alpha^1(i), 1 + 1)(j, 1) \\ &= (1 \cdot (-i), 0)(j, 1) \\ &= (-i, 0)(j, 1) \\ &= (-i \cdot \alpha^0(j), 0 + 1) \\ &= (-i \cdot j, 1) \\ &= (-k, 1). \end{aligned}$$

Similarly:

$$\begin{aligned}
 \hat{b}\hat{c}\hat{a} &= (i, 1)(j, 1)(1, 1) \\
 &= (i \cdot \alpha^1(j), 1 + 1)(0, 1) \\
 &= (i \cdot (-j), 0)(0, 1) \\
 &= (-k, 0)(1, 1) \\
 &= (-k \cdot \alpha^0(1), 1) \\
 &= (-k \cdot 1, 1) \\
 &= (-k, 1),
 \end{aligned}$$

and:

$$\begin{aligned}
 \hat{c}\hat{a}\hat{b} &= (j, 1)(1, 1)(i, 1) \\
 &= (j \cdot \alpha^1(1), 1 + 1)(i, 1) \\
 &= (j \cdot 1, 0)(i, 1) \\
 &= (j, 0)(i, 1) \\
 &= (j \cdot \alpha^0(i), 1) \\
 &= (j \cdot i, 1) \\
 &= (-k, 1).
 \end{aligned}$$

Therefore $\hat{a}$, $\hat{b}$ and $\hat{c}$ satisfy the relations in the definition of H_1 .

Now, we show $|H_1| \leq |H|$. We know $|H| = |Q_8 \rtimes \mathbb{Z}_2| = 16$. So we just need to show $|H_1| \leq 16$. Consider the subgroup generated by $\langle x \rangle$ where $x = ab$. We have

$$a \cdot x \cdot a = axa^{-1} = aaba^{-1} = ba^{-1} = ba = (ab)^{-1} = x^{-1}.$$

Similarity, $bx b^{-1} = x^{-1}$. Also, by definition of H_1 we have $abc = cab$ so $xc = cx$ which

means x and c commute. Therefore, the subgroup generated by $\langle x \rangle$ is normal in H_1 .

In the quotient group $\overline{H_1} = H_1/\langle x \rangle$, we know that $\bar{a} = \bar{b}$, because

$$a^{-1}b = ab = x \in \langle x \rangle.$$

By definition of H_1 we have $\bar{a}\bar{b}\bar{c} = \bar{b}\bar{c}\bar{a}$. Combining this with the facts that $\bar{a}^2 = 1$ and $\bar{a} = \bar{b}$, we see that

$$\bar{c} = \bar{a}^2\bar{c} = \bar{a}\bar{b}\bar{c} = \bar{b}\bar{c}\bar{a} = \bar{a}\bar{c}\bar{a}.$$

Since $\bar{a}^2 = 1$, this implies $\bar{a}\bar{c} = \bar{c}\bar{a}$.

Since $\bar{a}$ and $\bar{c}$ commute and both have order less than equal to 2, the quotient group $H_1/\langle x \rangle$ is an abelian group that is generated by two elements of order less than equal to 2 so $|H_1/\langle x \rangle| \leq 4$. Also, in the definition of H_1 we have the relation

$$abc = bca = cab. \tag{5.3.8}$$

By taking inverses in (5.3.8), we obtain

$$c^{-1}b^{-1}a^{-1} = a^{-1}c^{-1}b^{-1} = b^{-1}a^{-1}c^{-1}. \tag{5.3.9}$$

We have

$$\begin{aligned}
 (ab)^4 c &= ab \cdot ab \cdot ab \cdot (abc) \\
 &= ab \cdot ab \cdot ab \cdot (bca) && \text{(by Equation 5.3.8, } abc = bca) \\
 &= ab \cdot a(bac)a && (b^2 = 1) \\
 &= ab \cdot a(cba)a && \text{(by Equation 5.3.9, } bac = cba) \\
 &= ab(acb) && (a^2 = 1) \\
 &= ab(bac) && \text{(by Equation 5.3.9, } acb = bac) \\
 &= c && \text{(by definition } b^2 = 1, a^2 = 1)
 \end{aligned}$$

Therefore, $(ab)^4 = 1$ which means $|ab| \leq 4$. So, $|\langle ab \rangle| \leq 4$.

Now we can calculate the total order of H_1 as:

$$|H_1| = |\langle x \rangle| \times |H_1/\langle x \rangle| \leq 4 \times 4 = 16.$$

This completes the proof that $|H_1| \leq |H|$.

Since $|H_1| \leq 16$ so by Corollary 2.1.15 we can say $H_1 \cong H$. □

5.3B The group H_2

Theorem 5.3.10.

$$H_2 = \langle a, b : a^8 = b^2 = 1, bab = a^5 \rangle \cong \mathbb{Z}_8 \rtimes_{\psi} \mathbb{Z}_2,$$

where $\psi(n) = 5n$ for all $n \in \mathbb{Z}_8$.

Proof. Since $\gcd(5, 8) = 1$ it follows that ψ is an $\text{Aut}(\mathbb{Z}_8)$.

Let $H = \mathbb{Z}_8 \rtimes_{\psi} \mathbb{Z}_2$, so $H = \langle \hat{a}, \hat{b} \rangle$, where $\hat{a} = (1, 0)$ corresponding to the generator of $\mathbb{Z}_8$ and $\hat{b} = (0, 1)$ corresponding to the generator of $\mathbb{Z}_2$. Then

- $\hat{b}^2 = (0, 1) \cdot (0, 1) = (0 + \psi^1(0), 1 + 1) = (0 + 0, 0) = (0, 0)$.
- By induction on k we can say $\hat{a}^k = (k, 0)$ for all $k \geq 0$. For base case we see that $\hat{a}^0 = (0, 0)$. For the induction step assume $\hat{a}^k = (k, 0)$. Then we have

$$\hat{a}^{k+1} = \hat{a}^k \cdot \hat{a} = (k, 0) \cdot (1, 0) = (k + \psi^0(1), 0 + 0) = (k + 1, 0).$$

So,

$$\hat{a}^8 = (1, 0)^8 = (8, 0) = (0, 0) \quad (\text{since } 8 \equiv 0 \pmod{8})$$

- We have

$$\begin{aligned} \hat{b}\hat{a}\hat{b} &= ((0, 1) \cdot (1, 0)) \cdot (0, 1) \\ &= ((0 + \psi^1(1), 1 + 0)) \cdot (0, 1) \\ &= (0 + 5, 1) \cdot (0, 1) && (\text{because } \psi^1(1) = 5 \cdot 1 = 5) \\ &= (5 + \psi^1(0), 1 + 1) && (\text{because } \psi^1(0) = 5 \cdot 0 = 0, \\ &= (5 + 0, 0) && (\text{because } 2 \equiv 0 \pmod{2}) \\ &= (5, 0) \\ &= \hat{a}^5. && (\text{because } \hat{a} = (1, 0)) \end{aligned}$$

Therefore $\hat{a}$ and $\hat{b}$ satisfy the relations in the definition of H_2 .

To complete the proof we will show $|H_2| \leq |H|$. We claim that the subgroup generated by a is a normal subgroup of H_2 . We need to show that the normalizer of $\langle a \rangle$ is the whole group. We know every subgroup normalizes itself so we just check that it is normalized by b (because a and b generate the whole group). Since $b^{-1}ab = a^5$, it follows that $b^{-1}a^ib = (b^{-1}ab)^i = a^{5i} \in \langle a \rangle$. Thus, conjugating any element of the subgroup $\langle a \rangle$ by b results in another element of $\langle a \rangle$. Therefore, because the normalizer contains both a and b so the normalizer is all of H_2 . This completes the proof of the

claim.

We know $|H| = |\mathbb{Z}_8 \times \mathbb{Z}_2| = 16$. So we just need to show $|H_2| \leq 16$.

We know $|\langle a \rangle| \leq 8$. The quotient group $H_2/\langle a \rangle$ is generated by the element b and $b^2 = 1$, so the quotient group $H_2/\langle a \rangle$ has less than equal to 2 elements. Now the order of H_2 can be calculated as the product of the order of the normal subgroup $\langle a \rangle$ and the order of the quotient group $H_2/\langle a \rangle$:

$$|H_2| = |\langle a \rangle| \times |H_2/\langle a \rangle| \leq 8 \times 2 = 16.$$

Hence $|H_2| \leq 16$ so by Corollary 2.1.15 we can say $H_2 \cong H$. □

5.3C The group H_3

The following result shows that H_3 is the generalized dihedral group over $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Theorem 5.3.11.

$$H_3 = \langle a, b, c : a^3 = b^3 = c^2 = 1, ab = ba, (ac)^2 = (bc)^2 = 1 \rangle \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi} \mathbb{Z}_2$$

where $\psi(v) = (-1)v$ for $v \in \mathbb{Z}_3 \times \mathbb{Z}_3$.

Proof. Let $H = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi} \mathbb{Z}_2$, so $H = \langle \hat{a}, \hat{b}, \hat{c} \rangle$, where $\hat{a} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right)$, $\hat{b} = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right)$, and $\hat{c} = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right)$.

- It is easy to see that $\hat{a}^3 = \hat{b}^3 = \hat{c}^2 = 1$.

- We have

$$\begin{aligned} \hat{a}\hat{b} &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \\ &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 + 0 \right) \\ &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \\ &= \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, 0 \right) \end{aligned}$$

and

$$\begin{aligned}
 \hat{b}\hat{a} &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \psi^0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 + 0 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, 0 \right)
 \end{aligned}$$

so $\hat{a}\hat{b} = \hat{b}\hat{a}$.

- We have

$$\begin{aligned}
 \hat{a}\hat{c} &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0 + 1 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1 \right)
 \end{aligned}$$

so

$$\begin{aligned}
 \hat{a}\hat{c}\hat{a} &= (\hat{a}\hat{c})\hat{a} \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1 \right) \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi^1 \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1 + 0 \right) \\
 &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} -1 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) = \hat{c}.
 \end{aligned}$$

This implies $\hat{a}\hat{c}\hat{a} = 1$ so $(\hat{a}\hat{c})^2 = 1$.

- We have

$$\begin{aligned}
 \hat{b}\hat{c} &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0 + 1 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 \right),
 \end{aligned}$$

so

$$\begin{aligned}
 \hat{b}\hat{c}\hat{b} &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 \right) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \psi^1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 + 0 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ -1 \end{pmatrix}, 1 \right) \\
 &= \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \\
 &= \hat{c}.
 \end{aligned}$$

This implies $\hat{b}\hat{c}\hat{b} = 1$ so $(\hat{b}\hat{c})^2 = 1$. Therefore $\hat{a}, \hat{b}$ and $\hat{c}$ satisfy the relations in the definition of H_3 .

We will show $|H_3| \leq |H|$. In H_3 :

- Since $a^3 = b^3 = 1$, and $ab = ba$, the subgroup $N = \langle a, b \rangle$ consists of all elements of the form $a^i b^j$, where $i, j \in \{0, 1, 2\}$, so $|\langle a, b \rangle| \leq 9$.

We claim that $N \triangleleft H_3$. Obviously, N is normalized by a and b so we just need to show it is normalized by c . For $n = a^i b^j \in N$ we have

$$c(a^i b^j)c^{-1} = ca^i(c^{-1}c)b^j c^{-1} = (cac^{-1})^i (cbc^{-1})^j = (a^{-1})^i (b^{-1})^j = a^{-i} b^{-j} \in N.$$

This shows that conjugation by c preserves the subgroup N .

- Since c has order less than equal to 2, the order of quotient group H_3/N is less than equal to 2.

Therefore we have

$$|H_3| = |N| \times |H_3/N| \leq 9 \times 2 = 18.$$

Since $H = |(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2| = 18$ this implies $|H_3| \leq |H|$ so by Corollary 2.1.15 we can say $H_3 \cong H$. □

5.3D The group H_4

Remark 5.3.12. The definition of H_4 in [28, Theorem 2.1] erroneously omits the relation $b^3 = 1$. (Without this relation the group is infinite.)

Theorem 5.3.13.

$$H_4 = \langle a, b, c \mid a^3 = b^3 = c^3 = 1, ac = ca, bc = cb, b^{-1}ab = ac \rangle \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi} \mathbb{Z}_3$$

where $\psi(v) = Av$, where $A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ for $v \in \mathbb{Z}_3 \times \mathbb{Z}_3$.

Proof. Let $H = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi} \mathbb{Z}_3$, so $H = \langle \hat{a}, \hat{b}, \hat{c} \rangle$, where $\hat{a} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right)$, $\hat{b} = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right)$, and $\hat{c} = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right)$.

It is easy to see that $\hat{a}^3 = \hat{b}^3 = \hat{c}^3 = 1$. Also:

$$\hat{a}\hat{c} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 + 0 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, 0 \right)$$

and

$$\hat{c}\hat{a} = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \psi^0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 + 0 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0 \right) = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, 0 \right)$$

so $\hat{a}\hat{c} = \hat{c}\hat{a}$. Furthermore:

$$\hat{b}\hat{c} = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} + \psi^1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 + 0 \right) = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 \right)$$

and

$$\hat{c}\hat{b} = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0 \right) \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0 + 1 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1 \right) = \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1 \right)$$

so $\hat{b}\hat{c} = \hat{c}\hat{b}$.

We now verify that $\hat{a}$, $\hat{b}$, and $\hat{c}$ satisfy the final relation in the definition of H_4 , by showing that $\hat{a}\hat{b} = \hat{b}\hat{a}\hat{c}$. Note that:

$$\hat{a}\hat{b} = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0\right) \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1\right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \psi^0 \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 0+1\right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1\right) = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1\right).$$

We evaluate $\hat{b}\hat{a}\hat{c}$ in two steps:

$$\hat{b}\hat{a} = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}, 1\right) \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 0\right) = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} + \psi^1 \begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1\right) = \left(\begin{pmatrix} 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \end{pmatrix}, 1\right) = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, 1\right),$$

now we have

$$\begin{aligned} \hat{b}\hat{a}\hat{c} &= (\hat{b}\hat{a})\hat{c} = \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, 1\right) \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, 0\right) \\ &= \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \psi^1 \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1\right) \\ &= \left(\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}, 1\right) \\ &= \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, 1\right), \end{aligned}$$

so $\hat{a}\hat{b} = \hat{b}\hat{a}\hat{c}$.

Therefore $\hat{a}$, $\hat{b}$ and $\hat{c}$ satisfy the relations in the definition of H_4 . We will show $|H_4| \leq 27$. In H_4 :

- a and c each have order less than equal to 3, and since $ac = ca$, so $|\langle a, c \rangle| \leq 9$.
- The subgroup $N = \langle a, c \rangle$ consists of all elements of the form $a^i c^j$, where $i, j \in \{0, 1, 2\}$. We claim that N is a normal subgroup of H_4 . To do this, we need to show that for any $g \in H_4$ and any $n \in N$, the conjugate $gng^{-1} \in N$. It is enough to show the generator a, b , and c of H_4 normalize N .

Since a and c are in $\langle a, c \rangle$, we only need to consider b . We need to compute the conjugates of the generators a and c of N by b :

- We have $b^{-1}ab = ac \in \langle a, c \rangle = N$.
- The relation $bc = cb$ indicates that c commutes with b , so $bc b^{-1} = c \in \langle a, c \rangle = N$.

Since the conjugates of both generators a and c by the element b remain within the subgroup $N = \langle a, c \rangle$ we conclude that b normalizes N . Then a, b and c all normalize N so N is a normal subgroup of H_4 .

The quotient group H_4/N is generated by the coset bN . Since b has order less than equal to 3, the quotient group H_4/N has order less than or equal to 3. So, we have

$$|H_4| = |N| \times |H_4/N| \leq 9 \times 3 = 27 = |H|.$$

so by Corollary 2.1.15 we can say $H_4 \cong H$. □

Chapter 6

Cayley index of every finite group

Recall (see Definition 3.2.4). The *Cayley index* $c(\Gamma)$ of the Cayley graph $\Gamma = \text{Cay}(G; S)$ is the index of the left translations $L(G)$ in $\text{Aut}(\Gamma)$; since G is finite, this is equal to the number of automorphisms of Γ divided by the number of left translations of G .

Recall (see Definition 3.2.5). Let G be a group. A Cayley graph on G with the smallest Cayley index is called an *MRR (Most Rigid Representation)* for G .

Theorem 5.0.1, stated that the groups $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_2^4$, D_6 , D_8 , D_{10} , A_4 , H_1 , H_2 , H_3 , H_4 , $Q_8 \times \mathbb{Z}_3$, and $Q_8 \times \mathbb{Z}_4$ do not admit a GRR, but we did not give a proof.

We will now verify that none of these 13 groups have a GRR. (See Corollary 6.0.2.) The remainder of the chapter will calculate the Cayley index of every finite group that does not have a GRR. (See Table 6.5.) This is a verification of results that were already known.

Theorem 6.0.1 ([28, Table 1]). *In each line of Table 6.1, the value given in the Cayley-index column is the Cayley index of the specified group. Moreover, the specified connection set defines a Cayley graph whose Cayley index is equal to this value. Therefore, this Cayley graph is an MRR of the group.*

Proof. For each of the thirteen groups, the program in Appendix A.3 computes the Cayley index of the group and produces a connection set for which the corresponding Cayley graph attains this index. The computed values and connection sets are those listed in Table 6.1.

Group	Order	Cayley Index	Connection Set
$\mathbb{Z}_2^2$	4	2	$\{z_1\}$
$\mathbb{Z}_2^3$	8	6	$\{z_1, z_2, z_3\}$
$\mathbb{Z}_2^4$	16	8	$\{z_1, z_2, z_3, z_4, z_1z_2z_3, z_1z_4, z_1z_3\}$
D_6	6	2	$\{s, sr\}$
D_8	8	2	$\{s, sr\}$
D_{10}	10	2	$\{s, r^{\pm 1}\}$
A_4	12	2	$\{(1\ 2\ 3)^{\pm 1}, (1\ 2)(3\ 4)\}$
H_1	16	2	$\{a, b, c, (ab)^{\pm 1}\}$
H_2	16	2	$\{a^{\pm 1}, a^{\pm 2}, b\}$
H_3	18	2	$\{a^{\pm 1}, c, ac, bc\}$
H_4	27	2	$\{a^{\pm 1}, b^{\pm 1}, (a^{-1}b)^{\pm 1}, (bab^{-1})^{\pm 1}\}$
$Q_8 \times \mathbb{Z}_3$	24	2	$\{i^{\pm 1}, (iz)^{\pm 1}, (jz)^{\pm 1}\}$
$Q_8 \times \mathbb{Z}_4$	32	2	$\{i^{\pm 1}, j^{\pm 1}, (z)^{\pm 1}, (iz)^{\pm 1}, (-kz)^{\pm 1}\}$

Table 6.1: Order, Cayley index, and MRR connection set for each of the 13 groups in Theorem 5.0.1

□

Corollary 6.0.2. *None of the 13 groups listed in Table 6.1 have a GRR.*

Proof. The table shows that the Cayley index of each group is greater than 1. □

Our verification of Table 6.5 assumes the following results without proof.

Theorem 6.0.3 ([28, Proposition 4.8]). *For every integer $n \geq 2$, the Cayley index of $Q_8 \times \mathbb{Z}_2^n$ is 8.*

Theorem 6.0.4 (Imrich–Watkins [22, Thm 2]). *Let G be a finite abelian group. Then $c(G) \leq 2$ unless G is one of the following seven groups:*

$$\mathbb{Z}_2^3, \mathbb{Z}_2^4, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2^2, \mathbb{Z}_3^2, \mathbb{Z}_3^3, \text{ and } \mathbb{Z}_4^2.$$

Remark 6.0.5. Our definition of a generalized dicyclic group (Definition 2.1.3) is slightly broader than the definition used by Imrich and Watkins in [22, p. 245]. Imrich and Watkins require generalized dicyclic groups to be nonabelian, whereas our

definition includes every group of the form $\text{Dic}(A, z)$, including the cases in which this group is abelian.

We use the broader definition because it allows all groups arising from the construction $\text{Dic}(A, z)$ to be treated uniformly. In particular, this avoids having to separate the abelian cases from the nonabelian cases whenever results or computations are stated for groups of this form. When applying a result from [22], however, we must always verify that its hypothesis requiring the group to be nonabelian is satisfied.

Theorem 6.0.6 (Imrich–Watkins [22, Thm 2(1b)]). *Let $G = \text{Dic}(A, z)$ be a finite nonabelian generalized dicyclic group. If G is not of the form $Q_8 \times \mathbb{Z}_2^r$ for some $r \geq 0$, and $|G| > 96$, then $c(G) = 2$.*

The above Theorem calculates the Cayley index of generalized dicyclic groups of order greater than 96. The following result looks at the ones that have smaller order.

Lemma 6.0.7 ([28, proof of Thm 5.8]). *If $G = \text{Dic}(A, z)$, $|G| \leq 96$, and G is neither abelian nor a Hamiltonian 2-group, then $c(G) = 2$, except when A is one of the following groups: $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, or $\mathbb{Z}_4 \times \mathbb{Z}_2$.*

Proof. The program in Appendix A.4 checks (up to) 1000 random Cayley graphs of each nonabelian generalized dicyclic group whose abelian subgroup of index 2 has order at most 48. It prints an error message if the program does not find a Cayley graph whose Cayley index is 2.

The output shows error messages only for the groups listed in the left column of Table 6.2. The program may describe a group using a different presentation from the one used in Table 6.5, so the right column identifies the corresponding entry in Table 6.5. These groups are the exceptional cases mentioned in the statement of the lemma and Hamiltonian 2-groups.

Therefore, this establishes that the lemma is true. □

Group	Order of the Group	Group in Table 6.5
$\text{Dic}(\mathbb{Z}_4, 2)$	8	$\cong Q_8$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_3, (1, 0))$	12	$\cong \text{Dic}(\mathbb{Z}_6, 3)$
$\text{Dic}(\mathbb{Z}_8, 4)$	16	$\text{Dic}(\mathbb{Z}_8, 4)$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_4, (1, 0))$	16	$\cong \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_4, (0, 2))$	16	$\cong Q_8 \times \mathbb{Z}_2$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_4, (1, 2))$	16	$\cong \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_5, (1, 0))$	20	$\cong \text{Dic}(\mathbb{Z}_{10}, 5)$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, (0, 0, 2))$	32	$\cong Q_8 \times \mathbb{Z}_2^2$
$\text{Dic}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4, (0, 0, 0, 2))$	64	$\cong Q_8 \times \mathbb{Z}_2^3$

Table 6.2: Nonabelian generalized dicyclic groups for which no Cayley graph of index 2 was found.

We do not need Table 6.6 for our proof, but for completeness, we verified the information given in [28, Table 4].

Theorem 6.0.8. *Each line of Table 6.6 lists the correct Cayley index of the specified group. Moreover, the specified connection set defines a Cayley graph that is an MRR of the group.*

Proof. This is verified by the program in Appendix A.6. □

Remark 6.0.9. While studying the results presented in Table 4 of [28], which we have reproduced in Table 6.6, we identified two inaccuracies in the listed Most Rigid Representations (MRRs) for the generalized dicyclic groups $\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$ and $\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$ which yields the results in Table 6.3. The authors computed the Cayley index of these groups using the connection sets

$$\{z_1^{\pm 1}, z_2^{\pm 1}, (z_1 z_2)^{\pm 1}, x^{\pm 1}, (z_1 x)^{\pm 1}\} \quad \text{and} \quad \{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_1^5 x)^{\pm 1}, (z_1^3 z_2 x)^{\pm 1}\},$$

Group	Connection Set S	Cayley Index
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$	$\{z_1^{\pm 1}, z_2^{\pm 1}, (z_1 z_2)^{\pm 1}, x^{\pm 1}, (z_1 x)^{\pm 1}\}$	32
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$	$\{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_1^5 x)^{\pm 1}, (z_1^3 z_2 x)^{\pm 1}\}$	8

Table 6.3: Incorrect connection set in Table 4 of [28]

Group	Connection Set S	Cayley Index
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$	$\{z_1 z_2 x, z_2^{-1}, z_2^2, z_1 z_2^{-1}, z_1 x, z_2^{-1} x^{-1}\}$	2
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$	$\{z_1^{\pm 1}, (z_1^2 z_2)^{\pm 1}, x^{\pm 1}, (z_1^3 x)^{\pm 1}, (z_2 x)^{\pm 1}\}$	2

Table 6.4: Correct connection sets yielding Cayley index 2

respectively, and concluded that the Cayley index in each case is 2. However, our findings show that these connection sets are incorrect. This is established by the program in Appendix A.5.

To address these errors, we found connection sets that do give a Cayley index of 2 for each group. Specifically, if we choose

$$S = \{z_1 z_2 x, z_2^{-1}, z_2^2, z_1 z_2^{-1}, z_1 x, z_2^{-1} x^{-1}\}$$

for $\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$, and

$$S = \{z_1^{\pm 1}, (z_1^2 z_2)^{\pm 1}, x^{\pm 1}, (z_1^3 x)^{\pm 1}, (z_2 x)^{\pm 1}\}$$

for $\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$, the corresponding Cayley graphs do have Cayley index 2 as shown in the Table 6.4. Our Table 6.6 incorporates these corrections.

Theorem 6.0.10. *Each line of Table 6.5 lists the correct Cayley index of the specified group. Moreover, the specified connection set defines a Cayley graph that is an MRR of the group.*

Proof. Let G be a finite group. By Theorem 5.0.1, we know that the Cayley index of G is 1 unless either G is abelian or G is generalized dicyclic, or G is one of the 13 specific groups that are listed in the statement of Theorem 5.0.1. Table 6.1 tells us the Cayley index and the MRR of each of the 13 specific groups, so we can assume G

is either abelian or generalized dicyclic.

Case 1. *Assume G is abelian.*

Subcase 1.1. *Assume $G = \mathbb{Z}_2^n$ for $n \geq 5$. It is verified in Theorem 5.1.1.*

Subcase 1.2. *Assume G is $\mathbb{Z}_2, \mathbb{Z}_2^2$ or one of the seven exceptional abelian groups listed in Theorem 6.0.4 which are:*

$$\mathbb{Z}_2^3, \mathbb{Z}_2^4, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2^2, \mathbb{Z}_3^2, \mathbb{Z}_3^3, \text{ and } \mathbb{Z}_4^2.$$

All of these (including the connection set of an MRR) were verified using the program in Appendix A.7.

Subcase 1.3. *All other finite abelian groups.* We covered all elementary abelian 2-groups so we can assume the exponent of G is greater than 2. By Example 5.2.2 the Cayley index is not 1. However by Theorem 6.0.4 we know that Cayley index is at most 2. Therefore, the Cayley index of G is exactly 2.

Case 2. *Let $G = \text{Dic}(A, z)$ be a nonabelian generalized dicyclic group.*

Subcase 2.1. *G is a Hamiltonian 2-group.*

The cases Q_8 and $Q_8 \times \mathbb{Z}_2$ (including the connection set of an MRR) are verified by the program in Appendix A.8. The general case $G = Q_8 \times \mathbb{Z}_2^n$ for $n \geq 2$ is verified in Theorem 6.0.3.

Subcase 2.2. *$|G| > 96$ and G is not a Hamiltonian 2-group.* Then by Theorem 6.0.6, we have $c(G) = 2$.

Subcase 2.3. *$|G| \leq 96$ and G is not Hamiltonian 2-group.* In this case, we apply Lemma 6.0.7, which states that $c(G) = 2$ unless A is isomorphic to one of the following: $\mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{10}$, or $\mathbb{Z}_4 \times \mathbb{Z}_2$.

The Cayley index and the connection set of an MRR of each of the corresponding

exceptional groups

$$\text{Dic}(\mathbb{Z}_6, 3), \quad \text{Dic}(\mathbb{Z}_8, 4), \quad \text{Dic}(\mathbb{Z}_{10}, 5), \quad \text{and} \quad \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$$

were computed and verified using the program referenced in Appendix A.9. □

Group	Order	Cayley Index	Connection Set
Elementary abelian 2-groups			
$\mathbb{Z}_2$	2	1	$\{\}$
$\mathbb{Z}_2^2$	4	2	$\{z_1\}$
$\mathbb{Z}_2^3$	8	6	$\{z_1, z_2, z_3\}$
$\mathbb{Z}_2^4$	16	8	$\{z_1, z_2, z_3, z_4, z_1 z_2 z_3, z_1 z_4, z_1 z_3\}$
$\mathbb{Z}_2^n, n \geq 5$	2^n	1	
Other abelian groups			
$\mathbb{Z}_4 \times \mathbb{Z}_2$	8	6	$\{z_1^{\pm 1}, z_2\}$
$\mathbb{Z}_4^2$	16	4	$\{z_1^{\pm 1}, z_2^{\pm 1}, z_1^2, (z_1 z_2)^{\pm 1}\}$
$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	16	8	$\{z_1^{\pm 1}, z_2, z_3, z_4, (z_1 z_2)^{\pm 1}, (z_1 z_3)^{\pm 1}\}$
$\mathbb{Z}_3^2$	9	8	$\{z_1^{\pm 1}, z_2^{\pm 1}\}$
$\mathbb{Z}_3^3$	27	12	$\{z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}, (z_1 z_2)^{\pm 1}, (z_1 z_3)^{\pm 1}, (z_2 z_3)^{\pm 1}\}$
All other abelian groups		2	
Hamiltonian 2-groups			
Q_8	8	16	$\{i^{\pm 1}\}$
$Q_8 \times \mathbb{Z}_2$	16	16	$\{i^{\pm 1}, j^{\pm 1}, z_1, i^{\pm 1} z_1\}$
$Q_8 \times \mathbb{Z}_2^n, n \geq 2$	2^{n+3}	8	
Other generalized dicyclic groups			
$\text{Dic}(\mathbb{Z}_6, 3)$	12	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8, 4)$	16	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_{10}, 5)$	20	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$	16	4	$\{z_1^{\pm 1}, x^{\pm 1}, (z_1 x)^{\pm 1}\}$
All other generalized dicyclic groups		2	
Exceptional groups			
D_6	6	2	$\{s, sr\}$
D_8	8	2	$\{s, sr\}$
D_{10}	10	2	$\{r^{\pm 1}, s\}$
A_4	12	2	$\{(1\ 2\ 3)^{\pm 1}, (1\ 2)(3\ 4)\}$
$Q_8 \times \mathbb{Z}_3$	24	2	$\{i^{\pm 1}, (iz)^{\pm 1}, (jz)^{\pm 1}\}$
$Q_8 \times \mathbb{Z}_4$	32	2	$\{i^{\pm 1}, j^{\pm 1}, (z)^{\pm 1}, (iz)^{\pm 1}, (-kz)^{\pm 1}\}$
H_1	16	2	$\{a, b, c, (ab)^{\pm 1}\}$
H_2	16	2	$\{a^{\pm 1}, a^{\pm 2}, b\}$
H_3	18	2	$\{a^{\pm 1}, c, ac, bc\}$
H_4	27	2	$\{a^{\pm 1}, b^{\pm 1}, (a^{-1}b)^{\pm 1}, (bab^{-1})^{\pm 1}\}$
Every finite group not listed above		1	

Table 6.5: Cayley indices of all finite groups with connection sets for an MRR

Group	Cayley index	Connection set for an MRR
$\text{Dic}(\mathbb{Z}_6, 3)$	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8, 4)$	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_{10}, 5)$	4	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$	4	$\{z_1^{\pm 1}, x^{\pm 1}, (z_1 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_2, (4, 0))$	2	$\{z_1^{\pm 1}, z_2, x^{\pm 1}, (z_1 x)^{\pm 1}, (z_2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4, (2, 0))$	2	$\{z_1 z_2 x, z_2^{-1}, z_2^2, z_1 z_2^{-1}, z_1 x, z_2^{-1} x^{-1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2^2, (0, 1, 0))$	2	$\{z_1^{\pm 1}, z_3, x^{\pm 1}, (z_1 x)^{\pm 1}, (z_3 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_6 \times \mathbb{Z}_3, (3, 0))$	2	$\{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_2 x)^{\pm 1}, (z_1 z_2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_2^2, (4, 0, 0))$	2	$\cong \text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_2, (4, 0)) \times \mathbb{Z}_2$
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4, (4, 0))$	2	$\{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_1^6 z_2^{-1} x)^{\pm 1}, (z_1^5 z_2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4, (0, 2))$	2	$\{z_1^{\pm 1}, (z_1^2 z_2)^{\pm 1}, x^{\pm 1}, (z_1^3 x)^{\pm 1}, (z_2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4^2 \times \mathbb{Z}_2, (2, 0, 0))$	2	$\cong \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4, (2, 0)) \times \mathbb{Z}_2$
$\text{Dic}(\mathbb{Z}_4^2 \times \mathbb{Z}_2, (0, 0, 1))$	2	$\{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_2^3 x)^{\pm 1}, (z_1^3 z_2^2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2^3, (0, 1, 0, 0))$	2	$\cong \text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2^2, (0, 1, 0)) \times \mathbb{Z}_2$
$\text{Dic}(\mathbb{Z}_{12} \times \mathbb{Z}_3, (6, 0))$	2	$\{z_1^{\pm 1}, z_2, x^{\pm 1}, (z_1^7 z_2 x)^{\pm 1}, (z_1^3 z_2 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_6 \times \mathbb{Z}_6, (3, 0))$	2	$\cong \text{Dic}(\mathbb{Z}_6 \times \mathbb{Z}_3, (3, 0)) \times \mathbb{Z}_2$
$\text{Dic}(\mathbb{Z}_{12} \times \mathbb{Z}_4, (6, 0))$	2	$\{z_1^{\pm 1}, z_2^{\pm 1}, x^{\pm 1}, (z_1^4 z_2 x)^{\pm 1}, (z_1^9 z_2^3 x)^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_{12} \times \mathbb{Z}_4, (0, 2))$	2	$\{z_1^{\pm 1}, (z_1^3 z_2)^{\pm 1}, x^{\pm 1}, (z_1 x)^{\pm 1}, (z_1 z_2 x)^{\pm 1}\}$

Table 6.6: Corrected version of [28, Table 4]. The connection sets for $\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_4; (2, 0))$ and $\text{Dic}(\mathbb{Z}_8 \times \mathbb{Z}_4; (0, 2))$ have been corrected. Some rows do not provide a connection set, because G has the same Cayley index as $G \times \mathbb{Z}_2$ unless G is $\mathbb{Z}_2^2$, $\mathbb{Z}_2^3$, $\mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, or $\mathbb{Z}_3^2$ [28, Corollary 4.5].

Chapter 7

Finite groups that do not have a normal Cayley graph

Recall (see Definition 2.3.8). A Cayley graph $\Gamma = \text{Cay}(G; S)$ is *normal* if every automorphism of the Cayley graph is affine.

Recall (see Definition 2.2.1). The left translation $L(G) = \{\ell_g \mid g \in G\}$ where $\ell_g(h) = gh$ for all $h \in G$, forms a group under function composition.

In this chapter, we prove the following result.

Theorem 7.0.1 (Wang, Wang, and Xu [33, Thm. 1]). *A finite group G has a Cayley graph that is normal if and only if G is not isomorphic with $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $Q_8 \times \mathbb{Z}_2^r$ for some $r \geq 0$.*

Theorem 7.0.1 applies to all finite groups. The result can also be extended to many infinite groups, but we do include a proof here.

Theorem 7.0.2 (Leeman and de la Salle [24, Thm. 1]). *If G is an infinite group that has a finite generating set, then there is a finite, inverse-closed generating set S of G , such that the translations form a subgroup of index at most 2 in the automorphism group of $\text{Cay}(G; S)$.*

Since every subgroup of index 1 or 2 is normal, this has the following immediate consequence:

Corollary 7.0.3 (Leeman and de la Salle). *If G is an infinite group that has a finite generating set, then G has a locally finite Cayley graph that is normal.*

7.1 Preliminaries on normal Cayley graphs

The following result explains why Cayley graphs satisfying the condition in Definition 2.3.8 are called “normal.” The equivalent condition is commonly used as the definition of normal Cayley graphs in the literature [33, Definition 1].

Corollary 7.1.1. *A Cayley graph $\Gamma = \text{Cay}(G; S)$ is normal if and only if the left translations form a normal subgroup of $\text{Aut}(\Gamma)$.*

Proof. ($\Leftarrow$). Assume the left translations are a normal subgroup of $\text{Aut}(\Gamma)$. Then by Lemma 2.2.3 every graph automorphism is an affine map, which means the Cayley graph is normal.

($\Rightarrow$). Assume that $\Gamma = \text{Cay}(G; S)$ is a normal Cayley graph. Then by definition, every automorphism of Γ is affine. By Lemma 2.2.3, every affine map normalizes $L(G)$. Therefore $L(G)$ is normalized by every element of $\text{Aut}(\Gamma)$, and hence the left translations form a normal subgroup of $\text{Aut}(\Gamma)$. $\square$

Corollary 7.1.2. *If the Cayley index of $\text{Cay}(G; S)$ is less than or equal to 2 then the Cayley graph $\text{Cay}(G; S)$ is normal.*

Proof. Suppose the Cayley index is 1. Then it is obvious that the Cayley graph is normal because every group is a normal subgroup of itself. If the Cayley index is 2 then the Cayley graph is normal as we know that the group of left translations is a subgroup of index 2 and every subgroup of index 2 is normal. $\square$

7.2 Proof of Theorem 7.0.1

Example 7.2.1. $\mathbb{Z}_4 \times \mathbb{Z}_2$ does not have a normal Cayley graph.

Proof. This is verified by the program in Appendix A.10, because it prints False as the result. $\square$

Lemma 7.2.2. *$\varphi(x) = x^{-1}$ is a graph automorphism of every Cayley graph of $Q_8 \times \mathbb{Z}_2^r$ ($r \geq 0$).*

Group	Connection Set
$\mathbb{Z}_2^3$	$\{z_1, z_2, z_3\}$
$\mathbb{Z}_2^4$	$\{z_1, z_2, z_3, z_4\}$
$\mathbb{Z}_4^2$	$\{(z_1^2 z_2^3)^{\pm 1}, (z_1^3 z_2^3)^{\pm 1}, (z_1^3)^{\pm 1}\}$
$\mathbb{Z}_4 \times \mathbb{Z}_2^2$	$\{(z_1^2 z_3)^{\pm 1}, (z_1^3 z_3)^{\pm 1}, z_2 z_3, (z_1^2 z_2)^{\pm 1}\}$
$\mathbb{Z}_3^2$	$\{z_1^{\pm 1}, z_2^{\pm 1}\}$
$\mathbb{Z}_3^3$	$\{z_1^{\pm 1}, z_2^{\pm 1}, z_3^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_6, 3)$	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_8, 4)$	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_{10}, 5)$	$\{z_1^{\pm 1}, x^{\pm 1}\}$
$\text{Dic}(\mathbb{Z}_4 \times \mathbb{Z}_2, (0, 1))$	$\{(z_1^3)^{\pm 1}, (z_1^2 x^3)^{\pm 1}, (z_1 x^3)^{\pm 1}\}$

Table 7.1: Connection set for a normal Cayley graph

Proof. We will see in part c(0) of the proof of Example 8.1.1, that φ is a graph automorphism. $\square$

Example 7.2.3. $Q_8 \times \mathbb{Z}_2^r$ for $r \geq 0$ does not have a normal Cayley graph.

Proof. Consider $\varphi(x) = x^{-1}$. It is a graph automorphism of every Cayley graph of $Q_8 \times \mathbb{Z}_2^r$ by Lemma 7.2.2 but it fixes 1 and it is not a group automorphism because the group is not abelian so φ is not an affine map. $\square$

Theorem 7.2.4. *Each connection set in Table 7.1 gives a normal Cayley graph for the corresponding group.*

Proof. This is verified by the program in Appendix A.11, because for every of them the program said True. $\square$

Proof of Theorem 7.0.1. ($\Rightarrow$). See Examples 7.2.1 and 7.2.3.

($\Leftarrow$). We prove the contrapositive. Assume G does not have a normal Cayley graph. According to Corollary 7.1.2, the Cayley index of G is greater than 2. Therefore, G is a group in Table 6.5 where the Cayley index is greater than 2. Table 7.1 lists all of these groups except for $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $Q_8 \times \mathbb{Z}_2^r$. By Theorem 7.2.4 all of these groups have a normal Cayley graph. Since G does not have a normal Cayley graph this implies that G is either $\mathbb{Z}_4 \times \mathbb{Z}_2$ or $Q_8 \times \mathbb{Z}_2^r$. $\square$

Chapter 8

Colour-preserving automorphisms of complete Cayley graphs

The main results of this chapter were published in [3].

Theorem 8.0.1. *If G is a (finite or infinite) group, then the following are equivalent:*

1. G has a Cayley graph that is strongly CCA.
2. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is strongly CCA.
3. G has a Cayley graph that is CCA.
4. The complete graph $\text{Cay}(G; G \setminus \{1\})$ is CCA.
5. G is not of the form $Q_8 \times B$, where Q_8 is the quaternion group of order 8, and B is an abelian group, such that b^2 is trivial for all $b \in B$.

Furthermore, if G is finite, then these are also equivalent to:

6. Either G has a Cayley graph that is normal, or $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

We first establish the easy parts of Theorem 8.0.1. As was explained in Note 1.4.5, the only really new results are $(1 \Rightarrow 2)$ and the case of $(3 \Rightarrow 1)$ for some infinite groups.

Lemma 8.0.2. *The implications stated in Note 1.4.5(1) are all true.*

Proof. The implications $(2 \Rightarrow 1)$ and $(4 \Rightarrow 3)$ are trivial. See Lemma 2.4.8(5) for $(1 \Rightarrow 3)$, and see [9, 1st paragraph of proof of Thm. 2.3] (or Example 8.1.1(c)) for $(4 \Rightarrow 5)$.

It is easy to see that $\text{Cay}(\mathbb{Z}_4 \times \mathbb{Z}_2; S)$ is strongly CCA for $S = \{(\pm 1, 0), (0, 1)\}$. The other part of $(6 \Rightarrow 1)$ is Lemma 2.4.8(6).

To establish the remaining implication $(3 \Rightarrow 4)$, note that if $\text{Cay}(G; S)$ is CCA, then we see from Lemma 2.4.8(7) that $\text{Cay}(G; G)$ is CCA, because $S \subseteq G$. Then the graph obtained by removing the loop at every vertex is also CCA (see Remark 2.0.2), so $\text{Cay}(G; G \setminus \{1\})$ is CCA. $\square$

8.1 Colour-preserving automorphisms of $\text{Cay}(G; G \setminus \{1\})$

In this section, we recall a result that provides an explicit description of all the colour-preserving automorphisms of any complete Cayley graph $\text{Cay}(G; G \setminus \{1\})$ (see Theorem 8.1.2). It was proved by D. P. Byrne, M. J. Donner, and T. Q. Sibley [6, p. 324] when G is finite, and it was generalized to infinite groups by P.-H. Leemann and M. de la Salle [24, Thm. 2]. This theorem will be needed in Section 8.2, so, for completeness, we provide a proof.

Example 8.1.1. Here are some important (known) examples of colour-preserving automorphisms of complete Cayley graphs.

- a. Assume G is abelian, and define $\iota: G \rightarrow G$ by $\iota(g) = g^{-1}$. Then ι a colour-preserving automorphism of the complete graph $\text{Cay}(G; G \setminus \{1\})$ that fixes 1 . It is a group automorphism, and it is nontrivial if there exists $g \in G$, such that $g^2 \neq 1$.
- b. Let $G = \text{Dic}(A, z, q)$ be a (finite or infinite) generalized dicyclic group, and define $\varphi: G \rightarrow G$ by $\varphi(q^i a) = q^{-i} a$ for $i \in \mathbb{Z}$ and $a \in A$. Then φ is a nontrivial colour-preserving automorphism of the complete graph $\text{Cay}(G; G \setminus \{1\})$ that fixes 1 , and it is a group automorphism.
- c. Let G be a (finite or infinite) Hamiltonian 2-group, so $G = Q_8 \times B$, for some group B of exponent dividing 2. For every $I \subseteq \{i, j, k\}$, there is a unique colour-

preserving automorphism φ_I of the complete graph $\text{Cay}(G; G \setminus \{\mathbf{1}\})$ that fixes $\mathbf{1}$, and satisfies

$$\text{for } \ell \in \{i, j, k\}, \quad \varphi_I(\ell) = \ell \Leftrightarrow \ell \in I.$$

Furthermore, φ_I is a group automorphism if and only if $|I|$ is odd.

There is some overlap between (b) and (c), because any Hamiltonian 2-group is also a dicyclic group. For example, if we write $Q_8 \times B = \text{Dic}(\langle k, B \rangle, i^2, i)$

$$Q_8 \times B = \text{Dic}(\langle k, B \rangle, i^2) = \langle \langle k, B \rangle, i \mid i^2 = i^2, i^{-1}ai = a^{-1}, \forall a \in \langle k, B \rangle \rangle,$$

then the automorphism described in (b) is equal to $\varphi_{\{k\}}$.

Proof. All of these examples are included in the main theorem of [6], but the notation and general presentation there are very different from ours, so we provide brief justifications for the reader's convenience.

It is easy to see (and well known) that if φ is a group automorphism, such that $\varphi(s) \in \{s^{\pm 1}\}$ for all $s \in S$, then φ is a colour-preserving automorphism of $\text{Cay}(G; S)$ that fixes $\mathbf{1}$ (see Lemma 2.4.8(4)).

(a) Note that ι is a group automorphism (because G is abelian). Since $\iota(g) = g^{-1}$ is obviously in $\{g^{\pm 1}\}$ for all $g \in G$, this implies that ι is a colour-preserving automorphism of $\text{Cay}(G; S)$.

(b) For $a \in A$, we have $\varphi(a) = a$ and

$$\varphi(qa) = q^{-1}a = a^{-1}q^{-1} = (qa)^{-1}.$$

Therefore $\varphi(g) \in \{g^{\pm 1}\}$ for all $g \in G$.

Hence, all that remains is to show that φ is a group automorphism. For $b \in A$, we have

$$\varphi((q^i a)b) = \varphi(q^i(ab)) = q^{-i}ab = \varphi(q^i a)\varphi(b)$$

and

$$\varphi((q^i a)(qb)) = \varphi(q^{i+1}(a^{-1}b)) = q^{-i-1}a^{-1}b = q^{-i}a \cdot q^{-1}b = \varphi(q^i a) \varphi(qb).$$

Thus φ is a group automorphism. Therefore, by Lemma 2.4.8(4), φ is a colour-preserving automorphism of $\text{Cay}(G; G \setminus \{\mathbf{1}\})$.

(c) The uniqueness follows from Lemma 2.5.11(1). So we only prove existence.

0. Let $\varphi_\emptyset = \iota$, where $\iota(x) = x^{-1}$, as in (a). This is not a group automorphism (because G is not abelian).

However, we can easily show that it is a colour-preserving graph automorphism (and it obviously fixes $\mathbf{1}$), by using an argument that is taken from the first paragraph of the proof of [9, Theorem 2.3]. Let $g, s \in G$. Then $\varphi_\emptyset(gs) = (gs)^{-1} = s^{-1}g^{-1}$. In $G = Q_8 \times B$, every element either inverts or commutes with every other element, so $s^{-1}g^{-1} \in \{g^{-1}s^{\pm 1}\} = \{\varphi(g)s^{\pm 1}\}$.

1. For $\ell \in \{i, j, k\}$, we may let $\varphi_{\{\ell\}}$ be the conjugation by ℓ . This is a group automorphism.
2. If $|I| = 2$, we have $I = \{i, j, k\} \setminus \{\ell\}$, for some $\ell \in \{i, j, k\}$. Then $\varphi_I = \varphi_{\{\ell\}} \circ \varphi_\emptyset$. This is not a group automorphism, because it is the composition of an automorphism with a non-automorphism.
3. The automorphism $\varphi_{\{i, j, k\}}$ is the trivial permutation (i.e., the identity map).

This is a group automorphism. □

Theorem 8.1.2 (Byrne, Donner, and Sibley [6], Leemann and de la Salle [24, Thm. 2]). *Let G be a (finite or infinite) group. If the complete Cayley graph $\text{Cay}(G; G \setminus \{\mathbf{1}\})$ has a nontrivial colour-preserving automorphism that fixes $\mathbf{1}$, then G is either abelian or generalized dicyclic. Furthermore, any such colour-preserving automorphism is one of the automorphisms in Example 8.1.1.*

Proof. This is similar to the proof of [9, Thm. 2.3].

By assumption, we may let φ be a nontrivial colour-preserving automorphism of the complete graph $\text{Cay}(G; G \setminus \{1\})$ that fixes 1 . Let

$$F = \{f \in G \mid \varphi(f) = f\},$$

and let F^c be the complement of F . Note that F is a proper subset of G , because φ is nontrivial, and that

$$\varphi(g) = g^{-1} \text{ for all } g \in F^c$$

(because φ is colour-preserving and fixes 1).

For all $f \in F$ and $h \in G$, such that $fh \in F^c$, we have

$$\varphi(fh) = (fh)^{-1} = h^{-1}f^{-1}$$

and

$$\varphi(fh) \in \{\varphi(f)h^{\pm 1}\} = \{fh^{\pm 1}\}$$

However, since $fh \notin F$, we know that $\varphi(fh) \neq fh$. So we must have

$$fh^{-1} = \varphi(fh) = h^{-1}f^{-1},$$

which means that h inverts f . Therefore fh also inverts f . Thus, we have shown:

$$\text{every element of } F^c \text{ inverts every element of } F. \quad (8.1.3)$$

Case 1. Assume $\varphi(x) = x^{-1}$ for all $x \in G$. For all $g, h \in G$, we have

$$h^{-1}g^{-1} = (gh)^{-1} = \varphi(gh) \in \{\varphi(g)h^{\pm 1}\} = \{g^{-1}h^{\pm 1}\} \subseteq g^{-1}\langle h \rangle, \quad (8.1.4)$$

so g normalizes $\langle h \rangle$. Since g and h are arbitrary elements of G , this implies that every cyclic subgroup of G is normal, from which it follows that every subgroup of G is normal. Therefore, G is either abelian or Hamiltonian.

We may assume G is Hamiltonian, for otherwise G and φ are described in Example 8.1.1(a). So $G = Q_8 \times A \times B$, for some torsion abelian group A in which every element has odd order, and some group B of exponent dividing 2 (see Definition 2.1.5).

We may assume A is nontrivial, for otherwise G and φ are described in Example 8.1.1(c) (with $\varphi = \iota = \varphi_\emptyset$). Now, let a be a nontrivial element of A . For $g, h \in G$, the calculation in (8.1.4) shows that $h^{-1}g^{-1} \in \{g^{-1}h^{\pm 1}\}$. By taking inverses, we conclude that $gh \in \{h^{\pm 1}g\}$. Therefore, if $gh \neq hg$, then $gh = h^{-1}g$. Letting $g = j$ and $h = ia$, we conclude that

$$jia = gh = h^{-1}g = (ia)^{-1}j = a^{-1}i^{-1}j = (i^{-1}j)a^{-1},$$

since $i^{-1}j \in Q_8$ and $a^{-1} \in A$ commute (elements of Q_8 commute with elements of A), resulting in jia^{-1} . So $a = a^{-1}$. This contradicts the fact that every element of A has odd order.

Note. Henceforth, we may assume that Case 1 does not apply, so there is some $x \in G$, such that $\varphi(x) \neq x^{-1}$. Then $\varphi(x) = x$, so $x \in F$. Since $\varphi(x) \neq x^{-1}$, we also see that $x \neq x^{-1}$. Hence, inverting the elements of F is not the same as centralizing the elements of F . So we conclude from (8.1.3) that F contains its centralizer $C_G(F)$.

For any $q \in F^c$, we know that q^2 centralizes F (because q inverts F), so $q^2 \in C_G(F) \subseteq F$. This implies that q inverts q^2 . However, q obviously centralizes q^2 . So it must be the case that $q^{-2} = q^2$, which means $|q^2| \in \{1, 2\}$. However, we also know

from Lemma 2.5.11(2) that $|q| > 2$, since $\varphi(q) \neq q$. So we conclude that $|q^2| = 2$. Thus:

$$|q| = 4 \text{ for all } q \in F^c. \quad (8.1.5)$$

Furthermore, for all $g, h \in F^c$, we know that g and h both invert F , so $gh^{-1} \in C_G(F)$. This implies that all elements of F^c are in the same coset of $C_G(F)$:

$$F^c \subseteq C_G(F)q \text{ for all } q \in F^c.$$

Case 2. Assume F is a subgroup of G . We will show that G is of generalized dicyclic, and φ is the automorphism in Example 8.1.1(b).

Fix some $q \in F^c$.

- Since $F^c \subseteq C_G(F)q \subseteq Fq$, we see that all elements of F^c are in the same coset of F . This means $|G : F| = 2$.
- Since q inverts F , and conjugation by q is an automorphism, we see that inversion is an automorphism of F . This implies that F is abelian.
- Let $z = q^2$. We know from the above note that $|q| = 4$, so $|z| = 2$.

We have now established that $G = \text{Dic}(F, z, q)$.

So it only remains to show that $\varphi(q^i f) = q^{-i} f$ for all $i \in \mathbb{Z}$ and $f \in F$.

- If i is even, then $q^i f \in F$, so $\varphi(q^i f) = q^i f$. However, since i is even and $|q| = 4$, we also have $q^i = q^{-i}$.
- If i is odd, then $q^i f \in F^c$, so

$$\varphi(q^i f) = (q^i f)^{-1} = f^{-1} q^{-i} = q^{-i} f,$$

since q inverts every element of f (and i is odd).

Case 3. Assume F is not a subgroup of G . For convenience, let $C = C_G(F)$ be the centralizer of F . As mentioned in the above note, we have $C \subseteq F$, and we have $F^c \subseteq Cq$ for every $q \in F^c$.

Since $F^c \subseteq Cq$, we know that F contains all of the cosets of C except Cq . Also, since F is not a subgroup, we know that $\langle F \rangle$ is strictly larger than F , which means it contains some element of F^c , and therefore contains some element of Cq . Since $C \subseteq F$, this implies that $\langle F \rangle$ contains Cq . It also contains F , so it contains all of the other cosets of C , as well. Therefore $\langle F \rangle = G$. This implies that C is the centre of G .

Thus, all elements of F^c are in the same coset of the centre, so

the elements of F^c commute with each other.

Also recall (see (8.1.3)) that

every element of F^c inverts every element of F .

Now, let $f_1, f_2 \in F$. If $f_1 f_2 \notin F$, then it inverts both f_1 and f_2 , which implies that f_1 inverts f_2 and f_2 inverts f_1 . On the other hand, if $f_1 f_2 \in F$, then the conjugation action of any element of F^c respects multiplication, but inverts f_1 , f_2 , and $f_1 f_2$, so we must have $f_1 f_2 = f_2 f_1$. Therefore, if f_1 and f_2 are any elements of F , then

either f_1 and f_2 commute, or they invert each other.

Now consider any $f \in F$, such that $f \notin C$. Then $qf \notin qC$, so $qf \notin F^c$. This means $qf \in F$, so

$$qf = \varphi(qf) \in \{\varphi(q) f^{\pm 1}\} = \{q^{-1} f^{\pm 1}\},$$

so $q^2 \in \{1, f^{-2}\}$. However, we know from (8.1.5) that $|q| = 4$, so $q^2 \neq 1$. So we conclude that

$$q^2 = f^{-2}. \quad (8.1.6)$$

Therefore (recalling that q inverts f) we have

$$f^{-1}qf = f^{-2}q = q^2q = q^3 \in \langle q \rangle.$$

So f normalizes $\langle q \rangle$. Since this is also clearly true for the elements of F that are in C , we conclude that

$$\text{if } f \in F \text{ and } q \in F^c, \text{ then } f \text{ normalizes } \langle q \rangle.$$

We have now shown that g normalizes $\langle h \rangle$ for all $g, h \in G$. This means that every cyclic subgroup of G is normal. It follows easily that every subgroup of G is normal. (Also, G is not abelian, because elements of F^c invert elements of F .) Therefore G is a Hamiltonian group (see Definition 2.1.5).

We claim that G is a 2-group. To see this, write $G = Q_8 \times A \times B$, as in Definition 2.1.5. We wish to show that A is trivial. Suppose not. Then, since F contains all but one coset of the centre, there is some $f \in F$, such that $f \notin C$, and the A -component of f is nontrivial. From (8.1.6) we know that $|f^2| = 2$, which contradicts the fact that the A -component of f^2 is nontrivial.

All elements of the centre C of G have order 2. Therefore, since $\varphi(q) = q^{-1}$ (and φ is colour-preserving), we have $\varphi(qc) = \varphi(q)c^{\pm 1} = q^{-1}c = (qc)^{-1}$ for all $c \in C$. So F^c is the entire coset qC . Hence, F^c contains some $\ell \in \{i, j, k\}$. Then it is easy to see that φ is the permutation φ_I defined in Example 8.1.1(c), where $I = \{i, j, k\} \setminus \{\ell\}$. $\square$

The above theorem provides another proof of the (known) implication $(5 \Rightarrow 4)$ of

Theorem 8.0.1, which was discussed in Note 1.4.5(2) of the introduction.

Corollary 8.1.7 (Byrne et al. [6, cf. p. 324], Dobson et al. [9, Thm. 2.3]). *If the complete graph $\text{Cay}(G; G \setminus \{1\})$ is not CCA, then G is a Hamiltonian 2-group.*

Proof. Since $\text{Cay}(G; G \setminus \{1\})$ is not CCA, there exists a colour-preserving automorphism φ of this complete Cayley graph, such that φ is not affine. After composing with a translation, we may assume $\varphi(1) = 1$. Since φ is not affine, it is obviously not trivial, so Theorem 8.1.2 tells us that G is abelian or dicyclic, and that φ is one of the automorphisms in Example 8.1.1. However, since φ is not affine, it is not a group automorphism, so it is not listed in part (a) or (b) of that example. Hence, it must be part (c) that applies, so G is a Hamiltonian 2-group. $\square$

8.2 Complete graphs that are not strongly CCA

Notation 8.2.1. Let $\Gamma = \text{Cay}(G; S)$ be a Cayley graph of G .

1. $\mathcal{A}(\Gamma)$ is the group of all colour-permuting automorphisms of Γ .
2. $\mathcal{A}^0(\Gamma)$ is the group of all colour-preserving automorphisms of Γ .
3. $\mathcal{A}_1(\Gamma)$ and $\mathcal{A}_1^0(\Gamma)$ are the stabilizers of the vertex 1 in $\mathcal{A}(\Gamma)$ and $\mathcal{A}^0(\Gamma)$, respectively.
4. For $\varphi \in \mathcal{A}(\Gamma)$, and $g \in G$, let π_g^φ be the permutation of S that is induced by φ at the vertex g . That is, for all $s \in S$, we have

$$\varphi(gs) = \varphi(g) \pi_g^\varphi(s).$$

5. For $\varphi \in \mathcal{A}(\Gamma)$, let $\bar{\pi}^\varphi$ be the permutation of the colours that is induced by φ .

Thus, for all $g \in G$ and $s \in S$, we have

$$\bar{\pi}^\varphi(\{s^{\pm 1}\}) = \{\pi_g^\varphi(s)^{\pm 1}\}.$$

6. For $g \in G$, let ℓ_g be the left-translation by g , so $\ell_g(x) = gx$ for all $x \in G$. This is a colour-preserving automorphism of every Cayley graph of G .

We have the following elementary (and well-known) observation:

Lemma 8.2.2. *For $\varphi \in \mathcal{A}_1(\Gamma)$, we have $\varphi \in \text{Aut } G$ if and only if $\pi_g^\varphi = \pi_h^\varphi$ for all $g, h \in G$.*

Lemma 8.2.3. *Given $\varphi \in \mathcal{A}_1(\Gamma)$, $g \in G$, and $s \in S$, let*

$$\psi = \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} \ell_{\varphi(gs)}^{-1} \varphi \ell_{gs}.$$

Then $\psi \in \mathcal{A}_1^0(\Gamma)$ and $\psi(s) = s$.

Proof. It is clear that ψ is colour-permuting, because it is a composition of colour-permuting automorphisms. Furthermore, letting id denote a trivial permutation, we have

$$\begin{aligned} \overline{\pi}^\psi &= \overline{\pi}^{\ell_g^{-1}} \circ \overline{\pi}^{\varphi^{-1}} \circ \overline{\pi}^{\ell_{\varphi(g)}} \circ \overline{\pi}^{\ell_{\varphi(gs)}^{-1}} \circ \overline{\pi}^\varphi \circ \overline{\pi}^{\ell_{gs}} \\ &= \text{id} \circ \overline{\pi}^{\varphi^{-1}} \circ \text{id} \circ \text{id} \circ \overline{\pi}^\varphi \circ \text{id} \\ &= \overline{\pi}^{\varphi^{-1} \varphi} \\ &= \overline{\pi}^{\text{id}} \\ &= \text{id}. \end{aligned} \quad \left(\begin{array}{l} \text{translations are} \\ \text{colour-preserving} \end{array} \right)$$

So the colour-permuting automorphism ψ is actually colour-preserving.

Also, a straightforward calculation shows that $\psi(\mathbf{1}) = \mathbf{1}$. Therefore $\psi \in \mathcal{A}_1^0(\Gamma)$.

Furthermore,

$$\begin{aligned}
 \psi(s^{-1}) &= \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} \ell_{\varphi(gs)}^{-1} \varphi \ell_{gs}(s^{-1}) \\
 &= \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} \ell_{\varphi(gs)}^{-1} \varphi(g) \\
 &= \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} (\varphi(gs)^{-1} \varphi(g)) \\
 &= \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} (\pi_g^\varphi(s)^{-1}) \\
 &= \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} (\pi_g^\varphi(s^{-1})) && \text{(Lemma 2.5.2(6b))} \\
 &= \ell_g^{-1} \varphi^{-1} (\varphi(gs^{-1})) \\
 &= \ell_g^{-1} (gs^{-1}) \\
 &= s^{-1}.
 \end{aligned}$$

So, $\psi(s) = s$. □

Lemma 8.2.4. *Let $\Gamma = \text{Cay}(G; S)$ be a Cayley graph of G , and let*

$$S^* = \{s \in S \mid \text{no nontrivial element of } \mathcal{A}_1^0(\Gamma) \text{ fixes } s\}.$$

If S^* generates G , then Γ is strongly CCA.

Proof. Given $\varphi \in \mathcal{A}_1(\Gamma)$, we wish to show that $\varphi \in \text{Aut } G$. Fix some $g \in G$ and $s \in S^*$, and, as in Lemma 8.2.3, let

$$\psi = \ell_g^{-1} \varphi^{-1} \ell_{\varphi(g)} \ell_{\varphi(gs)}^{-1} \varphi \ell_{gs}.$$

so $\psi \in \mathcal{A}_1^0(\Gamma)$ and $\psi(s) = s$. Since $s \in S^*$, it follows from the definition of S^* that ψ is the identity map. Thus, for all $t \in S$, we have $\psi(t) = t$, so, by the definition of ψ , we have

$$\ell_{\varphi(g)}^{-1} \varphi \ell_g(t) = \ell_{\varphi(gs)}^{-1} \varphi \ell_{gs}(t),$$

which means $\pi_g^\varphi(t) = \pi_{gs}^\varphi(t)$. Therefore $\pi_g^\varphi = \pi_{gs}^\varphi$. Since s is an arbitrary element

of S^* and S^* generates G , repeated application of this fact implies that $\pi_g^\varphi = \pi_h^\varphi$ for all $g, h \in G$. Therefore $\varphi \in \text{Aut}(G)$ (see Lemma 8.2.2). $\square$

Definition 8.2.5 ([38, p. 8]). A permutation group is *semiregular* if no nonidentity element of the group has any fixed points.

Corollary 8.2.6. *Let $\Gamma = \text{Cay}(G; S)$ be a connected Cayley graph of G . If the action of $\mathcal{A}_1^0(\Gamma)$ on S is semiregular, then Γ is strongly CCA.*

Proof. In this case, we have $S^* = S$. Since Γ is connected, we know that S generates G . $\square$

Corollary 8.2.7. *Let $\Gamma = \text{Cay}(G; S)$ be a Cayley graph of G . If $\mathcal{A}_1^0(\Gamma)$ is trivial, then Γ is strongly CCA.*

Proof. Any trivial permutation group is obviously semiregular, so this is almost immediate from Corollary 8.2.6. The only issue (which is minor) is that the corollary requires Γ to be connected. However, it is easy to see that if $\mathcal{A}_1^0(\Gamma)$ is trivial, then either Γ is connected, or Γ has only two vertices. $\square$

We can now establish the implication $(5 \Rightarrow 2)$ of Theorem 8.0.1.

Corollary 8.2.8. *If G is not a Hamiltonian 2-group, then $\text{Cay}(G; G \setminus \{1\})$ is strongly CCA.*

Proof. In the notation of Lemma 8.2.4, it suffices to show that $\langle S^* \rangle = G$.

To this end, let φ be a nontrivial element of $\mathcal{A}_1^0(\Gamma)$. By Theorem 8.1.2 (and the assumption that G is not a Hamiltonian 2-group), φ must be described in (a) or (b) of Example 8.1.1. Since each of these parts describes a unique automorphism, this implies that φ is the only nontrivial element of $\mathcal{A}_1^0(\Gamma)$. (Also note that $S = G \setminus \{1\}$ in the complete graph $\text{Cay}(G; G \setminus \{1\})$.) Therefore, we have

$$S^* = G \setminus F, \text{ where } F = \{g \in G \mid \varphi(g) = g\}.$$

Since φ is nontrivial, we know that F is a proper subset of G . Also, in both (a) and (b) of Example 8.1.1, it is easy to see that F is a subgroup of G . (In (a), it is the subgroup $\{x \in G \mid x^2 = \mathbf{1}\}$; in (b), it is the subgroup A .) Therefore, it is immediate from Lemma 2.1.6 that $\langle S^* \rangle = G$. $\square$

8.3 Colour-permuting automorphisms of $\text{Cay}(G; G \setminus \{\mathbf{1}\})$

In this section, we prove Theorem 1.4.7, which was stated in the introduction. For the reader's convenience, we state the result again here:

Theorem 8.3.1. *If G is any (finite or infinite) group, then every colour-permuting automorphism of the complete graph $\text{Cay}(G; G \setminus \{\mathbf{1}\})$ is the composition of a group automorphism and a colour-preserving graph automorphism.*

In other words (and using the symbols defined in Notation 8.2.1), we prove:

$$\mathcal{A}(\text{Cay}(G; G \setminus \{\mathbf{1}\})) = \text{Aut}(G) \cdot \mathcal{A}^0(\text{Cay}(G; G \setminus \{\mathbf{1}\})).$$

(Note that the order of the factors on the right-hand side does not matter (see Lemma 2.1.9).)

Proof of Theorem 8.3.1. Let $K_G = \text{Cay}(G; G \setminus \{\mathbf{1}\})$, and let φ be a colour-permuting automorphism of K_G . We wish to show that φ is the composition of a group automorphism and a colour-preserving graph automorphism. By composing φ with a translation, we may assume, without loss of generality, that $\varphi(\mathbf{1}) = \mathbf{1}$.

If K_G is strongly CCA, then φ must be a group automorphism. So the desired conclusion is true in this case.

We may now assume that K_G is not strongly CCA. By the contrapositive of Corollary 8.2.8, this implies that G is a Hamiltonian 2-group:

$$G = Q_8 \times B,$$

for some abelian group B of exponent ≤ 2 . Let $G_2 = \langle i^2, B \rangle$ be the subgroup generated by the elements of order 2 in G . (Recall that $i^2 = j^2 = k^2$ is the unique element of order 2 in Q_8 .) This is the centre of G , and it is an abelian group of exponent 2 that has index 4 in G . By Lemma 2.5.8, we have

$$\varphi(gx) = \varphi(g) \varphi(x) \text{ for all } g \in G \text{ and } x \in G_2.$$

Therefore

$$\varphi(G_2) = G_2, \text{ and the restriction of } \varphi \text{ to } G_2 \text{ is a group automorphism.} \quad (8.3.2)$$

Note that $\text{Cay}(G; \{i^{\pm 1}\})$ is a disjoint union of 4-cycles (because i has order 4). Hence, the isomorphic graph $\text{Cay}(G; \{\varphi(i)^{\pm 1}\})$ is also a disjoint union of 4-cycles, which means that $\varphi(i)$ has order 4. Therefore $\varphi(i)^{\pm 2} = i^2$, because $g^2 = i^2$ for all $g \in G$ of order 4. Also, we have $\varphi(i^2) \in \{\varphi(i)^{\pm 2}\}$ (see Corollary 2.5.3(1)). Combining these observations yields

$$\varphi(i^2) = i^2.$$

Now, let $\tilde{Q}_8 = \langle \varphi(i), \varphi(j) \rangle$, and define $\alpha: Q_8 \rightarrow G$ by

$$\alpha(i^m j^n) = \varphi(i)^m \varphi(j)^n.$$

(We will soon see that α is well-defined.) Since i and j have order 4 (and $\varphi \in \mathcal{A}_1(K_G)$), we know that $\varphi(i)$ and $\varphi(j)$ have order 4 (by the argument in the preceding paragraph). Also note that $i \notin j G_2$, so (8.3.2) implies that $\varphi(i) \notin \varphi(j) G_2$; hence, $\varphi(i)$ does not centralize $\varphi(j)$. However, any two elements of G either commute or invert each other; therefore $\varphi(i)$ and $\varphi(j)$ invert each other, so $\varphi(i)$ and $\varphi(j)$ satisfy

exactly the same relations as i and j . We conclude that

$$\alpha \text{ is a (well-defined) isomorphism from } Q_8 \text{ to } \tilde{Q}_8. \quad (8.3.3)$$

Also note that, for all $m, n \in \mathbb{Z}$, Corollary 2.5.3(2) implies

$$\varphi(i^m j^n) \in \{\varphi(i^m) \varphi(j)^{\pm n}\} \subseteq \{\varphi(i)^{\pm m} \varphi(j)^{\pm n}\} \subseteq \alpha(Q_8) = \tilde{Q}_8,$$

so $\varphi(Q_8) = \tilde{Q}_8$. Therefore, since $Q_8 \cap G_2 = \langle i^2 \rangle$, we see that

$$\tilde{Q}_8 \cap \varphi(G_2) = \varphi(Q_8) \cap \varphi(G_2) = \varphi(Q_8 \cap G_2) = \varphi(\langle i^2 \rangle) = \langle i^2 \rangle.$$

Since $\varphi(B) \subseteq \varphi(G_2)$ and $i^2 \notin B$, this implies $\tilde{Q}_8 \cap \varphi(B) = \{1\}$. Also, since the restriction of φ to G_2 is a group automorphism, we know that $\varphi(B)$ is a subgroup of G and we have $|G : \varphi(B)| = |G : B| = 8$; from this, we can conclude that $\tilde{Q}_8 \cdot \varphi(B) = G$. So we see from Lemma 2.1.7 that

$$G = \tilde{Q}_8 \times \varphi(B). \quad (8.3.4)$$

Define $\beta: G \rightarrow G$ by

$$\beta(qb) = \alpha(q) \varphi(b) \text{ for } q \in Q_8 \text{ and } b \in B.$$

We see from (8.3.2), (8.3.3), and (8.3.4) that β is an automorphism of G .

Now, let $\psi = \beta^{-1} \circ \varphi$. To complete the proof, we will show that ψ is a colour-preserving automorphism of $\text{Cay}(G; G \setminus \{1\})$. (This implies that, as desired, $\varphi = \beta \circ \psi$ is the composition of a group automorphism, namely β , and a colour-preserving graph automorphism, namely ψ .) First, note that ψ is a colour-permuting automorphism (because it is the composition of two colour-permuting automorphisms) and that

$\psi(\mathbf{1}) = \mathbf{1}$ (because β and φ both fix $\mathbf{1}$).

If $m, n \in \mathbb{Z}$, and n is odd, then conjugation by j^n inverts i^m , so

$$i^m j^{-n} = j^{-n} \cdot (j^n i^m j^{-n}) = j^{-n} \cdot i^{-m} = (i^m j^n)^{-1}.$$

On the other hand, if n is even, then $j^{-n} = j^n$, so $i^m j^{-n} = i^m j^n$. Thus, we have

$$i^m j^{-n} \in \{(i^m j^n)^{\pm 1}\} \text{ for all } m, n \in \mathbb{Z}. \quad (8.3.5)$$

Hence, for all $q \in Q_8$, we have

$$\begin{aligned} \varphi(q) &= \varphi(i^m j^n) && \text{(for some } m, n \in \mathbb{Z}) \\ &\in \{\varphi(i^m) \varphi(j)^{\pm n}\} && \text{(Corollary 2.5.3(2))} \\ &= \{\varphi(i)^m \varphi(j)^{\pm n}\} && \text{(Corollary 2.5.3(1) with } g = \mathbf{1}) \\ &= \{\beta(i)^m \beta(j)^{\pm n}\} && \text{(definitions of } \beta \text{ and } \alpha) \\ &= \{\beta(i^m j^{\pm n})\} && (\beta \text{ is a group homomorphism)} \\ &\subseteq \{\beta((i^m j^n)^{\pm 1})\} && ((8.3.5)) \\ &= \{\beta(q^{\pm 1})\} && \text{(definition of } m \text{ and } n) \\ &= \{\beta(q)^{\pm 1}\} && (\beta \text{ is a group homomorphism}). \end{aligned}$$

Therefore

$$\beta(q) \in \{\varphi(q)^{\pm 1}\} \text{ for all } q \in Q_8. \quad (8.3.6)$$

Now, for any $s \in G$, we have

$$\begin{aligned}
 \beta(s) &= \beta(qb) && \text{(for some } q \in Q_s \text{ and } b \in B) \\
 &= \beta(q) \beta(b) && (\beta \text{ is a group automorphism}) \\
 &\in \{\varphi(q)^{\pm 1} \beta(b)\} && (8.3.6) \\
 &= \{(\varphi(q) \beta(b))^{\pm 1}\} && \left(\begin{array}{l} \beta(b) \in G_2 \text{ has order 1 or 2} \\ \text{and is in the centre of } G \end{array} \right) \\
 &= \{(\varphi(q) \varphi(b))^{\pm 1}\} && \text{(definitions of } \beta \text{ and } \alpha) \\
 &= \{\varphi(qb)^{\pm 1}\} && \text{(Lemma 2.5.8)} \\
 &= \{\varphi(s)^{\pm 1}\} && \text{(definition of } q \text{ and } b).
 \end{aligned}$$

Since $\varphi(s^{-1}) = \varphi(s)^{-1}$ (by Corollary 2.5.3(1) with $g = \mathbf{1}$) and $\beta(s^{-1}) = \beta(s)^{-1}$ (because β is a group homomorphism), this implies

$$\varphi(\{s^{\pm 1}\}) = \beta(\{s^{\pm 1}\}) \text{ for all } s \in G.$$

Therefore, we have

$$\psi(\{s^{\pm 1}\}) = \beta^{-1}(\varphi(\{s^{\pm 1}\})) = \beta^{-1}(\beta(\{s^{\pm 1}\})) = \{s^{\pm 1}\}.$$

Hence, for all $g, s \in G$, we see from Corollary 2.5.3(2) that

$$\psi(gs) \in \{\psi(g) \psi(s^{\pm 1})\} = \{\psi(g) s^{\pm 1}\}.$$

This means that ψ is colour-preserving, as desired. □

We will close by showing that this theorem yields a direct proof of the implication $(4 \Rightarrow 2)$ of Theorem 8.0.1. However, this observation does not shorten any of our

arguments, because the logic is circular: the proof of Theorem 8.3.1 relies on the implication $(5 \Rightarrow 2)$ (i.e., it relies on Corollary 8.2.8), which is *a priori* stronger than $(4 \Rightarrow 2)$, because $(4 \Rightarrow 5)$ is trivial (see Note 1.4.5(1)).

Corollary 8.3.7. *If the complete graph $\text{Cay}(G; G \setminus \{1\})$ is CCA, then it is strongly CCA.*

Proof. Let φ be a colour-permuting automorphism of $\text{Cay}(G; G \setminus \{1\})$. By Theorem 8.3.1, we may write $\varphi = \psi \circ \alpha$, where ψ is a colour-preserving graph automorphism and $\alpha \in \text{Aut } G$. However, since $\text{Cay}(G; G \setminus \{1\})$ is CCA, we know that ψ is an affine map. Hence, φ is the composition of two affine maps, and is therefore affine. $\square$

We also mention the following simple observations.

Proposition 8.3.8. *$\text{Cay}(G; G \setminus 1)$ is a GRR if and only if $|G| \leq 2$.*

Proof. We know that the automorphism group of the complete graph $\text{Cay}(G; G \setminus 1)$ is $\text{Sym}(G)$. Then if $|G| = n$, then the order of the automorphism group is $n!$. Furthermore, $n! = n$ if and only if $n = 1$ or $n = 2$.

Therefore, the complete graph $\text{Cay}(G; G \setminus 1)$ is a GRR if and only if $|G| \leq 2$. $\square$

Proposition 8.3.9. *$\text{Cay}(G; G)$ is normal if and only if either $|G| \leq 3$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Note that every permutation of G is an automorphism of $\text{Cay}(G; G)$. Therefore, $\text{Cay}(G; G)$ is normal if and only if every permutation of G that fixes the identity element of G is an automorphism of G .

($\Leftarrow$). If G has only 1 or 2 elements, then the identity map is the only permutation of G that fixes the identity element, and this is obviously an automorphism of G . So $\text{Cay}(G; G)$ is normal.

Now we consider G with 3 elements $\{1, a, a^{-1}\}$. The only non identity permutation that fixes the identity element is the transposition (a, a^{-1}) . This is equal to the group automorphism $\varphi(x) = x^{-1}$. So $\text{Cay}(G; G)$ is normal.

For $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, we have $\text{Aut } G = \text{GL}_2(2)$, so $|\text{Aut } G| = 6 = |S_3|$. Hence, every permutation of the nonidentity elements of G comes from a group automorphism. So $\text{Cay}(G; G)$ is normal.

($\Rightarrow$). We prove the contrapositive: if $|G| \geq 4$ and $G \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then G is not normal.

Case 1. Assume $|G| = 4$. By assumption, we have $G \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so we conclude that $G \cong \mathbb{Z}_4 = \{0, 1, 2, 3\}$. Let $\varphi = (2 \ 3)$. Then φ is a permutation of $\mathbb{Z}_4$ that fixes 0, but it is not an automorphism of this group because

$$\varphi(1 + 1) = \varphi(2) = 3 \neq 2 = 1 + 1 = \varphi(1) + \varphi(1).$$

So, this Cayley graph is not normal.

Case 2. Assume $|G| \geq 5$. Choose two distinct non-zero elements a and b of G . Since $|G| \geq 5$, there exists $c \in G$ that is distinct from 0, a , b , and their sum, $a + b$.

Now, let φ be the permutation that interchanges c and $a + b$, but fixes all other elements of G . It is evident that φ is not a group automorphism because it fails to preserve the group operation. Specifically, we have $\varphi(a + b) = c$, which is not equal to $\varphi(a) + \varphi(b) = a + b$. Consequently, $\text{Cay}(G; G)$ is not normal. $\square$

Bibliography

- [1] Sheldon B. Akers and Balakrishnan Krishnamurthy. A group-theoretic model for symmetric interconnection networks. *IEEE Trans. Comput.*, 38(4):555–566, 1989.
- [2] Melanie Albert, Jenna Bratz, Patricia Cahn, Timothy Fargus, Nicholas Haber, Elizabeth McMahon, Jaren Smith, and Sarah Tekansik. Color-permuting automorphisms of Cayley graphs. *Congr. Numer.*, 190:161–171, 2008.
- [3] Shirin Alimirzaei and Dave Witte Morris. Colour-permuting automorphisms of complete Cayley graphs. *Art Discrete Appl. Math.*, 8(1):Paper No. 1.04, 18, 2025.
- [4] László Babai. Automorphism groups, isomorphism, reconstruction. In *Handbook of combinatorics, Vol. 1, 2*, pages 1447–1540. Elsevier Sci. B. V., Amsterdam, 1995.
- [5] Norman Biggs. *Algebraic graph theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1993.
- [6] David P. Byrne, Matthew J. Donner, and Thomas Q. Sibley. Groups of graphs of groups. *Beitr. Algebra Geom.*, 54(1):323–332, 2013.
- [7] Chong-yun Chao. On a theorem of Sabidussi. *Proc. Amer. Math. Soc.*, 15:291–292, 1964.
- [8] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.
- [9] Edward Dobson, Ademir Hujdurović, Klavdija Kutnar, and Joy Morris. On color-preserving automorphisms of Cayley graphs of odd square-free order. *J. Algebraic Combin.*, 45(2):407–422, 2017.
- [10] Edward Dobson, Pablo Spiga, and Gabriel Verret. Cayley graphs on abelian groups. *Combinatorica*, 36(4):371–393, 2016.
- [11] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.
- [12] Ahmed El-Amawy and Shahram Latifi. Properties and performance of folded hypercubes. *IEEE Transactions on Parallel and Distributed Systems*, 2(01):31–42, 1991.

-
- [13] Brandon Fuller. Finding CCA groups and graphs algorithmically. Master's thesis, University of Lethbridge, 2018.
- [14] Christopher D. Godsil. GRRs for nonsolvable groups. In *Algebraic methods in graph theory, Vol. I, II (Szeged, 1978)*, volume 25 of *Colloq. Math. Soc. János Bolyai*, pages 221–239. North-Holland, Amsterdam-New York, 1981.
- [15] Christopher D. Godsil. On the full automorphism group of a graph. *Combinatorica*, 1(3):243–256, 1981.
- [16] Christopher D. Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.
- [17] Dieter Hetzel. Über reguläre graphische darstellung von auflösbaren gruppen. Diplomarbeit, Technische Universität Berlin, 1976.
- [18] Ademir Hujdurović, Klavdija Kutnar, Dave Witte Morris, and Joy Morris. On colour-preserving automorphisms of Cayley graphs. *Ars Math. Contemp.*, 11(1):189–213, 2016.
- [19] Wilfried Imrich. Graphen mit transitiver Automorphismengruppe. *Monatsh. Math.*, 73:341–347, 1969.
- [20] Wilfried Imrich. Graphs with transitive abelian automorphism group. In P. Erdős, A. Rényi, and Vera T. Sós, editors, *Combinatorial Theory and its Applications, Vol. 2*, pages 651–656. North-Holland Publishing Co., 1970.
- [21] Wilfried Imrich. On graphs with regular groups. *J. Combinatorial Theory Ser. B*, 19(2):174–180, 1975.
- [22] Wilfried Imrich and M. E. Watkins. On automorphism groups of Cayley graphs. *Period. Math. Hungar.*, 7(3-4):243–258, 1976.
- [23] Josef Lauri and Raffaele Scapellato. *Topics in graph automorphisms and reconstruction*, volume 432 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, second edition, 2016.
- [24] Paul-Henry Leemann and Mikael de la Salle. Most rigid representation and Cayley index of finitely generated groups. *Electron. J. Combin.*, 29(4):Paper No. 4.40, 9, 2022.
- [25] Cai Heng Li. On isomorphisms of finite cayley graphs—a survey. *Discrete Mathematics*, 256(1-2):301–334, 2002.
- [26] Dave Witte Morris. *Advanced Abstract Algebra*. University of Lethbridge, Lethbridge, Canada, 2021. Available at <https://deductivepress.ca/dmorris/books/GradAlgebra-2021.pdf>.

-
- [27] Joy Morris. Colour-permuting and colour-preserving automorphisms. Talk at the 8th Slovenian Conference on Graph Theory, Kranjska Gora, Slovenia, June 21–27, 2015.
 - [28] Joy Morris and Josh Tymburski. Most rigid representations and Cayley index. *Art Discrete Appl. Math.*, 1(1):Paper No. 1.05, 12, 2018.
 - [29] S. Morteza Mirafzal. More odd graph theory from another point of view. *Discrete Math.*, 341(1):217–220, 2018.
 - [30] Lewis A. Nowitz and Mark E. Watkins. Graphical regular representations of non-abelian groups. I, II. *Canadian J. Math.*, 24:993–1008; *ibid.* 24 (1972), 1009–1018, 1972.
 - [31] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.
 - [32] Gert Sabidussi. Vertex-transitive graphs. *Monatsh. Math.*, 68:426–438, 1964.
 - [33] Changqun Wang, Dianjun Wang, and Mingyao Xu. Normal cayley graphs of finite groups. *Science in China Series A: Mathematics*, 41(3):242–251, 1998.
 - [34] Mark E. Watkins. On the action of non-Abelian groups on graphs. *J. Combinatorial Theory Ser. B*, 11:95–104, 1971.
 - [35] Mark E. Watkins. On graphical regular representations of $C_n \times Q$. In *Graph theory and applications (Proc. Conf., Western Michigan Univ., Kalamazoo, Mich., 1972; dedicated to the memory of J. W. T. Youngs)*, volume Vol. 303 of *Lecture Notes in Math.*, pages 305–311. Springer, Berlin-New York, 1972.
 - [36] Mark E. Watkins. Graphical regular representations of alternating, symmetric, and miscellaneous small groups. *Aequationes Math.*, 11:40–50, 1974.
 - [37] Arthur T. White. *Graphs, groups and surfaces*, volume 8 of *North-Holland Mathematics Studies*. North-Holland Publishing Co., Amsterdam, second edition, 1984.
 - [38] Helmut Wielandt. *Finite permutation groups*. Academic press, 1964.
 - [39] Wikipedia contributors. Dedekind group — Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Dedekind_group, 2025. Accessed April 15, 2025.
 - [40] Ming-Yao Xu. Some work on vertex-transitive graphs by Chinese mathematicians. In *Group theory in China*, volume 365 of *Math. Appl. (China Ser.)*, pages 224–254. Kluwer Acad. Publ., Dordrecht, 1996.

Appendix A

Computer programs

This chapter provides the source code of all programs used throughout this work. Each file is in a separate section, and the title of the section is the name of the file.

A.1 basic.sage

```
#This file provides basic definitions  
#used within other SageMath code.
```

```
Z2 = CyclicPermutationGroup(2)
```

```
Z3 = CyclicPermutationGroup(3)
```

```
Z4 = CyclicPermutationGroup(4)
```

```
Q8 = QuaternionGroup()
```

```
def cayleygraph(G,S):  
    """Construct a Cayley graph. The connection  
    set S does not need to be symmetric."""  
    V = list(G)  
    E = [[g, g*s] for g in V for s in S]  
    return Graph([V,E])
```

```
def CI(X):  
    "Calculate the Cayley index of the graph X"  
    return X.automorphism_group().order() // X.order()
```

```
def cayleyindex(G):
```

```

    "Find the Cayley index of G."
    Glist = []
    for g in G:
        if (g^-1 not in Glist) and (g != G.one()):
            Glist.append(g)
    return min(CI(cayleygraph(G,S))
               for S in Set(Glist).subsets())

def Dic(factors, z):
    """Construct a generalized dicyclic group. The abelian
    subgroup A of index 2 is specified by listing the
    orders of the factors in a representation of A as a
    direct product of cyclic groups.

    EXAMPLE::

        sage: Dic([4,5,6], (2,0,0))
        Dic(Z_4 x Z_5 x Z_6, (2, 0, 0))
        """
    gens = []
    q = []
    jumppoint = Integer(1)
    for ak,zk in zip(factors, z):
        # create a generator of order ak for the
        # abelian subgroup A
        gens.append(
            [tuple(range(jumppoint, jumppoint + ak)),
             tuple(range(jumppoint + 2*ak - 1,
                          jumppoint + ak - 1, -1))])
        # add another 4-cycle to the generator q
        # that inverts A
        for i in range(ak):
            q.append(
                (jumppoint + i,
                 jumppoint + i + ak,
                 jumppoint + ((i + zk) % ak),
                 jumppoint + ak + ((i + zk) % ak)))
        jumppoint = jumppoint + 2*ak
    gens.append(q)
    G = PermutationGroup(gens=gens, canonicalize=False)

    # provide a nice string representation of G
    Astring = " x ".join([f"Z_{n}" for n in factors])
    G._repr_ = lambda: f"Dic({Astring}, {z})"

```

```

    # verify that G is the correct dicyclic group
    Agens = G.gens()[:-1] # generators of the subgroup A
    A = G.subgroup(Agens)
    q = G.gens()[-1]      # generator q that inverts A

    # verify that A is abelian
    for a in Agens:
        for b in Agens:
            assert a * b == b * a, "A is not abelian"

    # Check that each generator of A has the correct order
    for gen, expected_order in zip(Agens, factors):
        assert gen.order() == expected_order, (
            f"Generator has order {gen.order()}, "
            + f"expected {expected_order}"
        )

    # Check that A has the correct order
    assert A.order() == prod(factors), "order of A incorrect"
    # Construct the expected z element in A
    expected_z = prod(gen^exp for gen, exp in zip(Agens, z))
    assert q^2 == expected_z, "q^2 != z"
    # verify that q inverts each generator of A
    for a in Agens:
        assert q * a * q^-1 == a^-1, f"q does not invert {a}"
    # verify that the order of G is 2 * |A|
    assert G.order() == 2 * A.order(), "Incorrect group order"

    return G

def is_normal_cayley_graph(G, S):
    """
    Determines whether the Cayley graph Cay(G; S)
    is normal.
    """
    # Build the Cayley graph
    X = cayleygraph(G, S)

    # Check that all automorphisms fixing identity are
    # group automorphisms
    for phi in X.automorphism_group():
        if phi(G.one()) != G.one():
            continue
        if not all(

```

```
        phi(g * h) == phi(g) * phi(h)
        for g in G
        for h in G
    ):
        return False

    return True
```

A.2 elementaryabelian.sage

```
# This program checks up to 100 random nonempty connection
# sets S for the groups Z_2, Z_2^5, Z_2^6, and Z_2^7.
# For each set S that it is considered, the program constructs the
    Cayley
# graph Cay(Z_2^n; S) and computes its Cayley index.
# When a set S is found with Cayley index 1, the
# program outputs G and S then moves on to the next group.
# If no such S is found for a particular G, then the program does
    not print anything for that group.
```

```
from sage.all import ZZ, AdditiveAbelianGroup, Graph
from random import sample
```

```
def cayleygraph(G, S):
    V = list(G)
    E = [[g, g + s] for g in V for s in S]
    return Graph([V, E])

def CI(X):
    """Calculate the Cayley index of the graph X"""
    return X.automorphism_group().order() // X.order()

def check_random_GRR(n):
    G = AdditiveAbelianGroup([2]*n)

    # non-identity elements
    e = G.identity()
    nonzero = [g for g in G if g != e]

    # random size of S
    k = ZZ.random_element(1, len(nonzero) + 1)

    # random connection set
```

```

    S = sample(nonzero, k)

    X = cayleygraph(G, S)

    return S if CI(X) == 1 else False

for n in [1, 5, 6, 7]:
    for _ in range(100):
        S = check_random_GRR(n)
        if S:
            print(f"G = Z_2^{n}, S={set(S)}")
            break

```

A.3 exceptional13groups.sage

*#We calculate the Cayley index and MRR connection sets for
#each of the 13 groups listed in Table 5.1 or Theorem 4.0.1.*

```

load("basic.sage")

# 1
Z2xZ2 = direct_product_permgroups([Z2,Z2])
z_1, z_2 = Z2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert Z2xZ2.subgroup([z_1,z_2])==Z2xZ2
print()
print(f"| (Z_2)^2 |: {Z2xZ2.order()}")
print(f"Cayley index of (Z_2)^2: {cayleyindex(Z2xZ2)}")
S = [z_1]
X = cayleygraph(Z2xZ2, S)
print(f"Cayley index of Cay((Z_2)^2; S) : {CI(X)}")

# 2
Z2xZ2xZ2 = direct_product_permgroups([Z2,Z2,Z2])
z_1, z_2, z_3 = Z2xZ2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert z_3.order() == 2
assert Z2xZ2xZ2.subgroup([z_1,z_2,z_3])==Z2xZ2xZ2
print()

```

```
print(f"| $(Z_2)^3$ |: {Z2xZ2xZ2.order()}")
print(f"Cayley index of  $(Z_2)^3$ : {cayleyindex(Z2xZ2xZ2)}")
S = [z_1, z_2, z_3]
X = cayleygraph(Z2xZ2xZ2, S)
print(f"Cayley index of Cay( $(Z_2)^3$ ; S): {CI(X)}")

# 3
Z2xZ2xZ2xZ2 = direct_product_permgroups([Z2,Z2,Z2,Z2])
z_1, z_2, z_3, z_4 = Z2xZ2xZ2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert z_3.order() == 2
assert z_4.order() == 2
assert Z2xZ2xZ2xZ2.subgroup([z_1, z_2, z_3, z_4]) == Z2xZ2xZ2xZ2
print()
print(f"| $(Z_2)^4$ |: {Z2xZ2xZ2xZ2.order()}")
print(f"Cayley index of  $(Z_2)^4$ : {cayleyindex(Z2xZ2xZ2xZ2)}")
S = [z_1, z_2, z_3, z_4, z_1*z_2, z_1*z_3, z_2*z_4]
X = cayleygraph(Z2xZ2xZ2xZ2, S)
print(f"Cayley index of Cay( $(Z_2)^4$ ; S): {CI(X)}")

# 4
D6 = DihedralGroup(3)
r, s = D6.gens()
assert D6.order() == 6
assert r.order() == 3      # rotation
assert s.order() == 2      # reflection
assert D6.subgroup([r, s]) == D6
print()
print(f"|D_6|: {D6.order()}")
print(f"Cayley index of D_6: {cayleyindex(D6)}")
S = [s, s*r]
X = cayleygraph(D6, S)
print(f"Cayley index of Cay(D_6; S): {CI(X)}")

# 5
D8 = DihedralGroup(4)
r, s = D8.gens()
assert D8.order() == 8
assert r.order() == 4      # rotation
assert s.order() == 2      # reflection
assert D8.subgroup([r, s]) == D8
```

```
print()
print(f"|D_8|: {D8.order()}")
print(f"Cayley index of D_8: {cayleyindex(D8)}")
S = [s, s*r]
X = cayleygraph(D8, S)
print(f"Cayley index of Cay(D_8; S):{CI(X)}")

# 6
D10 = DihedralGroup(5)
r, s = D10.gens()
assert D10.order() == 10
assert r.order() == 5      # rotation
assert s.order() == 2      # reflection
assert D10.subgroup([r, s]) == D10
print()
print(f"|D_10|: {D10.order()}")
print(f"Cayley index of D_10: {cayleyindex(D10)}")
S = [s, s*r]
X = cayleygraph(D10, S)
print(f"Cayley index of Cay(D_10; S):{CI(X)}")

# 7
A_4 = AlternatingGroup(4)
a = A_4("(1,2,3)")
a_inv = a^-1
b = A_4("(1,2)(3,4)")
print()
print(f"|A_4 |: {A_4.order()}")
print(f"Cayley index of A_4: {cayleyindex(A_4)}")
S = [a, b]
X = cayleygraph(A_4, S)
print(f"Cayley index of Cay(A_4; S):{CI(X)}")

# 8
H1 = PermutationGroup([
    [(1,6), (2,5), (3,4), (7,8)],      # a
    [(2,6), (4,8)],                  # b
    [(1,8), (2,7), (3,6), (4,5)]      # c
], canonicalize=False)
a, b, c = H1.gens()
assert a^2 == H1.identity(), "a^2 =1"
assert b^2 == H1.identity(), "b^2 =1"
```

```

assert c^2 == H1.identity(), "c^2 = 1"
assert a*b*c == b*c*a == c*a*b, "abc=bca=cab"
print()
print(f"|H_1|: {H1.order()}")
print(f"Cayley index of H_1: {cayleyindex(H1)}")
S = [a, b, c, a*b]
X = cayleygraph(H1, S)
print(f"Cayley index of Cay(H_1; S):{CI(X)}")

```

```

# 9
H2 = PermutationGroup([
    [(1,2,3,4,5,6,7,8)],      # a (8-cycle)
    [(2,6), (4,8)]            # b
], canonicalize=False)
a,b = H2.gens()
assert a^8 == H2.identity(), "a^8 = 1"
assert b^2 == H2.identity(), "b^2 = 1"
assert b * a * b == a^5, "bab = a^5"
print()
print(f"|H_2|: {H2.order()}")
print(f"Cayley index of H_2: {cayleyindex(H2)}")
S= [a, a^2, b]
X = cayleygraph(H2, S)
print(f"Cayley index of Cay(H_2; S):{CI(X)}")

```

```

# 10
H3 = PermutationGroup([
    [(1,2,3), (4,5,6), (7,8,9)],      # a
    [(1,4,7), (2,5,8), (3,6,9)],      # b
    [(1,9), (2,8), (3,7), (4,6)]      # c
], canonicalize=False)
a, b, c = H3.gens()
assert a^3 == H3.identity(), "a^3 = 1"
assert b^3 == H3.identity(), "b^3 = 1"
assert c^2 == H3.identity(), "c^2 = 1"
assert a * b == b * a, "ab = ba"
assert (a * c)^2 == H3.identity(), "(ac)^2 = 1"
assert (b * c)^2 == H3.identity(), "(bc)^2 = 1"
print()
print(f"|H_3|: {H3.order()}")
print(f"Cayley index of H_3: {cayleyindex(H3)}")
S = [a, c, a * c, b * c]
X = cayleygraph(H3, S)

```

```

print(f"Cayley index of Cay(H_3; S):{CI(X)}")

# 11
H4 = PermutationGroup([
    [(1,2,3), (4,5,6), (7,8,9)],          # a
    [(2,5,8), (3,9,6)],                  # b
    [(1,4,7), (2,5,8), (3,6,9)]          # c
], canonicalize=False)
a, b, c = H4.gens()
assert a^3 == H4.identity(), "a^3 = 1"
assert b^3 == H4.identity(), "b^3 = 1"
assert c^3 == H4.identity(), "c^3 = 1"
assert a * c == c * a, "ac = ca"
assert b * c == c * b, "bc = cb"
assert b^-1 * a * b == a*c, "b^-1ab=ac"
print()
print(f"|H_4|: {H4.order()}")
print(f"Cayley index of H_4: {cayleyindex(H4)}")
S = [a, b, a^-1 * b, b*a*b^-1]
X = cayleygraph(H4, S)
print(f"Cayley index of Cay(H_4; S):{CI(X)}")

# 12
i,j= Q8.gens()
Q8xZ3 = direct_product_permgroups([Q8, Z3])
i,j,z_1= Q8xZ3.gens()
assert i.order() == 4
assert j.order() == 4
assert z_1.order() == 3
assert Q8xZ3.subgroup([i,j,z_1])== Q8xZ3
print()
print(f"|Q_8 x Z_3|: {Q8xZ3.order()}")
print(f"Cayley index of Q_8 x Z_3: {cayleyindex( Q8xZ3)}")
S = [ i, i*z_1, j*z_1]
X = cayleygraph(Q8xZ3, S)
print(f"Cayley index of Cay((Q_8 x Z_3; S):{CI(X)}")

# 13
i,j= Q8.gens()
Q8xZ4 = direct_product_permgroups([Q8, Z4])
i,j,z_1= Q8xZ4.gens()

```

```
assert i.order() == 4
assert j.order() == 4
assert z_1.order() == 4
assert Q8xZ4.subgroup([i,j,z_1])== Q8xZ4
print()
print(f"|Q_8 x Z_4|: {Q8xZ4.order()}")
print(f"Cayley index of Q8xZ4: {cayleyindex(Q8xZ4)}")
S = [ i, j, z_1, i*z_1, j*i*z_1]
X = cayleygraph(Q8xZ4 , S)
print(f"Cayley index of Cay(Q_8 x Z_4; S):{CI(X)}")
```

A.4 smalldicyclic.sage

```
#This program checks up to 1000 random Cayley graphs
#of nonabelian generalized dicyclic group whose abelian
#subgroup of index 2 has order at most 48.
#It tries to find a connection set that gives Cayley
#index 2. If no such connection set is found
#after 1000 attempts, the program prints an error.
```

```
load("basic.sage")
```

```
from itertools import combinations_with_replacement
from random import sample
```

```
def cayleyindex_random(G, max_attempts=1000):
    """
    Estimate the Cayley index of a group G by
    checking up to 'max_attempts' random subsets of
    G \ {1} as connection sets for Cayley graphs.

    For each attempt, a random subset S is selected
    and the Cayley graph Cay(G; S) is constructed.
    The function tracks the smallest Cayley
    index encountered.

    Returns 2 immediately if a Cayley graph with
    index 2 is found. Otherwise, returns the minimum
    index observed after all attempts.
    """
    OrderOfAutG = G.gap().AutomorphismGroup().Order()
```

```
min_index = Infinity
Glist = []

for g in G:
    if (g^-1 not in Glist) and (g != G.one()):
        Glist.append(g)

attempts = 0
while attempts < max_attempts:
    subset_size = sample(
        range(1, len(Glist) + 1), 1)[0]
    S = Set(sample(Glist, subset_size))

    X = cayleygraph(G, S)
    CI_X = CI(X)

    if CI_X < min_index:
        min_index = CI_X

    if CI_X == 2:
        return min_index

    attempts += 1

return min_index

def generate_Dicyclic_groups(order):
    """
    Generate nonabelian generalized dicyclic groups of a given
    order. The function constructs all abelian groups A
    of index 2 whose order divides the given input
    'order', and returns groups of the form Dic(A, z),
    where z is an involution in A. Only non-abelian
    dicyclic groups are yielded.
    """
    prime_power_divisors = [1] + [d for d in order.divisors()
        if is_prime_power(d)]
    for factors in combinations_with_replacement(
        prime_power_divisors, order.bit_length()
    ):
        if prod(factors) == order:
            factors = [ZZ(d) for d in factors if d > 1]
            # ignore abelian groups
            if not any(k > 2 for k in factors):
```

```

        continue
    evens = [
        i for i in range(len(factors))
        if is_even(factors[i])]
    for one_set in Set(evens).subsets():
        if one_set:
            z = [
                factors[i] // 2
                if i in one_set else 0
                for i in range(len(factors))
            ]
            yield Dic(factors, z)

# Run the Search for Cayley Index 2
max_order = 48

for order in xrange(1, max_order + 1):
    for G in generate_Dicyclic_groups(order):
        if cayleyindex_random(G) == 2:
            print("          ", G)
        else:
            print("***** Error", G)

A.5  table5.3.sage

#For Dic(Z_4 x Z_4, (2,0)) and Dic(Z_8 x Z_4, (0,2)),
#we verify that the Cayley index
#obtained from the connection set given in Table 5.3 differs from
#the value listed in the table.

load("basic.sage")

#1
# Dic(Z_4 x Z_4, (2,0))
G = Dic([4,4], (2,0))
z1,z2,x = G.gens()
S = [z1, z2, z1*z2,x,z1*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4 x Z_4, (2,0)); S):{CI(X)}")

```

```

#2
# Dic(Z_8 x Z_4, (0,2))
G = Dic([8,4], (0,2))
z1,z2,x = G.gens()
S = [z1, z2,x,z1^5*x, z1^3*z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_8 x Z_4, (4,0)); S):{CI(X)}")

```

A.6 table5.6.sage

*#For each group in Table 5.6, we verify that the Cayley
#index of the group and the connection set for an MRR
#match the values listed in the table.*

```
load("basic.sage")
```

```

# Dic(Z_6, 3)
G = Dic([6], (3,))
z_1,x = G.gens()
print(f"Cayley index of Dic(Z_6, 3): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_6, 3); S):{CI(X)}")

```

```

# Dic(Z_8, 4)
G = Dic([8], (4,))
z_1,x = G.gens()
print()
print(f"Cayley index of Dic(Z_8, 4): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_8, 4); S):{CI(X)}")

```

```

# Dic(Z_10, 5)
G = Dic([10], (5,))
z_1,x = G.gens()
print()
print(f"Cayley index of Dic(Z_10, 5): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_10, 5); S):{CI(X)}")

```

```

# Dic(Z_4 x Z_2, (0,1))
G = Dic([4, 2], (0, 1))
z_1, z_2, x = G.gens()
print()
print(f"Cayley index of Dic(Z_4 x Z_2, (0,1)): {cayleyindex(G)}")
S = [z_1, x, z_1*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4 x Z_2, (0,1) ); S):{CI(X)}")

# Dic(Z_8 x Z_2, (4,0))
G = Dic([8,2], (4,0))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_8 x Z_2, (4,0)): {cayleyindex(G)}")
S = [z1, z2,x,z1*x,z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_8 x Z_2, (4,0)); S):{CI(X)}")

# Dic(Z_4 x Z_4, (2,0))
G = Dic([4,4], (2,0))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_4 x Z_4, (2,0)): {cayleyindex(G)}")
S = [z1*z2*x, z2^-1, z2^2, z1*z2^1, z1*x, z2^-1*x^-1]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4 x Z_4, (2,0)); S):{CI(X)}")

# Dic(Z_4 x (Z_2)^2, (0,1,0))
G = Dic([4,2,2], (0,1,0))
z1,z2,z3,x = G.gens()
print()
print(f"Cayley index of Dic(Z_4 x (Z_2)^2, (0,1,0)):
      {cayleyindex(G)}")
S = [z1, z3,x, z1*x,z3*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4 x (Z_2)^2, (0,1,0)); S):{CI(X)}")

# Dic(Z_6 x z_3, (3,0))
G = Dic([6,3], (3,0))

```

```

z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_6 x z_3, (3,0)): {cayleyindex(G)}")
S = [z1, z2,x,z2*x, z1*z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_6 x z_3, (3,0)); S):{CI(X)}")

# Dic(Z_8 x (Z_2)^2, (4,0,0))
# Define Dic(Z_8 x Z_2, (4,0))
G1 = Dic([8, 2], (4, 0))

# Create the direct product G1 x Z_2
G_prod = G1.direct_product(Z2)[0]

# Define Dic(Z_8 x (Z_2)^2, (4,0,0))
G_big = Dic([8, 2, 2], (4, 0, 0))

print()
# Check if they are isomorphic
iso = G_big.is_isomorphic(G_prod)
if iso:
    print("True, the groups are isomorphic.")
else:
    print("False , the groups are not isomorphic")

# Dic(Z_8 x Z_4, (4,0))
G = Dic([8,4], (4,0))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_8 x Z_4, (4,0)): {cayleyindex(G)}")
S = [z1, z2,x,z1^6*z2^-1*x, z1^5*z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_8 x Z_4, (4,0)); S):{CI(X)}")

# Dic(Z_8 x Z_4, (0,2))
G = Dic([8,4], (0,2))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_8 x Z_4, (0,2)): {cayleyindex(G)}")
S = [z1, z1^2*z2,x,z1^3*x,z2*x]
X = cayleygraph(G, S)

```

```

print(f"Cayley index of Cay(Dic(Z_8 x Z_4, (0,2)); S):{CI(X)}")

#Dic(Z_4^2 x Z_2, (2,0,0))
# Dic(Z_4 x Z_4, (2,0))
G1 = Dic([4, 4], (2, 0))
# Create the direct product G1 x Z_2
G_prod = G1.direct_product(Z2)[0]
# Define Dic(Z_4 x Z_4 x Z_2, (2,0,0))
G_big = Dic([4, 4, 2], (2, 0, 0))

print()
# Check if they are isomorphic
iso = G_big.is_isomorphic(G_prod)
print()
# Print result
if iso:
    print("True, the groups are isomorphic.")
else:
    print("False , the groups are not isomorphic")

# Dic(Z_4^2 x Z_2, (0,0,1))
G = Dic([4,4,2], (0,0,1))
z1,z2,z3,x = G.gens()
print()
print(f"Cayley index of Dic(Z_4^2 x Z_2, (0,0,1)): {cayleyindex(G)}")
S = [z1, z2,x,z2^3*x, z1^3*z2^2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4^2 x Z_2, (0,0,1)); S):{CI(X)}")

# Dic(Z_4 x Z_2^3, (0,1,0,0))
# Dic(Z_4 x Z_2^2, (0,1,0))
G1 = Dic([4, 2, 2], (0, 1, 0))

# Create the direct product G1 x Z_2
G_prod = G1.direct_product(Z2)[0]

# Define Dic(Z_4 x Z_2^3, (0,1,0,0))
G_big = Dic([4, 2, 2, 2], (0, 1, 0, 0))

print()

```

```

# Check if they are isomorphic
iso = G_big.is_isomorphic(G_prod)
if iso:
    print("True, the groups are isomorphic.")
else:
    print("False , the groups are not isomorphic")

# Dic(Z_12 x Z_3, (6,0))
G = Dic([12,3], (6,0))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_12 x Z_3, (6,0)): {cayleyindex(G)}")
S = [z1, z2,x,z1^7*z2*x, z1^3*z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay( Dic(Z_12 x Z_3, (6,0)); S):{CI(X)}")

# Dic(Z_6 x Z_3, (3,0))
G1 = Dic([6, 3], (3, 0))

# Create the direct product G1 x Z_2
G_prod = G1.direct_product(Z2)[0]

# Dic(Z_6 x Z_6, (3,0))
G_big = Dic([6, 6], (3, 0))

print()
# Check if they are isomorphic
iso = G_big.is_isomorphic(G_prod)
if iso:
    print("True, the groups are isomorphic.")
else:
    print("False , the groups are not isomorphic")

#Dic(Z_12 X Z_4, (6,0))
G = Dic([12,4], (6,0))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_12 x Z_4, (6,0)): {cayleyindex(G)}")
S = [z1, z2,x,z1^4*z2*x, z1^9*z2^3*x]
X = cayleygraph(G, S)

```

```

print(f"Cayley index of Cay(Dic(Z_12 X Z_4, (6,0)); S):{CI(X)}")

# Dic(Z_12 X Z_4, (0,2))
G = Dic([12,4], (0,2))
z1,z2,x = G.gens()
print()
print(f"Cayley index of Dic(Z_12 x Z_4, (0,2)): {cayleyindex(G)}")
S = [z1,x,z1^3*z2,z1*x, z1*z2*x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_12 X Z_4, (0,2)); S):{CI(X)}")

```

A.7 table5.5elementaryabelian.sage

*#This program verifies the Cayley index and the connection
#set of an MRR of Z_2 , Z_2^2 and the seven exceptional
#abelian groups in Theorem 5.0.5.*

```

load("basic.sage")

# 1
z_1 = Z2.gens()[0]
assert z_1.order() == 2
print()
print(f"|Z_2|: {Z2.order()}")
print(f"Cayley index of Z_2: {cayleyindex(Z2)}")
S = []
X = cayleygraph(Z2, S)
print(f"Cayley index of Cay(Z_2; S): {CI(X)}")

# 2
Z2xZ2 = direct_product_permgroups([Z2,Z2])
z_1, z_2 = Z2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert Z2xZ2.subgroup([z_1,z_2])==Z2xZ2
print()
print(f"| (Z_2)^2 |: {Z2xZ2.order()}")
print(f"Cayley index of (Z_2)^2: {cayleyindex(Z2xZ2)}")

```

```
S = [z_1]
X = cayleygraph(Z2xZ2, S)
print(f"Cayley index of Cay((Z_2)^2; S) : {CI(X)}")

# 3
Z2xZ2xZ2 = direct_product_permgroups([Z2,Z2,Z2])
z_1, z_2, z_3 = Z2xZ2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert z_3.order() == 2
assert Z2xZ2xZ2.subgroup([z_1,z_2,z_3])==Z2xZ2xZ2
print()
print(f"| (Z_2)^3 |: {Z2xZ2xZ2.order()}")
print(f"Cayley index of (Z_2)^3: {cayleyindex(Z2xZ2xZ2)}")
S = [z_1, z_2, z_3]
X = cayleygraph(Z2xZ2xZ2, S)
print(f"Cayley index of Cay((Z_2)^3; S): {CI(X)}")

# 4
Z2xZ2xZ2xZ2 = direct_product_permgroups([Z2,Z2,Z2,Z2])
z_1, z_2, z_3, z_4 = Z2xZ2xZ2xZ2.gens()
assert z_1.order() == 2
assert z_2.order() == 2
assert z_3.order() == 2
assert z_4.order() == 2
assert Z2xZ2xZ2xZ2.subgroup([z_1,z_2,z_3, z_4])==Z2xZ2xZ2xZ2
print()
print(f"| (Z_2)^4 |: {Z2xZ2xZ2xZ2.order()}")
print(f"Cayley index of (Z_2)^4: {cayleyindex(Z2xZ2xZ2xZ2)}")
S = [z_1, z_2, z_3, z_4, z_1*z_2, z_1*z_3, z_2*z_4]
X = cayleygraph(Z2xZ2xZ2xZ2, S)
print(f"Cayley index of Cay((Z_2)^4; S): {CI(X)}")

# 5
Z4xZ2 = direct_product_permgroups([Z4,Z2])
z_1, z_2 = Z4xZ2.gens()
assert z_1.order() == 4
assert z_2.order() == 2
assert Z4xZ2.subgroup([z_1,z_2])==Z4xZ2
print()
print(f"| Z_4 x Z_2 |: {Z4xZ2.order()}")
print(f"Cayley index of Z_4 x Z_2: {cayleyindex(Z4xZ2)}")
```

```

S = [z_1, z_2]
X = cayleygraph(Z4xZ2, S)
print(f"Cayley index of Cay(Z_4 x Z_2; S):{CI(X)}")

# 6
Z4xZ2xZ2 = direct_product_permgroups([Z4,Z2,Z2])
z_1, z_2, z_3 = Z4xZ2xZ2 .gens()
assert z_1.order() == 4
assert z_2.order() == 2
assert z_3.order() == 2
assert Z4xZ2xZ2 .subgroup([z_1,z_2,z_3])==Z4xZ2xZ2
print()
print(f"|Z4xZ2xZ2|: {Z4xZ2xZ2.order()}")
print(f"Cayley index of Z_4x(Z_2)^2:{cayleyindex(Z4xZ2xZ2 )}")
S = [ z_1, z_2, z_3, z_1* z_2, z_1* z_3]
X = cayleygraph(Z4xZ2xZ2, S)
print(f"Cayley index of Cay(Z_4 x (Z_2)^2 ; S):{CI(X)}")

# 7
Z3xZ3 = direct_product_permgroups([Z3,Z3])
z_1, z_2 = Z3xZ3 .gens()
assert z_1.order() == 3
assert z_2.order() == 3
assert Z3xZ3 .subgroup([z_1,z_2])== Z3xZ3
print()
print(f"|Z_3 x Z_3|: {Z3xZ3.order()}")
print(f"Cayley index of (Z_3)^2: {cayleyindex(Z3xZ3 )}")
S = [ z_1, z_2]
X = cayleygraph(Z3xZ3, S)
print(f"Cayley index of Cay((Z_3)^2; S):{CI(X)}")

# 8
Z3xZ3xZ3 = direct_product_permgroups([Z3,Z3,Z3])
z_1, z_2, z_3 = Z3xZ3xZ3 .gens()
assert z_1.order() == 3
assert z_2.order() == 3
assert z_3.order() == 3
assert Z3xZ3xZ3 .subgroup([z_1,z_2,z_3])== Z3xZ3xZ3
print()
print(f"|Z_3 x Z_3 x Z_3|: {Z3xZ3xZ3.order()}")
print(f"Cayley index of (Z_3)^3: {cayleyindex(Z3xZ3xZ3 )}")

```

```

S = [ z_1, z_2, z_3, z_1*z_2, z_1*z_3, z_2*z_3]
X = cayleygraph(Z3xZ3xZ3, S)
print(f"Cayley index of Cay((Z_3)^3 ; S):{CI(X)}")

# 9
Z4xZ4 = direct_product_permgroups([Z4,Z4])
z_1, z_2 = Z4xZ4 .gens()
assert z_1.order() == 4
assert z_2.order() == 4
assert Z4xZ4 .subgroup([z_1,z_2])==Z4xZ4
print()
print(f"|Z_4 x Z_4|: {Z4xZ4.order()}")
print(f"Cayley index of Z_4 x Z_4: {cayleyindex(Z4xZ4 )}")
S = [ z_1, z_2, z_1^2, z_1* z_2]
X = cayleygraph(Z4xZ4, S)
print(f"Cayley index of Cay(Z_4 x Z_4; S):{CI(X)}")

```

A.8 table5.5Hamiltonian2-group.sage

*#This program verifies the Cayley index and the connection
#set of an MRR of Q_8 and $Q_8 \setminus \text{times } Z_2$.*

```
load("basic.sage")
```

```

# 1
i,j= Q8.gens()
assert i.order() == 4
assert j.order() == 4
assert Q8.subgroup([i,j])== Q8
print()
print(f"|Q_8|: {Q8.order()}")
print(f"Cayley index of Q_8: {cayleyindex(Q8)}")
S = [i]
X = cayleygraph(Q8, S)
print(f"Cayley index of Cay(Q_8 ; S):{CI(X)}")

```

```

# 2
Q8xZ2= direct_product_permgroups([Q8, Z2])
i,j,z_1= Q8xZ2.gens()
assert i.order() == 4

```

```

assert j.order() == 4
assert z_1.order() == 2
assert Q8xZ2.subgroup([i,j,z_1])== Q8xZ2
print()
print(f"|Q_8 x z_2|: {Q8xZ2.order()}")
print(f"Cayley index of Q_8 x Z_2: {cayleyindex(Q8xZ2)}")
S = [ i, j, z_1, i*z_1,i^-1*z_1 ]
X = cayleygraph(Q8xZ2, S)
print(f"Cayley index of Cay(Q_8 x Z_2; S):{CI(X)}")

```

A.9 table5.5exceptionaldicycllic.sage

*#We verify the Cayley index and the connection set of an
#MRR of each of the corresponding exceptional groups in
#Lemma 5.0.7.*

```
load("basic.sage")
```

```

# 1
G = Dic([6], (3,))
z_1,x = G.gens()
assert z_1.order() == 6
assert x.order() == 4
assert x * z_1 * x^-1 == z_1^-1
assert x^2 == z_1^3,"x^2 must equal the involution (3,)"
print()
print(f"|Dic(Z_6, 3)|: {G.order()}")
print(f"Cayley index of Dic(Z_6, 3): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_6, 3); S):{CI(X)}")

```

```

# 2
G = Dic([8], (4,))
z_1,x = G.gens()
assert z_1.order() == 8
assert x.order() == 4
assert x * z_1 * x^-1 == z_1^-1
assert x^2 == z_1^4,"x^2 must equal the involution (4,)"
print()
print(f"|Dic(Z_8, 4)|: {G.order()}")

```

```

print(f"Cayley index of Dic(Z_8, 4): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_8, 4); S):{CI(X)}")

# 3
G = Dic([10], (5,))
z_1, x = G.gens()
assert z_1.order() == 10
assert x.order() == 4
assert x * z_1 * x^-1 == z_1^-1
assert x^2 == z_1^5, "x^2 must equal the involution (5,)"
print()
print(f"|Dic(Z_10, 5)|: {G.order()}")
print(f"Cayley index of Dic(Z_10, 5): {cayleyindex(G)}")
S = [z_1, x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_10, 5); S):{CI(X)}")

# 4
G = Dic([4, 2], (0, 1))
z_1, z_2, x = G.gens()
assert z_1.order() == 4
assert z_2.order() == 2
assert x.order() == 4
assert x * z_1 * x^-1 == z_1^-1
assert x * z_2 * x^-1 == z_2^-1
assert x^2 == z_2, "x^2 must equal the involution (0,1)"
print()
print(f"|Dic(Z_4 x Z_2, (0,1))|: {G.order()}")
print(f"Cayley index of Dic(Z_4 x Z_2, (0,1)): {cayleyindex(G)}")
S = [z_1, x, z_1 * x]
X = cayleygraph(G, S)
print(f"Cayley index of Cay(Dic(Z_4 x Z_2, (0,1)); S):{CI(X)}")

```

A.10 Z4xZ2.sage

```

# This program verifies that the group Z_4 x Z_2 does
# not have a normal Cayley graph. It tries all subsets S of
#G \ {1}, by using is_normal_cayley_graph(G, S)
#to test whether any Cayley graph Cay(G; S) is normal.

```

```
load("basic.sage")

def has_normal_cayley_graph(G):
    r"""
    Verify whether G has a normal Cayley graph
    by checking all subsets of  $G \setminus \{1\}$ . It
    builds Cayley graphs and checks if any
    of them are normal.
    """
    Glist = [g for g in G if g != G.one()]
    for S in Set(Glist).subsets():
        if is_normal_cayley_graph(G, S):
            return True
    return False

#  $Z_4 \times Z_2$ 
G = direct_product_permgroups([Z4, Z2])
print(has_normal_cayley_graph(G))
```

A.11 table6.1.sage

*#This program verifies that each connection set in Table
#6.1 gives a normal Cayley graph for the corresponding
#group.*

```
load("basic.sage")

# $(Z_2)^3$ 
G = direct_product_permgroups([Z2] * 3)
z_1, z_2, z_3 = G.gens()
S = [z_1, z_2, z_3]
print()
print("(Z_2)^3:", is_normal_cayley_graph(G, S))

# $(Z_2)^4$ 
G = direct_product_permgroups([Z2] * 4)
z_1, z_2, z_3, z_4 = G.gens()
S = [z_1, z_2, z_3, z_4]
print()
print("(Z_2)^4:", is_normal_cayley_graph(G, S))
```

```
#(Z_4)^2
G = direct_product_permgroups([Z4,
Z4])
z_1, z_2 = G.gens()
S = [ z_1^2 * z_2^3, z_1^3 * z_2^3, z_1^3 ]
print()
print("(Z_4)^2:", is_normal_cayley_graph(G, S))
```

```
# Z_4 x (Z_2)^2
G = direct_product_permgroups([Z4,
Z2,Z2])
z_1, z_2, z_3 = G.gens()
S = [z_1^2*z_3, z_1^3*z_3, z_2*z_3, z_1^2*z_2]
print()
print("Z_4 x (Z_2)^2:", is_normal_cayley_graph(G, S))
```

```
# (Z_3)^2
G=direct_product_permgroups([Z3]*2)
z_1, z_2 = G.gens()
S= [z_1^2*z_2^2, z_2^2]
print()
print("(Z_3)^2:", is_normal_cayley_graph(G, S))
```

```
# (Z_3)^3
G=direct_product_permgroups([Z3]*3)
z_3, z_2, z_1 = G.gens()
S = [z_1, z_2, z_3]
print()
print("(Z_3)^3:", is_normal_cayley_graph(G, S))
```

```
#Dic(Z_6,3)
G = Dic([6], (3,))
z_1,q= G.gens()
S = [z_1, q]
print()
print("Dic(Z_6,3):", is_normal_cayley_graph(G, S))
```

```
#Dic(Z_8,4)
G = Dic([8], (4,))
```

```
z_1, q= G.gens()
S = [z_1, q]
print()
print("Dic(Z_8,4):", is_normal_cayley_graph(G, S))
```

```
#Dic(Z_10,5)
G = Dic([10], (5,))
z_1, q= G.gens()
S = [z_1, q]
print()
print("Dic(Z_10,5):", is_normal_cayley_graph(G, S))
```

```
#Dic(Z_4 x Z_2, (0,1))
G = Dic([4, 2], (0, 1))
z_1, z_2, q = G.gens()
S=[z_1^3, z_1^2*q^3, z_1*q^3]
print()
print("Dic(Z_4 x Z_2, (0,1)):", is_normal_cayley_graph(G, S))
```