

INTEGRAL CAYLEY GRAPHS

by

Azhvan Ahmady

M.Sc., Sharif University of Technology, 2006

B.Sc., Teacher Training University, 2004

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Doctor of Philosophy

in the
Department of Mathematics
Faculty of Science

© Azhvan Ahmady 2013
SIMON FRASER UNIVERSITY
Summer 2013

All rights reserved.

However, in accordance with the *Copyright Act of Canada*, this work may be reproduced without authorization under the conditions for “Fair Dealing.” Therefore, limited reproduction of this work for the purposes of private study, research, criticism, review and news reporting is likely to be in accordance with the law, particularly if cited appropriately.

APPROVAL

Name: Azhvan Ahmady

Degree: Doctor of Philosophy

Title of Thesis: Integral Cayley Graphs

Examining Committee: Dr. Karen Yeats, Assistant Professor
Chair

Dr. Bojan Mohar, Professor
Senior Supervisor

Dr. Jason Bell, Professor
Supervisor

Dr. Ladislav Stacho, Associate Professor
SFU Examiner

Dr. Joel Friedman, Professor of Mathematics,
University of British Columbia,
External Examiner

Date Approved: August 22nd, 2013

Partial Copyright Licence



The author, whose copyright is declared on the title page of this work, has granted to Simon Fraser University the right to lend this thesis, project or extended essay to users of the Simon Fraser University Library, and to make partial or single copies only for such users or in response to a request from the library of any other university, or other educational institution, on its own behalf or for one of its users.

The author has further granted permission to Simon Fraser University to keep or make a digital copy for use in its circulating collection (currently available to the public at the "Institutional Repository" link of the SFU Library website (www.lib.sfu.ca) at <http://summit/sfu.ca> and, without changing the content, to translate the thesis/project or extended essays, if technically possible, to any medium or format for the purpose of preservation of the digital work.

The author has further agreed that permission for multiple copying of this work for scholarly purposes may be granted by either the author or the Dean of Graduate Studies.

It is understood that copying or publication of this work for financial gain shall not be allowed without the author's written permission.

Permission for public performance, or limited permission for private scholarly use, of any multimedia materials forming part of this work, may have been granted by the author. This information may be found on the separately catalogued multimedia material and in the signed Partial Copyright Licence.

While licensing SFU to permit the above uses, the author retains copyright in the thesis, project or extended essays, including the right to change the work for subsequent purposes, including editing and publishing the work in whole or in part, and licensing other parties, as the author may desire.

The original Partial Copyright Licence attesting to these terms, and signed by this author, may be found in the original bound copy of this work, retained in the Simon Fraser University Archive.

Simon Fraser University Library
Burnaby, British Columbia, Canada

revised Fall 2011

Abstract

A graph X is said to be integral if all eigenvalues of the adjacency matrix of X are integers. This property was first defined by Harary and Schwenk who suggested the problem of classifying integral graphs. Since the general problem of classifying integral graphs seemed too difficult, graph theorists started to investigate special classes of graphs which included trees, graphs of bounded degree, regular graphs and Cayley graphs. What proves so interesting about this problem is that no one can yet identify what the integral trees are or which 5-regular graphs are integral. In this thesis, integral Cayley graphs are studied. Several topics on the integral Cayley graphs are presented. First, a classification of integral Cayley graphs over abelian groups in terms of the associated Boolean algebra of the subgroups is presented. Secondly, the notions of character and representation integrality are introduced. It has been shown that character integrality is a weaker notion than representation integrality. An internal classification of character integral subsets is proved. General results about representation integral subsets are presented and in an attempt to generalize the results from abelian to non-abelian case, Hamiltonian and dihedral groups are studied. Thirdly, two open problems about integrality of Cayley graphs are solved. Simple eigenvalues in Cayley graphs are studied, and some observations lead to two interesting results in this topic. Finally, the classification of cubic and 4-regular integral Cayley graphs are presented. A general approach to characterize all integral Cayley graphs over abelian groups is presented. Furthermore, a sharp upper bound over the size of the group in terms of the graph degree has been suggested and proved. The thesis concludes with a section devoted to open problems and conjectures in this area.

To Sweet Penguin

Acknowledgments

Firstly, I would like to thank my advisor, Bojan Mohar, for all his help and guidance that he has given me throughout my graduate studies. I would like to show my sincere gratitude to Jason Bell, my supervisor from whom I have learned a great deal and from his enthusiasm for mathematics I have greatly benefited.

I want to thank my great friends Azad Shokri, for being a good chiropractor and cracking my back many times, and Sophie Burrill who has been very supportive and has made my studies in SFU enjoyable. My family has always been very supportive of my academic career. Their constant love and encouragement have always been with me, for which I am very grateful. Special thanks goes to my love Skyler M. Warren for all of her support during the writing of this thesis.

Contents

Approval	ii
Partial Copyright License	iii
Abstract	iv
Dedication	v
Acknowledgments	vi
Contents	vii
List of Figures	x
1 Preliminaries	1
1.1 Introduction	1
1.1.1 Graphs	2
1.1.2 Linear Algebra	5
1.1.3 Group theory and Algebra	7
1.2 Overview of the thesis	12
2 Integral Cayley graphs over abelian groups	13
2.1 Introduction	14
2.2 Integral Cayley graphs	18
2.3 B -integrality	21
2.4 Integral Cayley graphs over abelian groups	24

3	Integral Cayley graphs over non-abelian groups	27
3.1	Introduction	27
3.2	Character and representation integrality	30
3.3	Hamiltonian groups	37
3.4	Some special cases	40
3.4.1	Simple Cayley graphs of $Q_8 \times C_p$, where $p \neq 3$	40
3.4.2	$Q_8 \times C_3$	43
3.4.3	Cayley multigraphs of $Q_8 \times C_p$	43
3.4.4	Simple Cayley graphs of $Q_8 \times C_p^d$	45
3.5	Dihedral groups	47
3.5.1	Irreducible representations of D_n	47
3.5.2	The case D_p where p is a prime number	50
3.5.3	The general case	52
4	CIS and Cayley integral groups	54
4.1	Introduction	54
4.2	Cayley integral simple groups	56
4.3	Cayley Integral Groups	62
5	Integral Cayley graphs of small degree	78
5.1	Abelian groups admitting integral Cayley graphs of small degree	79
5.2	Non-abelian groups admitting cubic integral Cayley graphs	86
5.3	Non-abelian groups admitting 4-regular integral Cayley graphs	89
6	Miscellaneous results	94
6.1	Cayley graphs with small number of distinct eigenvalues	94
6.2	Simple eigenvalues in Cayley graphs	96
6.3	Open problems and conjectures	100
	Appendix A Representation theory in GAP	102
A.1	Representation theory of non-abelian groups of order 12	103
A.2	Representation theory of non-abelian groups of order 18	106
A.3	Representation theory of non-abelian groups of order 24	111

Appendix B Cayley graphs programming	133
B.1 Spectrum computation with GAP	133
B.2 Cayley graph construction with GRAPE	137
B.3 $(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ admits no connected cubic integral Cayley graph	139
Bibliography	143

List of Figures

2.1	Non-cubic connected integral graphs with $\Delta \leq 3$	16
2.2	Tutte 8-cage, smallest cubic graph of girth 8	17
2.3	Complete Gray Code in hypercube Q_4	18
5.1	Connected cubic bipartite integral graphs.	92
5.2	Connected cubic non-bipartite integral graphs.	93

Chapter 1

Preliminaries

1.1 Introduction

A graph essentially is a discrete mathematical model of a network of objects. For example, such objects can be cities, computers, atoms, or those that are more abstract. Graphs are applied in numerous fields, like chemistry, social science, electrical engineering, architecture, computer science and many others. Roughly speaking, a graph is a set of vertices representing the nodes of the network (cities, computers or atoms), and a set of edges between vertices. These edges can represent roads between cities, links between computers, or bonds between atoms. These edges may have weights, representing distances, capacities, forces, and they can be directed (one-way roads). There is a large variety of problems in graph theory. One classic example is the famous traveling salesman problem: given a list of cities and the distances between each pair of cities, what is the shortest possible route to visit each city exactly once and return to the origin city? For small graphs this problem may seem easy, but as the number of vertices increases, the problem becomes very difficult. Such problem can be applied to quite different areas, for example in planning, logistics, and the manufacture of microchips or DNA sequencing, the process of determining the precise order of nucleotides within a DNA molecule. One way to cope with the difficulty of working with large graphs is to use computers. In order to read and store graphs into computers we represent graphs with matrices.

Depending on the specific problem and personal preference, graph theorists use different kinds of matrices to represent a graph, the most popular ones being the $(0, 1)$ -adjacency matrix and the Laplace matrix. Often, the algebraic properties of the matrix are used as a

bridge between different kinds of structural properties of the graph. The relation between the structural (combinatorial, topological) properties of the graph and the algebraic ones of the corresponding matrix is therefore a very interesting one. For example, using the spectrum of light, scientists have had great success in being able to indirectly determine the compounds of chemicals that could not be directly measured. For instance, by examining the light given off by stars we can determine their chemical composition, even though we could never directly gather any material from those stars. Another interesting example is from theoretical chemistry, where chemists associate a graph with hydrocarbon molecule. The eigenvalues of the matrix of this graph are used to predict stability of the molecule. In an analogous way we can use the spectra of various matrices (i.e., the eigenvalues of the matrices) to get information about a graph that would otherwise be difficult to obtain.

In this chapter, we will provide some introductory comments about connections between the eigenvalues of matrices and the properties of graphs in a general setting. The study of the relations between these two objects is spectral graph theory. Thus to work in spectral graph theory, one not only need to be familiar with graph theory but also must understand the basic tools from algebra. Eigenvalues, eigenvectors, determinants, Courant-Fischer formula, Perron-Frobenius and others are the tools of the trade.

In this thesis we study special classes of graphs which have a lot of structure. In the eye of the mathematical beholder, graphs with significant structure and symmetry are the most beautiful graphs. Cayley graphs are the main graphs we study and they are used in many different areas. In computer science Cayley graphs are used for the design and analysis of network architectures for parallel computers. Of course, the application of Cayley graphs in an area like computer science is not limited to just this example. We refer readers interested in further applications of Cayley graphs in computer science to [11, 21, 20].

1.1.1 Graphs

A *graph* (or sometimes a *multi-graph*) $\Gamma = (V, E)$ consists of a set V of *vertices* and a set E of *edges* and a relation that associates with each edge two vertices called its *endpoints*. We only consider graphs with finite set of vertices and edges. The edge $uv \in E$ joins vertices u and v , and u and v are called the *endpoints* of the edge uv . We use $u \sim v$ to show there is an edge between u and v . A *loop* is an edge $vv \in E$ from a vertex v to itself. *Multiple edges* are edges having the same pair of endpoints. A *simple* graph is a graph which does not have any loop or multiple edges. All graphs studied in this thesis are simple unless otherwise

stated. The *order* of Γ is the number of vertices of Γ and the *size* of Γ is the number of edges. Vertices u and v are said to be *adjacent* or *neighbors* if they are the endpoints of the same edge. The *degree* of a vertex v , denoted by $\deg(v)$, is the number of neighbors of v . The maximum degree of a graph Γ , denoted by $\Delta(\Gamma)$, is the maximum degree of its vertices. If all vertices have the same degree then the graph is called *regular*. We say a graph is *complete* if any two vertices are adjacent, and *empty* if no two vertices are adjacent. The *complement* $\bar{\Gamma}$ of a graph Γ is the graph on the same vertices, but with complementary edge set, that is, two vertices are adjacent in Γ if they are not adjacent in $\bar{\Gamma}$. Two graphs are called *isomorphic* if there is a bijection between the respective vertex sets preserving edges.

A *subgraph* of a graph Γ is a graph X such that $V(X) \subseteq V(\Gamma)$ and $E(X) \subseteq E(\Gamma)$. If for a subgraph X of Γ we have $V(X) = V(\Gamma)$ then we call X a *spanning* subgraph and we say X spans Γ . If S is a subset of V , then the *induced* subgraph of Γ on S , denoted by $\Gamma[S]$, is the subgraph of Γ with vertex set S and edge set consists of those edges in Γ that both their endpoints are contained in S . We use $\Gamma - S$ instead of $\Gamma[V - S]$, if $S = \{v\}$ then $\Gamma - \{v\}$ will be shortened to $\Gamma - v$. An *independent* set is a set of vertices which induces empty subgraph, and a *clique* is an induced complete subgraph. A graph is called *bipartite* if the vertices can be partitioned into two induced independent sets.

If two graphs are isomorphic, then we shall (in general) not distinguish between them, or even call them the same. An *automorphism* of a graph is a bijection from the vertex set to itself preserving edges. The set of automorphisms of a graph, with the composition operator, forms a group, called the *automorphism group*.

A *walk* of length k from vertex u to vertex v (referred to as a (u, v) -walk) is a sequence of, not necessarily distinct, vertices $u = u_0, u_1, \dots, u_k = v$, such that for any i ($0 \leq i < k$) the vertices u_i and u_{i+1} are adjacent. We call u and v the endpoints, and u_i for $1 \leq i < k$ the internal vertices of the walk. If $u = v$, the walk is called a *closed* walk. If all vertices are distinct then the walk is called a *path*. A *cycle* is a closed walk that all internal vertices are distinct from each other and the end point. The *girth* of a graph is the length of its shortest cycle. If the graph does not have any cycles, its girth is infinite. If there is a path between any two vertices of the graph, then the graph is called *connected*. The maximal connected subgraphs of G are called the *components* of Γ . The *distance* between two vertices is the length of the shortest path between these vertices. The maximal distance taken over all pairs of vertices is called the *diameter* of the graph.

The *line graph* $L(\Gamma)$ of a simple graph Γ is obtained by associating a vertex with each

edge of the graph and connecting two vertices with an edge if the corresponding edges of Γ have a vertex in common.

Suppose Γ_1 and Γ_2 are two simple graphs with disjoint vertex sets V_1 and V_2 and edge sets E_1 and E_2 . The *join* of graphs Γ_1 and Γ_2 , denoted by $\Gamma_1 \nabla \Gamma_2$, is the graph with the vertex set $V_1 \cup V_2$ and the edge set consisting of those in E_1 and E_2 together with all the edges joining V_1 and V_2 .

The *Cartesian product* (denoted by $\Gamma_1 \square \Gamma_2$) of two simple graphs Γ_1 and Γ_2 has the vertex-set $V(\Gamma_1) \times V(\Gamma_2)$. For $u, v \in V(\Gamma_1)$ and $x, y \in V(\Gamma_2)$, (u, x) is adjacent to (v, y) if either “ $u = v$ and $xy \in E(\Gamma_2)$ ” or “ $uv \in E(\Gamma_1)$ and $x = y$ ”.

The *tensor product* of graphs Γ_1 and Γ_2 denoted by $\Gamma_1 \times \Gamma_2$, is a graph with the vertex-set $V(\Gamma_1) \times V(\Gamma_2)$. For $u, v \in V(\Gamma_1)$ and $x, y \in V(\Gamma_2)$, (u, x) is adjacent to (v, y) in $\Gamma_1 \times \Gamma_2$ if “ $uv \in E(\Gamma_1)$ and $xy \in E(\Gamma_2)$ ”.

If Γ_1 and Γ_2 are (simple) graphs on the disjoint vertex sets V_1 and V_2 and edge sets E_1 and E_2 respectively, then we denote by $\Gamma_1 \dot{\cup} \Gamma_2$ the simple graph with vertex set $V = V_1 \cup V_2$ and edge set $E = E_1 \cup E_2$. The graph $\Gamma_1 \dot{\cup} \Gamma_2$ is called the *disjoint union* of Γ_1 and Γ_2 . The notation $n\Gamma$ will represent the disjoint union of n copies of Γ .

Let Γ be a graph of order n . The *adjacency matrix* of Γ is the matrix $A(\Gamma) \in \mathbb{R}^{V \times V}$ whose (u, v) -entry is equal to 1 if u is adjacent to v and 0 otherwise. Occasionally we consider multi-graphs (possibly with loops) in which case (u, v) -entry is equal to the number of edges from u to v . The spectrum of a graph Γ is by definition the spectrum of the adjacency matrix $A(\Gamma)$, that is, its set of eigenvalues together with their multiplicities. If $\lambda_1(\Gamma), \dots, \lambda_n(\Gamma)$ are the eigenvalues of Γ we assume they are in the non-increasing order, that is:

$$\lambda_1(\Gamma) \geq \dots \geq \lambda_n(\Gamma).$$

If $\lambda_1(\Gamma), \dots, \lambda_r(\Gamma)$ are the distinct eigenvalues of Γ with multiplicities k_1, \dots, k_r respectively, then we denote the spectrum of Γ by:

$$\text{Spec}(\Gamma) = [\lambda_1^{k_1}, \dots, \lambda_r^{k_r}].$$

The *characteristic polynomial* of Γ is that of $A(\Gamma)$. Graphs with the same spectrum are called *co-spectral*.

1.1.2 Linear Algebra

In this subsection, we discuss a number of results from linear algebra used throughout the thesis. We use the standard notation in accordance with the book [33]. I_n will denote the identity matrix of order n , and J_n will denote a (square) matrix of order n with all entries equal to 1. j_n will denote a vector of size n with all components equal 1. If the order of the matrices or vectors are clear from the context, we will drop the subscripts and we will use I , J or j to show the identity matrix, all ones matrix or all ones vector of the assumed order. We use $\text{tr}(A)$ to denote the trace of a square matrix A , and $\det(A)$ or $|A|$ to denote the determinant of A . All properties of trace and determinant are assumed. For two matrices A and B we denote their *Kronecker product* or *tensor product* by $A \otimes B$.

We begin with definitions of eigenvalues and eigenvectors for matrices in general. For completeness we first define Hermitian adjoint, Hermitian and normal matrices. Let $A = [a_{ij}]$ be a matrix over the field of complex numbers, \mathbb{C} . The *transpose* of A , denoted by A^T is the matrix over the same field as A , with (i, j) -entry equal to a_{ji} (that is, rows are exchanged for columns and vice versa).

The *Hermitian adjoint* A^* of A is defined by $A^* = (\bar{A})^T$, where \bar{A} is the entry-wise conjugate of A . A complex square matrix A is a *Hermitian* (or *self-adjoint*) matrix if it is equal to its own Hermitian adjoint, i.e., $A = A^* = (\bar{A})^T$. A complex square matrix A is a *normal* matrix if $A^*A = AA^*$. A real Hermitian matrix is called a (real) *symmetric* matrix. It should be added that if A is a real matrix, $A^* = A^T$ and so it is normal if $A^T A = A A^T$. Every Hermitian matrix, and hence every real symmetric matrix is normal.

Let A be an $n \times n$ matrix over \mathbb{C} . We consider the equation

$$A\mathbf{x} = \lambda\mathbf{x}, \quad \mathbf{x} \neq 0,$$

where \mathbf{x} is an $n \times 1$ vector and λ is a scalar. If a scalar λ and a non-zero vector \mathbf{x} happen to satisfy this equation, then λ is called an *eigenvalue* of A and \mathbf{x} is called an *eigenvector* of A associated with λ . The set of all eigenvalues is called the *spectrum* of A . The set of eigenvectors of A associated with the eigenvalue λ together with the zero vector is called the *eigenspace* associated with λ . The dimension of this space is called the *geometric multiplicity* of A . On the other hand, the *algebraic multiplicity* of A is the multiplicity of A as a root of the polynomial $\det(A - \lambda I)$. For Hermitian matrices the two multiplicities of A are equal.

As the adjacency matrix of a graph is a Hermitian matrix, we do not distinguish between geometric and algebraic multiplicity and speak solely about the multiplicity of an eigenvalue.

If $\mathbf{x} = (x_v) \in \mathbb{R}^V$ is an eigenvector of $A(\Gamma)$ corresponding to the eigenvalue λ then, we have $A(\Gamma)\mathbf{x} = \lambda\mathbf{x}$, which we can express as:

$$\lambda x_v = \sum_{u \sim v} x_u \quad (v \in V).$$

The following are some basic results from linear algebra. See [23] for more details.

Theorem 1.1.1. *Let A be a real $n \times n$ symmetric matrix. Then*

- *two eigenvectors of A with different eigenvalues are orthogonal.*
- *all eigenvalues of A are real numbers.*
- *\mathbb{R}^n has an orthonormal basis consisting of eigenvectors of A .*

Theorem 1.1.2. (Simultaneous diagonalization) *Suppose \mathcal{F} is a collection of commuting $n \times n$ Hermitian matrices (i.e., $AB = BA$ for $A, B \in \mathcal{F}$), then \mathbb{C}^n has a basis consisting of common eigenvectors of all $A \in \mathcal{F}$.*

Consider two sequences of real numbers: $\lambda_1 \geq \dots \geq \lambda_n$, and $\mu_1 \geq \dots \geq \mu_m$ with $m < n$. The second sequence *interlaces* the first one whenever

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i} \quad \text{for } i = 1, \dots, m.$$

Let $A \in \mathbb{R}^{V \times V}$, where $|V| = n$. Let $0 < m \leq n$, a $m \times m$ symmetric minor of A is the matrix obtained from A by restricting V to a subset U of size m . That is to say, a symmetric minor of A on U obtained by deleting all rows and columns from A which are indexed by elements of $V \setminus U$.

Theorem 1.1.3. (Interlacing eigenvalues) *Let A be an $n \times n$ symmetric matrix with eigenvalues $\lambda_1 \geq \dots \geq \lambda_n$. Let B be an $(n - k) \times (n - k)$ symmetric minor of A with eigenvalues $\mu_1 \geq \dots \geq \mu_{n-k}$, then the sequence of eigenvalues of B interlaces the sequence of eigenvalues of A . i.e.*

$$\lambda_i \geq \mu_i \geq \lambda_{i+k} \quad \text{for } i = 1, \dots, n - k.$$

Since adjacency matrix of an induced subgraph of Γ is a symmetric minor of the adjacency matrix of Γ , we can apply the interlacing theorem to induced subgraphs. Thus for any induced subgraph X of Γ , the sequence of eigenvalues (in non-increasing order) of X interlaces the sequence of eigenvalues (in non-increasing order) of Γ . A useful characterization of the eigenvalues is given by the *Rayleigh's* and *Courant-Fisher's* formula (see [23] for more details).

- $\lambda_n(A) = \min\{\mathbf{x}^T A \mathbf{x} \mid \mathbf{x} \in \mathbb{R}^V, \|\mathbf{x}\| = 1\}$
- $\lambda_1(A) = \max\{\mathbf{x}^T A \mathbf{x} \mid \mathbf{x} \in \mathbb{R}^V, \|\mathbf{x}\| = 1\}$
- $\lambda_{n-k+1}(A) = \min\{\max\{\mathbf{x}^T A \mathbf{x} \mid \mathbf{x} \in \mathbb{R}^W, \|\mathbf{x}\| = 1\} \mid \dim(W) = k\}$

Theorem 1.1.4. (Perron-Frobenius) *If an $n \times n$ matrix has nonnegative entries then it has a nonnegative real eigenvalue λ which has maximum absolute value among all eigenvalues. This eigenvalue λ has a nonnegative real eigenvector. If, in addition, the matrix has no block-triangular decomposition (i.e., it does not contain a $k \times (n - k)$ block of 0-s disjoint from the diagonal), then it has multiplicity 1 and the corresponding eigenvector is positive.*

In the following theorem, the eigenvalues of Hermitean matrices A and B are arranged in non-increasing order.

Theorem 1.1.5. (Weyl inequalities) *Let A and B be Hermitian matrices of order n , and let $1 \leq i, j \leq n$.*

- 1) *If $i + j - 1 \leq n$ then $\lambda_{i+j-1}(A + B) \leq \lambda_i(A) + \lambda_j(B)$.*
- 2) *If $i + j - n \geq 1$ then $\lambda_i(A) + \lambda_j(B) \leq \lambda_{i+j-n}(A + B)$.*

1.1.3 Group theory and Algebra

In this section we will introduce the basic notation and properties of Algebraic structures which we will use throughout the thesis. We are assuming the basic understanding of the most common algebraic structures like groups, rings and algebras. Our notation and definitions for groups has taken from [47], for rings and algebras from [34]. All groups considered are finite written multiplicatively (unless otherwise stated), and all fields are subfields of the complex numbers. The letters G , H and K are reserved for groups and subgroups unless otherwise stated. We use 1 to denote both *identity* element and *trivial* subgroup $\{1\}$, the distinction will be clear from the context. $H \leq G$ means H is a *subgroup* of G and $H \trianglelefteq G$ means H is a

normal subgroup of G . If g and h are elements of the group G , then $g^h = h^{-1}gh$ denotes the *conjugate* of g by h . The set of all conjugates of g in G is called the *conjugacy class* of g and is denoted by $\text{cl}_G(g)$. We denote the *order* of an element g in G by $\text{ord}(g)$, and the order of the group G by $|G|$. The *exponent* of a group is defined as the least common multiple of the orders of all elements of the group. If there is no least common multiple, the exponent is taken to be infinity. We denote the *centralizer* of a subset S of G by $C_G(S)$, which is the set of all elements of G that commute with each element of S . When $S = \{g\}$ is a singleton set, then $C_G(\{g\})$ will be abbreviated to $C_G(g)$. We denote the *center* of a group G by $Z(G)$, which is $\bigcap_{g \in G} C_G(g)$. Let S be a subset of G , then the subgroup generated by S denoted by $\langle S \rangle$ is defined as the smallest subgroup of G containing S . Thus, $\langle S \rangle$ is the intersection of all subgroups containing S . If $G = \langle S \rangle$, then we call S a generating set for G or a set of generators of G . When $S = \{a\}$, is a singleton, then $\langle \{a\} \rangle$ will be shortened to $\langle a \rangle$ and this called the *cyclic* subgroup generated by a . A group is *cyclic* if it is generated by a single element. In all the group theory notation, the group in the subscripts will be deleted when there is no danger of confusion or when the group is clear from the context. The notations $[G : H]$, G' and $[g, h]$ are stand for (respectively); the index of the subgroup H in G , the derived subgroup of G and the commutator of g and h which is $g^{-1}h^{-1}gh$.

If $G = H \times K$, then π_H (the canonical projection on H) is defined as follows:

$$\pi_H : H \times K \rightarrow H, \quad \pi_H(h, k) = h \quad \text{for all } (h, k) \in H \times K.$$

The canonical projection on K is similarly defined and is denoted by π_K . We denote the *group algebra* of G over the field \mathbb{F} by $\mathbb{F}G$. That is, $\mathbb{F}G$ is the vector space over \mathbb{F} with basis G and multiplication defined by extending the group multiplication linearly. Therefore, $\mathbb{F}G$ is the set of all formal sums $\sum_{g \in G} a_g g$ where $a_g \in \mathbb{F}$ and we assume $1 \cdot g = g$ to have $G \subseteq \mathbb{F}G$. We multiply elements of $\mathbb{F}G$ according to multiplication in G , so we have

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g \in G} \sum_{h \in G} a_g b_h gh.$$

With this, $\mathbb{F}G$ will become an \mathbb{F} -algebra of dimension $|G|$. Identifying $\sum_{g \in G} a_g g$ with the function $g \mapsto a_g$, we can view the vector space $\mathbb{F}G$ as the space of all \mathbb{F} -valued functions on G . We sometimes identify a subset S of G with the element $\sum_{s \in S} s$ of the group algebra $\mathbb{C}G$.

Let V be a finite dimensional \mathbb{F} -vector space. A *linear representation* (or simply a representation) of G on V is a group homomorphism $\rho : G \mapsto GL_{\mathbb{F}}(V)$, where $GL_{\mathbb{F}}(V)$

denotes the group of invertible \mathbb{F} -linear operators on V . The degree of representation is the dimension of V . Let $M_n(\mathbb{F})$ be the algebra of all $n \times n$ matrices over \mathbb{F} , where $n = \dim(V)$. If we pick an ordered basis for V and denote the matrix corresponding to $\rho(g)$ by $\tilde{\rho}(g)$, then $\tilde{\rho}$ is a group homomorphism from G to $M_n(\mathbb{F})$. Two representations ρ_1 and ρ_2 of G on V_1 and V_2 respectively, are *equivalent* if there is a linear isomorphism T from V_1 onto V_2 such that

$$T\rho_1(g) = \rho_2(g)T \quad \forall g \in G$$

If ρ is a representation of G , then the *character afforded* by ρ (denoted by χ_ρ) is the linear functional on $\mathbb{F}G$ such that $\chi_\rho(g) = \text{tr}(\rho(g))$ for each g in G . It is clear that characters are *class functions* (functions which are constant on the conjugacy classes) and the set of characters will span the space of all class functions on G . By degree of χ_ρ we mean the degree of ρ which is simply $\chi_\rho(1)$. A character of degree one is called a *linear character*.

The *left regular representation* ρ_{reg} of G on $V = \mathbb{F}G$ is defined by

$$\rho_{reg}(g) : \mathbb{F}G \mapsto \mathbb{F}G, \quad \rho_{reg}(g) \left(\sum_{h \in G} a_h h \right) = \sum_{h \in G} a_h gh.$$

If W is a $\rho(g)$ -invariant subspace of V for each $g \in G$, then we call W a $\rho(G)$ -invariant subspace of V . If we restrict each $\rho(g)$ to W , we will get $\rho_W : G \mapsto GL(W)$ which is a linear representation of G on W called the *subrepresentation* of ρ on W . If V has no $\rho(G)$ -invariant subspace, we call ρ an *irreducible* representation of G and the corresponding character χ_ρ an *irreducible* character of G . If $V = W_1 \oplus W_2$ and both W_1 and W_2 are $\rho(G)$ -invariant subspaces of V , then we write $\rho = \rho_{W_1} \oplus \rho_{W_2}$ and we say ρ is a direct sum of ρ_{W_1} and ρ_{W_2} . If we pick an ordered basis β_1 for W_1 and an ordered basis β_2 for W_2 , and order them according to (β_1, β_2) , then the relation between corresponding matrix representations of ρ , ρ_{W_1} and ρ_{W_2} is as follows:

$$\tilde{\rho}(g) = \begin{bmatrix} \tilde{\rho}_{W_1}(g) & 0 \\ 0 & \tilde{\rho}_{W_2}(g) \end{bmatrix}.$$

According to a theorem of *Maschke*, every representation of G can be decomposed into a direct sum of irreducible sub-representations.

Theorem 1.1.6. *If ρ_1, \dots, ρ_k are a complete set of non-equivalent irreducible representations*

of G , then

$$\rho_{\text{reg}} = \bigoplus_{i=1}^k m_i \rho_i,$$

where m_i is the degree of ρ_i .

For a group G , we denote by $\text{IRR}(G)$ and $\text{Irr}(G)$ a complete set of non-equivalent irreducible representations of G (over the field \mathbb{C}) and the complete set of non-equivalent irreducible characters of G , respectively. Note that $\text{IRR}(G)$ is not necessarily unique, but $\text{Irr}(G)$ is unique. It is easy to see that $|\text{IRR}(G)| = h(G)$ where $h(G)$ is the *class number* of G counting the number of conjugacy classes of G . If G is abelian, then every irreducible representation $\rho \in \text{IRR}(G)$ is 1-dimensional and thus it can be identified with its character $\chi_\rho \in \text{Irr}(G)$.

Let G and G' be finite groups and $\rho : G \mapsto GL(V)$, $\rho' : G' \mapsto GL(V')$ be two (complex) representations corresponding to G and G' . We define $\rho \times \rho'$ as

$$\rho \times \rho' : G \times G' \mapsto GL(V \otimes V')$$

$$(\rho \times \rho')(g, g') = \rho(g) \otimes \rho'(g')$$

for all $(g, g') \in G \times G'$.

Theorem 1.1.7. *Let $\text{IRR}(G) = \{\rho_1, \dots, \rho_k\}$ and $\text{IRR}(G') = \{\rho'_1, \dots, \rho'_k\}$. Then*

$$\text{IRR}(G \times G') = \{\rho_i \times \rho'_j \mid 1 \leq i \leq h(G), 1 \leq j \leq h(G')\}.$$

If G is abelian, then each ρ_i is a homomorphism from G to \mathbb{F} so $(\rho_i \times \rho'_j)(g, g') = \rho_i(g) \otimes \rho'_j(g') = \rho_i(g)\rho'_j(g')$ (under the assumption that $1 \otimes v := v$ and so $\mathbb{F} \otimes V = V$).

Theorem 1.1.8. *Let ρ be a matrix representation of G affording the character χ and let $g \in G$ such that $\text{ord}(g) = n$. Then*

1. $\rho(g)$ is similar to a diagonal matrix $\text{diag}(\epsilon_1, \dots, \epsilon_k)$.
2. $\epsilon_i^n = 1$ for $1 \leq i \leq k$.
3. $\chi(g) = \sum_{i=1}^k \epsilon_i$ and $|\chi(g)| \leq \chi(1)$.
4. $\chi(g^{-1}) = \overline{\chi(g)}$.

Theorem 1.1.9. (*Orthogonality Relations*) Let $g, h \in G$ and $\chi_i, \chi_j \in \text{Irr}(G)$. Then

1. $\sum_{g \in G} \chi_i(g) \overline{\chi_j(g)} = \delta_{ij} |G|.$
2. $\sum_{\chi \in \text{Irr}(G)} \chi(g) \overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate} \\ 0 & \text{otherwise} \end{cases}$

Theorem 1.1.10. If χ_{reg} is the character afforded by the regular representation ρ_{reg} of G . Then

$$\chi_{reg}(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{otherwise} \end{cases}$$

We notice that if $N \trianglelefteq G$, then there is a one-to-one correspondence between representations of G/N and representations of G with kernel containing N . Furthermore, under this correspondence, irreducible representations correspond to irreducible representations.

1.2 Overview of the thesis

The rest of the thesis is organized as follows. In the second chapter, we discuss the known results in the literature and motivate some problems. We will present a new proof of the characterization of Cayley integral graphs over abelian groups. In chapter three, we will extend our results from Chapter 2 to some classes of non-abelain groups. We will consider integrality notion from different perspectives. Chapter four is totally devoted to two classification problems. In chapter five, we classify groups which admit connected integral Cayley graphs of small degree. Chapter six is a collection of miscellaneous results and a list of conjectures and open problems in this area.

Chapter 2

Integral Cayley graphs over abelian groups

The notion of the integral graphs was first introduced by Harary and Schwenk [32] who suggested the problem of determining which graphs satisfy this property. This problem ignited a significant investigation among algebraic graph theorists for integral graphs. Although this problem is seemingly very simple to explain, its complexity is demonstrated in that it has been actively researched by many mathematicians during the last forty years and is still open for discussion. In fact; integral graphs are not only infinitely many but they exist in almost all classes of graphs and among all orders, despite their rarity. The general problem of “classification of all integral graphs” proved to be quite difficult to solve. Many graph theorists started to investigate some special classes of graphs including; trees, graphs with bounded degrees, regular graphs and Cayley graphs. What proves so interesting about this problem is that no one yet can identify what the integral trees are or which 5-regular graphs are integral.

Integral Cayley graphs have application in the study of *perfect state transfer* in quantum mechanics. There one associates a weighted graph with a quantum system. Vertices are representing the quantum spins, and weighted edges represent the strength to transfer qubits along that edge. The associated graph Γ of a quantum system admits a perfect state transfer from a vertex u to v if $\text{Aut}(\Gamma)_u = \text{Aut}(\Gamma)_v$, where $\text{Aut}(\Gamma)_u$ denotes the group of automorphisms of Γ which fix u . It is easy to see that if there is a perfect states transfer from a vertex u to v , then the subgraphs $\Gamma - u$ and $\Gamma - v$ are cospectral and the ratio of any

two non-zero eigenvalues is rational. Integral graphs and in particular circulant graphs have provided an extensive source of examples for perfect state transfers (for more details see [56] and [29]). There have been many more applications of Theorem 2.2.2 within mathematics and computer science. The key tool in all these results was an explicit way to determine the integrality of circulant graphs. Theorem 2.4.4 now provides sufficient tools to lift those results to the case of Cayley graphs over abelian groups ([17, 35]).

In this chapter we will investigate the integral Cayley graphs over abelian groups. We will exhibit some general results about integral graphs and present a new proof of classification of integral Cayley graphs over abelian groups.

2.1 Introduction

All matrices considered here are square matrices with entries from a subfield of the complex numbers. A matrix M is *integral* if all its eigenvalues over the complex numbers are rational integers. A graph Γ is called integral if its adjacency matrix is an integral matrix. Throughout this thesis we shall assume that G is a finite group. We use the multiplicative notation when G is non-abelian and sometimes additive notation in the case of abelian groups. Let S be a *symmetric subset* (i.e., $S = S^{-1}$) of G . The *Cayley graph* of G over S , denoted by $\text{Cay}(G, S)$, is the graph with vertex set G such that x and y ($x, y \in G$) are adjacent if $xy^{-1} \in S$. If S is not a symmetric subset, then we will get the *directed* Cayley graph with vertex set G and (x, y) is an arc if and only if $xy^{-1} \in S$. The Cayley graph $\text{Cay}(G, S)$ is connected if and only if S is a generating set of G . If S is not a generating set of G , then Cayley graph $\text{Cay}(G, S)$ is a disjoint union of $[G : \langle S \rangle]$ copies of the connected Cayley graph $\text{Cay}(\langle S \rangle, S)$.

Recall that a *multiset* is a set S together with multiplicity function $\mu_S : S \rightarrow \mathbb{N}$, where $\mu_S(x)$ is a positive integer for every $x \in S$ (counting “how many times x occurs in the multiset”). We set $\mu_S(x) = 0$ for $x \notin S$. A multiset S of group elements is symmetric if $\mu_S(s) = \mu_S(s^{-1})$ for every $s \in S$. If S is a symmetric multiset of elements of a group G , the *Cayley multigraph* $\text{Cay}(G, S)$ is defined as above except that it is a multigraph and the number of edges joining x, y in $\text{Cay}(G, S)$ is equal to $\mu_S(xy^{-1})$. A Cayley graph $\text{Cay}(G, S)$ is regular of degree $|S|$.

Let Γ be a simple graph and $\lambda_1 \geq \dots \geq \lambda_n$ its sequence of eigenvalues. The sum $s_k = \sum_{i=1}^n \lambda_i^k$ is called the k -th spectral moment which counts the number of closed walks of length k in Γ . The characteristic and minimal polynomial of a graph are monic polynomials

with integer coefficients, which implies that eigenvalues are algebraic integers. Since the spectrum of a disconnected graph is the union of the spectra of its components, in any investigation of integral graphs it is sufficient to consider only connected graphs.

Theorem 2.1.1. *If Γ is a k -regular graph with eigenvalues $k = \lambda_1(\Gamma) \geq \dots \geq \lambda_n(\Gamma)$, then $\bar{\Gamma}$ is a $(n - k - 1)$ -regular graph with eigenvalues $\lambda_1(\bar{\Gamma}) = n - k - 1$ and for $2 \leq i \leq n$, $\lambda_i(\bar{\Gamma}) = -1 - \lambda_{n-i+2}(\Gamma)$.*

As a result of this theorem, if Γ is a regular integral graph then the complement $\bar{\Gamma}$ of Γ is also integral.

Theorem 2.1.2. *Let Γ_1 be a graph of order n with eigenvalues $\lambda_1 \geq \dots \geq \lambda_n$, and Γ_2 a graph of order m with eigenvalues $\mu_1 \geq \dots \geq \mu_m$. Then*

- *The eigenvalues of the Cartesian product $\Gamma_1 \square \Gamma_2$ are $\lambda_i + \mu_j$ for $1 \leq i \leq n, 1 \leq j \leq m$;*
- *The eigenvalues of the tensor product $\Gamma_1 \times \Gamma_2$ are $\lambda_i \mu_j$ for $1 \leq i \leq n, 1 \leq j \leq m$.*

Thus the Cartesian product and tensor product of integral graphs are integral. For example the hypercube Q_n is defined recursively by $Q_1 = K_2$ and $Q_n = K_2 \square Q_{n-1}$. Thus eigenvalues of Q_n are numbers $n - 2i$ with multiplicity $\binom{n}{i}$ for $0 \leq i \leq n$.

Another example of a set consisting entirely of integral graphs is the set of complete graphs K_n ($n \geq 1$), with spectrum $[(n - 1)^1, -1^{n-1}]$. Cocktail-party graph $CP(n) = \overline{nK_2}$ is integral with spectrum: $[(2n - 2)^1, 0^n, (-2)^{n-1}]$. The complete multipartite graph $K_{s, \dots, s}$ on $n = st$ vertices and t colour classes of sizes s is integral. It is the complement of the integral graph tK_s , thus the spectrum of $K_{s, \dots, s}$ is: $[(n - s)^1, 0^{n-t}, (-s)^{t-1}]$. The spectrum of a path P_n of n vertices consists of numbers $2 \cos(\frac{\pi k}{n+1})$ for $1 \leq k \leq n$. Thus the only integral path is P_2 . One can easily see from a similar formula for eigenvalues of a cycle, that the only integral cycles are C_3, C_4 and C_6 . Also since the spectrum of the complete bipartite graph $K_{m,n}$ is $[(\sqrt{mn})^1, 0^{m+n-2}, (-\sqrt{mn})^1]$, thus $K_{m,n}$ is integral only if mn is a square of an integer.

If Γ_i are r_i -regular integral graphs on n_i vertices ($1 \leq i \leq 2$), then the join $\Gamma_1 \nabla \Gamma_2$ is integral if and only if $(r_1 - r_2)^2 + 4n_1n_2$ is a perfect square (see [16]). The line graph $L(\Gamma)$ of a regular integral graph Γ is also integral.

Theorem 2.1.3. *If Γ is a graph with d distinct eigenvalues then diameter of Γ is at most $d - 1$.*

Using this theorem one can easily see that;

Theorem 2.1.4. *The set of k -regular connected integral graphs is finite.*

It is easy to see that in any graph Γ , $\lambda_1(\Gamma) \leq \Delta(\Gamma)$. If Γ is connected, equality happens only in the case when Γ is regular. This can be used to prove that the set of connected integral graphs with bounded maximum degree is finite.

Suppose Γ_1 is a graph with n vertices and Γ_2 is a graph with m vertices. The *corona* of Γ_1 by Γ_2 , denoted by $\Gamma_1 \circ \Gamma_2$, is a graph with $n + mn$ vertices obtained from Γ_1 and n copies of Γ_2 by joining the i -th vertex of Γ_1 to each vertex in the i -th copy of Γ_2 ($1 \leq i \leq n$). The subdivision graph of Γ , $S(\Gamma)$, is obtained by inserting a single vertex in each edge of Γ .

Theorem 2.1.5 ([22]). *The only connected integral graphs which are not 3-regular and whose maximum vertex degrees are at most three are those illustrated in Figure 2.1.*

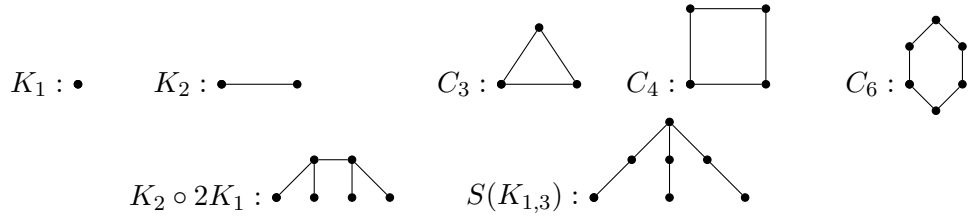


Figure 2.1: Non-cubic connected integral graphs with $\Delta \leq 3$

Theorem 2.1.6 ([19, 51]). *There are exactly thirteen connected cubic integral graphs. They are: $K_4, K_{3,3}, C_3 \square K_2, C_4 \square K_2, C_6 \square K_2$, the Petersen graph, $L(S(K_4))$, the Tutte's 8-cage, the graph on 10 vertices obtained from $K_{3,3}$ by specifying a pair of nonadjacent vertices and replacing each of them by a triangle, Desargues' graph and its cospectral-mate, the graph obtained from two (disjoint) copies of $K_{2,3}$ by adding three edges between vertices of degree two in different copies of $K_{2,3}$, and a bipartite graphs on 24 vertices (with girth 6).*

This theorem was proven by F.C. Bussemaker and D.M. Cvetković [19] in 1976. At the same time, independently, the similar result was reported (and published a bit later) by A.J. Schwenk [51]. These authors used different techniques to get the same result: F.C. Bussemaker and D. Cvetković combined the aid of a computer with theoretical reasoning, while A.J. Schwenk achieved the result completely “by hand and pencil”.

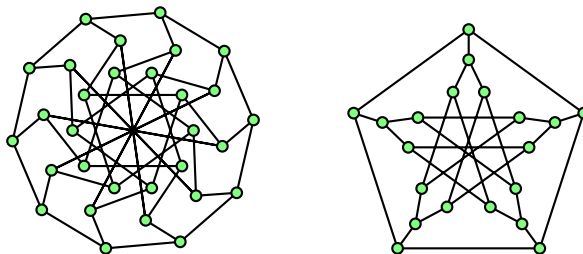


Figure 2.2: Tutte 8-cage, smallest cubic graph of girth 8

The initial idea in the first case was to list all possible sets of distinct eigenvalues, then find the possible multiplicities of them, subject to several restrictions resulting from the connections between spectral moments and the numbers of vertices, edges and triangles, and also from the Hoffman polynomial, and finally to deduce whether a graph with a considered spectrum exists.

Using Brendan McKay's program *geng* for generating graphs, one can see that there are exactly 263 connected integral graphs on up to 11 vertices (see [14, 15, 16]). In 2009, Alon et al. [4] showed that the total number of adjacency matrices of integral graphs with n vertices is less than or equal to $2^{\binom{n}{2} - \frac{n}{400}}$ for a sufficiently large n .

There are many cospectral integral graphs. Infinitely many pairs of cospectral integral regular graphs have been constructed in [13, 58]. The hypercube Q_n is determined by its spectrum for $n < 4$, but not for $n \geq 4$. Indeed, there are precisely two graphs with spectrum $[4^1, 2^4, 0^6, -2^4, -4^1]$ ([31]).

In 1998, 4-regular integral graphs began to attract attention. In [54] Stevanović determined all 24 connected 4-regular integral graphs avoiding ± 3 in the spectrum. D. Cvetković, S. Simić and D. Stevanović [24] found 1888 possible 4-regular bipartite integral graphs. The potential spectra of bipartite 4-regular integral graphs were determined in [24]. They are quite numerous and it cannot be expected that all 4-regular integral graphs will be determined in the near future. Later, D. Stevanović obtained nonexistence results for some of these potential spectra. It follows from these results that; except for 5 exceptional spectra, bipartite 4-regular integral graphs have at most 1260 vertices. As a corollary, a non-bipartite 4-regular integral graph Γ has at most 630 vertices, unless $\Gamma \times K_2$ has one of these exceptional spectra. For a survey of results regarding integral trees and other classes of integral graphs, we refer the reader to [16].

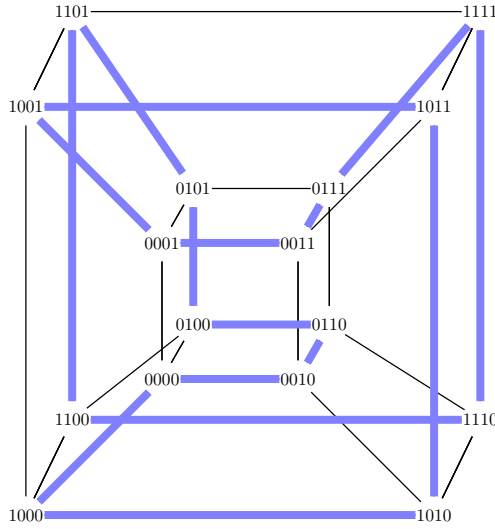


Figure 2.3: Complete Gray Code in hypercube Q_4

2.2 Integral Cayley graphs

In this chapter, ω_n (we will use ω when the index n is clear from the context) will denote the primitive n -th root of unity $e^{\frac{2\pi i}{n}}$. Let G be an abelian group, generated by a subset S . We know that every irreducible representation (character) of G is a group homomorphism from G to \mathbb{C}^\times (multiplicative group of \mathbb{C} , i.e. $\mathbb{C} \setminus \{0\}$). Thus $\rho \in \text{IRR}(G)$ is uniquely determined by its values on a generating set of the group. If $g \in G$ is an element of order n , then $\rho(g)$ is an n -th root of unity. This fact provides an easy construction of all irreducible representation of abelian groups. If $G = \langle a \rangle$ is a cyclic group of order n , then for each j ($1 \leq j \leq n$) $\rho_j(a) = \omega_n^j$ will uniquely determine an irreducible representation of G . There are $h(G) = |G|$ such irreducible representations, which implies that the set $\{\rho_j \mid 1 \leq j \leq n\}$ should constitute a complete set of irreducible representations of G . If G is an abelian finite group, then according to the *fundamental theorem of finitely generated* abelian groups, G is isomorphic to a direct product of cyclic subgroups. This along with Theorem 1.1.7 provide enough tools to construct all the irreducible representations of G .

The Cayley graph $\text{Cay}(C_n, S)$, where C_n denotes a general cyclic group of order n and S is a subset, is called a *circulant* graph of order n . In the context of circulant graphs (especially in the examples) we use \mathbb{Z}_n (the additive group of integers modulo n) and the additive notation. An alternate definition for a circulant graph is; any graph with a circulant

adjacency matrix. Given this, the following theorem is easy to prove.

Theorem 2.2.1. *If $\Gamma = \text{Cay}(\mathbb{Z}_n, S)$, then $\text{Spec}(\Gamma) = \{\lambda_x \mid x \in \mathbb{Z}_n\}$ where*

$$\lambda_x = \sum_{s \in S} \omega_n^{sx}.$$

It is easy to see that an eigenvector corresponding to the eigenvalue λ_x in the above theorem is the vector $\mathbf{v} = (\omega_n^{kx})_{k \in \mathbb{Z}_n}$.

Example 2.2.1. Let $X = \text{Cay}(\mathbb{Z}_6, \{2, 3\})$, then

$$\text{Spec}(X) = [2, \omega_6^2 - 1, \omega_6^4 + 1, \omega_6^3 + 1, \omega_6^2 + 1, \omega_6^4 - 1]$$

For an integer $n \geq 2$ and a proper divisor d of n we define

$$G_n(d) = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = d\}.$$

Theorem 2.2.2 (So [52]). *Let n be an integer, $n \geq 2$, $S \subseteq \mathbb{Z}_n$, $0 \notin S$, $-S = S$. The circulant $\text{Cay}(\mathbb{Z}_n, S)$ is integral, if and only if there are proper divisors d_1, \dots, d_r of n such that*

$$S = \bigcup_{j=1}^r G_n(d_j).$$

In the rest of this chapter, we will provide necessary tools to extend this result and prove a similar result for abelian groups.

An algebraic structure (L, \vee, \wedge) , consisting of a set L and two binary operations \vee (disjunction), and \wedge (conjunction), on L is a *lattice* if the following axiomatic identities hold for all elements a, b, c of L .

$$a \vee (b \vee c) = (a \vee b) \vee c \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad (\text{Associative laws})$$

$$a \vee b = b \vee a \quad a \wedge b = b \wedge a \quad (\text{Commutative laws})$$

$$a \vee (a \wedge b) = a \quad a \wedge (a \vee b) = a \quad (\text{Absorption laws}).$$

A lattice can be defined as a partially ordered set in which any two elements have a supremum and an infimum. A *boolean algebra* is a lattice equipped with a unary operation \neg , called “complement” or “not”, and two elements 0 and 1, such that it satisfies the following laws:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \quad (\text{Distributivity laws})$$

$$a \vee 0 = a \qquad a \wedge 1 = a \qquad \text{(Identity laws)}$$

$$a \vee \neg a = 1 \qquad a \wedge \neg a = 0 \qquad \text{(Complements laws).}$$

It is easy to give a ring structure to a boolean algebra with ring multiplication corresponding to \wedge and ring addition to exclusive disjunction; $a + b := (a \wedge \neg b) \vee (\neg a \wedge b)$. In this ring every element is an idempotent. Any ring with identity that every element is an idempotent is called a *boolean ring*. Boolean rings with identity and boolean algebras are essentially the same algebraic structure and we are not distinguishing them. The power set (set of all subsets) of any given nonempty set S forms a boolean algebra with the two operations $\vee := \cup$ (union) and $\wedge := \cap$ (intersection) and set difference with respect to S (complement) as the unary operation. The smallest element 0 is the empty set and the largest element 1 is the set S itself. The boolean ring operations are intersection and symmetric difference corresponding to ring multiplication and addition respectively.

Suppose S is a set and F is a family of subsets of S , then $\mathbb{B}(F)$ stands for the lattice of subsets of S obtained by arbitrary finite intersections, unions, and complements of the sets in the family F . It is easy to see that this lattice is indeed a boolean algebra (called the boolean algebra generated by F). The minimal non-empty elements of this algebra are called the atoms. Each element of $\mathbb{B}(F)$ is expressible as a disjoint union of the atoms. Consider the equivalence relation \sim on S , where $a \sim b$ if and only if for every $A \in F$ we have either $\{a, b\} \subseteq A$ or $\{a, b\} \cap A = \emptyset$.

Theorem 2.2.3. *The equivalence classes of this relation are the atoms of $\mathbb{B}(F)$.*

Proof. If T is an atom, then for any set $A \in F$ we have $T \cap A \in \mathbb{B}(F)$. Since $T \cap A \subseteq T$ and T is an atom, we have either $T \cap A = \emptyset$ or $T \cap A = T$. Thus, elements of T are equivalent. Let $a \in T$, if $[a]$ is the equivalence class containing a , then from what we said we get; $T \subseteq [a]$. If $a \sim b$ then, for any A in F we have $\{a, b\} \cap A = \emptyset$ or $\{a, b\} \subseteq A$. Since $T \in \mathbb{B}(F)$ and $a \in T$, we have $b \in T$. Then $[a] \subseteq T$ and therefore, $T = [a]$.

□

We let $\mathbb{B}(\mathcal{G})$ denote the boolean algebra generated by the subgroups of G . We show below that the atoms of this boolean algebra are all subsets of elements which generate the same cyclic subgroup of G .

Theorem 2.2.4. *The atoms of the boolean algebra $\mathbb{B}(\mathcal{G})$ are the sets $[a] = \{b \mid \langle b \rangle = \langle a \rangle\}$.*

Proof. We use the previous theorem to show that the equivalence classes of the relation \sim are $[a] = \{b \mid \langle b \rangle = \langle a \rangle\}$. As we know, $a \sim b$ if and only if every subgroup of G containing either both elements or none of them. Since $\langle a \rangle$ is the smallest subgroup of G containing a , thus $b \in \langle a \rangle$. This proves that $[a]$ is a subset of $\langle a \rangle$. Now if $a \sim b$ then $[a] = [b]$ and so $a \in [a] = [b] \subseteq \langle b \rangle$. This proves that $\langle a \rangle \subseteq \langle b \rangle$, with the symmetry we have the other side as well. \square

We notice that in $\mathbb{B}(\mathcal{G})$ we have $g \sim h$ if and only if there are integers k and l coprime with respect to $o(g) = o(h)$ such that $h = g^k$ and $g = h^l$.

We can define a similar algebraic structures for multisets, using multiset operations. Formally, we take all atoms of the boolean algebra $\mathbb{B}(\mathcal{G})$ and take all multisets that can be expressed as non-negative integer combinations of these atoms. This defines the collection $\mathcal{C}(\mathcal{G})$ of multisets that is called the *integral cone* over $\mathbb{B}(\mathcal{G})$.

A theorem by Bridges and Mena (see [18]) gives a complete characterization of which Cayley multigraphs over abelian groups are integral. Although the result of Bridges and Mena was originally stated for simple Cayley graphs, indeed they proved the multigraph version. For each group element $g \in G$, let A_g denote the permutation matrix (indexed by $G \times G$) associated with g and for a set $S \subseteq G$ let $A_S = \sum_{s \in S} A_s$. Bridges and Mena proved that for an abelian group G , a complex linear combination of the matrices $\{A_g : g \in G\}$ is a rational matrix with rational eigenvalues if and only if it is a rational combination of the matrices $\{A_Q : Q \text{ is an atom of } \mathbb{B}(\mathcal{G})\}$.

There has been some interests in finding a new proof of this result. Notably, So's result (Theorem 2.2.2) is a new proof in the special case when G is a cyclic group, and Klotz and Sander [38] found a new proof of the "if" direction for all abelian groups. In [10], our goal was to give a new proof of Theorem 2.4.4. The proof presented is based on characters, and is a fairly direct generalization of that given by So. However, the approach generalizes to non-abelian groups and enables one to consider a more general classes of groups, as we will see in the next chapter.

2.3 B -integrality

If Ω is a collection of graphs on the common vertex set V and B is an orthogonal basis of \mathbb{C}^V , then we say that Ω is *B-integral* if for every X in Ω , B is a set of eigenvectors for X

and all eigenvalues of X are integral. Equivalently, if $A(X)$ denotes the adjacency matrix of X , then $A(X)B = B\Lambda$, where Λ is a diagonal matrix with integer entries (and B is viewed as a matrix whose columns are the vectors from B)¹. If X and Y are (simple) graphs on the same vertex set V , then we denote by $X \cup Y$ the simple graph on V in which vertices u, v are adjacent if and only if they are adjacent in X or in Y (or in both). For any family of graphs Ω on a common vertex set, we let $U(\Omega)$ be the closure of Ω under the operation \cup . We begin with an easy lemma.

Lemma 2.3.1. (a) *If X is B -integral and $j \in B$, then \overline{X} is B -integral.*

(b) *If X and $X \cap Y$ are B -integral, then $X \cap \overline{Y}$ is B -integral.*

(c) *If Ω is an intersection-closed family of B -integral graphs, then $U(\Omega)$ is B -integral.*

Proof. (a) $j \in B$ implies that X is a regular graph, so the result is clear from the fact that $A(X) + A(\overline{X}) = J - I$.

To prove (b), observe that $A(X \cap \overline{Y}) = A(X) - A(X \cap Y)$, thus

$$A(X \cap \overline{Y})B = A(X)B - A(X \cap Y)B = B\Lambda_1 - B\Lambda_2 = B(\Lambda_1 - \Lambda_2).$$

Since Λ_1 and Λ_2 are integral, so is their difference, hence $X \cap \overline{Y}$ is B -integral.

By observing that $A(X \cup Y) = A(X) + A(Y) - A(X \cap Y)$, a proof similar to the above proof of (b) shows that (c) holds. \square

For any set of graphs Ω on a common vertex set V , we let $\mathbb{B}(\Omega)$ denote the set of all graphs on V which may be expressed using members of Ω and the operations \cap , \cup , and complement.

Lemma 2.3.2. *Let Ω be an intersection-closed family of B -integral graphs and assume that $j \in B$. Then $\mathbb{B}(\Omega)$ is B -integral.*

Proof. Set $\Omega_0 = \Omega$ and for every $k \in \mathbb{N}$ recursively define

$$\Omega_{k+1} = \{X_1 \cap \cdots \cap X_n : \text{either } X_i \in \Omega_k \text{ or } \overline{X_i} \in \Omega_k \text{ for every } 1 \leq i \leq n, n \geq 1\}.$$

It is immediate that each Ω_k is intersection-closed and it follows from De Morgan's law that $\mathbb{B}(\Omega) = \cup_{k=0}^{\infty} \Omega_k$. To complete the proof, we shall show, by induction on k , that every graph in Ω_k is B -integral. As a base, we observe that this holds for $k = 0$ by assumption. For the

¹Similar notion was defined by Klotz and Sander in [38].

inductive step, let X be a graph in Ω_{k+1} and suppose that $X = X_1 \cap \cdots \cap X_\ell \cap \overline{Y_1} \cap \cdots \cap \overline{Y_m}$ where $X_1, \dots, X_\ell, Y_1, \dots, Y_m \in \Omega_k$. Then we have

$$X = \left(\bigcap_{i=1}^{\ell} X_i \right) \cap \overline{\left(\bigcup_{j=1}^m Y_j \right)}.$$

Since Ω_k is intersection-closed and $X' = X_1 \cap \cdots \cap X_\ell \in \Omega_k$ and $X' \cap (\bigcup_{j=1}^m Y_j) = (\bigcup_{j=1}^m (X' \cap Y_j)) \in U(\Omega_k)$, it follows from Lemma 2.3.1 that X is B -integral, as desired. \square

In the following lemma, G is a group not necessarily abelian.

Lemma 2.3.3. *Let S and T be symmetric multisets of a group G . If $gT = Tg$ (equality holding as multisets) for every $g \in G$, then the adjacency matrices of Cayley multigraphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ commute.*

Proof. Let A_S and A_T be the adjacency matrices of both Cayley multigraphs, and let $g, h \in G$. Since S and T are symmetric, we have

$$\begin{aligned} (A_S A_T)_{g,h} &= \sum_{x \in G} \mu_S(gx^{-1}) \mu_T(xh^{-1}) = \sum_{x \in G} \mu_{Sg}(x) \mu_{Th}(x) \\ &= \sum_{x \in G} \mu_{Sg}(xg) \mu_{Th}(xg) = \sum_{x \in G} \mu_S(x) \mu_{Thg^{-1}}(x). \end{aligned}$$

Taking a similar expression for $A_T A_S$ and using the fact that S and T are symmetric, we derive

$$\begin{aligned} (A_T A_S)_{g,h} &= \sum_{x \in G} \mu_{Tgh^{-1}}(x) \mu_S(x) = \sum_{x \in G} \mu_{Tgh^{-1}}(x^{-1}) \mu_S(x^{-1}) \\ &= \sum_{x \in G} \mu_{hg^{-1}T}(x) \mu_S(x). \end{aligned}$$

To obtain equality for every g and h , it suffices to see that $\mu_{Thg^{-1}}(x) = \mu_{hg^{-1}T}(x)$ for every $g, h, x \in G$; equivalently, $\mu_{Tk}(x) = \mu_{kT}(x)$ for every $k, x \in G$. But this is precisely our assumption that $Tk = kT$. \square

Lemma 2.3.3 implies that the adjacency matrices of all Cayley multigraphs $\text{Cay}(G, T)$, where T is any normal subgroup of G (or any other union of conjugacy classes), commute. Therefore, they have a common set of eigenvectors.

2.4 Integral Cayley graphs over abelian groups

Throughout this section, G will always be a (finite) abelian group. Let G^* denote the dual group of G , consisting of all complex characters of G . It is well known that G^* is a group under pointwise multiplication (according to 1.1.7), and that $G^* \cong G$. We define F to be the matrix indexed by $G^* \times G$ and given by the rule that for $\alpha \in G^*$ and $x \in G$ we have $F_{\alpha,x} = \alpha(x)$. Note that each row of F is a character. Furthermore, it follows from the orthogonality of characters 1.1.9 that $FF^* = |G|I_n$, where F^* is the conjugate transpose of F and $n = |G|$. Finally, observe that if r is the exponent of G , then every element of F is an r^{th} root of unity.

In the remainder, for any vector $v \in \mathbb{C}^{\mathcal{A}}$ (where \mathcal{A} is a non-empty index set) and any $n \in \mathbb{Z}$, we let v^n denote the vector in $\mathbb{C}^{\mathcal{A}}$ given by coordinate-wise exponentiation, i.e., $(v^n)_i = (v_i)^n$ for each $i \in \mathcal{A}$.

Observation 2.4.1. *Let $x, y \in G$ and let F_x, F_y denote the column vectors of F indexed by x and y , respectively. If $x \sim y$, then there exist integers $j, k \in \mathbb{Z}$ so that $(F_x)^j = F_y$ and $(F_y)^k = F_x$.*

Proof. Since $x \sim y$, we may choose $j, k \in \mathbb{Z}$ so that $x^j = y$ and $y^k = x$. Now, for any character $\alpha \in G^*$ we have $\alpha(y) = \alpha(x^j) = (\alpha(x))^j$ and it follows that $F_y = (F_x)^j$. A similar argument shows that $F_x = (F_y)^k$. \square

The following lemma is the key point in generalizing the sufficiency proof of Theorem 2.4.4 offered by Klotz and Sander in [38]. The proof presented here is due to Matt DeVos.

Lemma 2.4.2. *Let $v \in \mathbb{Q}^G$. If $Fv \in \mathbb{Q}^{G^*}$, then for every $x, y \in G$ with $x \sim y$, we have $v_x = v_y$.*

Proof. Let F_x and F_y denote the column vectors of F indexed by x and y and let ℓ (m) be the smallest integer so that every term of F_x (F_y) is a ℓ^{th} (m^{th}) root of unity. It follows from Observation 2.4.1 that $\ell = m$. Now, fix a primitive ℓ^{th} root of unity ω and express each entry of F_x and F_y in the form ω^i for some $i \in \{0, 1, \dots, \ell - 1\}$. Using this interpretation, and recalling that $u := Fv$ is rational, we obtain an expression for the (complex) inner product of F_x and u as

$$F_x \cdot u = (F^*u)_x = \sum_{i=0}^{\ell-1} a_i \omega^i$$

where each $a_i \in \mathbb{Q}$. Note that $F_x \cdot u = (F^*u)_x = nv_x$. Now, let $P(z) \in \mathbb{C}[z]$ denote the polynomial $P(z) = \sum_{i=0}^{\ell-1} a_i z^i - nv_x$. Observe that $P(\omega) = 0$. Next, choose $j \in \{0, 1, \dots, \ell-1\}$ so that $F_y = (F_x)^j$. Note that $\gcd(j, \ell) = 1$. We may assume $x \neq y$, as otherwise there is nothing to prove. It follows that $j \geq 2$, so $\ell \geq 3$. The polynomial P has rational coefficients and has ω as a root. It follows from this and the fact that the polynomial

$$\Phi_\ell(z) = \prod_{i \in \{1.. \ell\}: \gcd(i, \ell)=1} (z - \omega^i)$$

is irreducible over \mathbb{Q} , that ω^j is also a root of P . But then we have

$$0 = P(\omega^j) = \sum_{i=0}^{\ell-1} a_i \omega^{ij} - nv_x = F_y \cdot u - nv_x$$

which implies that $v_y = \frac{1}{n} F_y \cdot u = v_x$ as desired. \square

Lemma 2.4.3. *Let G be a finite abelian group, S a symmetric subset of G and $\chi \in \text{Irr}(G)$. Consider the vector $\mathbf{x} = (\chi(g))_{g \in G}$. Then \mathbf{x} is an eigenvector of $\Gamma = \text{Cay}(G, S)$, with eigenvalue*

$$\lambda_\chi = \sum_{s \in S} \chi(s).$$

Proof. Considering the g -th entry of $A(\Gamma)\mathbf{x}$ we have:

$$(A(\Gamma)\mathbf{x})_g = \sum_{h \in G} A(\Gamma)_{g,h} \chi(h) = \sum_{s \in S} A(\Gamma)_{g,sg} \chi(sg) = \sum_{s \in S} \chi(sg) = \left(\sum_{s \in S} \chi(s) \right) \chi(g) = \lambda_\chi \chi(g)$$

\square

Let X be a non-empty set and $S \subseteq X$. The *characteristic vector* of S , denoted by $\mathbb{1}_S$, is a vector in $\{0, 1\}^X$ such that $\mathbb{1}_S(x) = 1$ if and only if $x \in S$. We are now ready to state and prove the following theorem.

Theorem 2.4.4 (Bridges, Mena [18]). *If G is an abelian group, then $\text{Cay}(G, S)$ is integral if and only if $S \in \mathcal{C}(G)$, where $\mathcal{C}(G)$ is the integral cone of multisets generated by the subgroups of G .*

Proof. (Necessity) By lemma 2.4.3 each character α as a vector in G^* is an eigenvector for $\text{Cay}(G, S)$ with eigenvalue $\alpha(S) = \sum_{g \in S} \alpha(g)$. Alternately, if we view α as a vector in \mathbb{C}^G , this eigenvalue may be written as $\alpha \cdot \mathbb{1}_S$. Suppose that $\text{Cay}(G, S)$ is integral. Then we

have $\alpha \cdot \mathbb{1}_S \in \mathbb{Q}$ for every $\alpha \in G^*$. Equivalently, $F\mathbb{1}_S$ is rational-valued. But then, it follows from the previous lemma that whenever $x, y \in G$ satisfy $x \sim y$, we have $(\mathbb{1}_S)_x = (\mathbb{1}_S)_y$. This implies that $S \in \mathbb{B}(\mathcal{G})$, as desired.

(Sufficiency) Let $\Omega = \{\text{Cay}(G, H) : H \leq G\}$. By Lemma 2.3.3, the adjacency matrices of all graphs in Ω commute and hence they have a common orthogonal set B of eigenvectors. For every $X \in \Omega$ we have that X has B as a basis of eigenvectors, and X is a disjoint union of cliques (with loops at every vertex), so X is B -integral. It now follows from Lemma 2.3.2 that $\mathbb{B}(\Omega) = \{\text{Cay}(G, S) : S \in \mathbb{B}(\mathcal{G})\}$ is B -integral. Since the adjacency matrix A_T of each multigraph $\text{Cay}(G, T)$, $T \in \mathcal{C}(G)$, is an integral linear combination of adjacency matrices of $\text{Cay}(G, S)$, $S \in \mathbb{B}(\mathcal{G})$, also A_T is B -integral. This completes the proof. \square

Let G be a cyclic group of order n generated by a . We want to determine the atoms of $\mathbb{B}(\mathcal{G})$. To show that So's result in 2.2.2 is a special case of the theorem 2.4.4.

We recall that $\text{ord}(a^k) = \frac{\text{ord}(a)}{\gcd(\text{ord}(a), k)}$. If d is a divisor of n , then $\text{ord}(a^d) = \frac{n}{d}$. We have;

$$\text{ord}(a^{id}) = \text{ord}((a^d)^i) = \frac{\text{ord}(a^d)}{\gcd(\text{ord}(a^d), i)} = \frac{\frac{n}{d}}{\gcd(\frac{n}{d}, i)}$$

Thus $[a^d] = \{a^{id} \mid (i, \frac{n}{d}) = 1\} = \{a^k \mid \gcd(k, n) = d\}$. This for the group \mathbb{Z}_n with additive notation (see 2.2.2) turns to $[d] = \{k \mid \gcd(k, n) = d\} = G_n(d)$. Therefore, clearly Theorem 2.4.4 implies Theorem 2.2.2.

Chapter 3

Integral Cayley graphs over non-abelian groups

In this chapter we consider the general case of Cayley integral graphs over non-abelian groups. We will first list known results in this area. In the second section, we will introduce different notions of integrality in the lattice of subsets of a group. Character and representation integrality are the main topics in this section. We characterize all character integral subsets of a group, and prove that representation integrality is equivalent to integrality of the corresponding Cayley graph. In the third section, we will study the integral Cayley graphs over Hamiltonian groups. Last section will deal with integrality of Cayley graphs over Dihedral groups.

3.1 Introduction

Theorem 3.1.1. *Suppose $\Gamma = \text{Cay}(G, S)$, where G is a finite group and S is a non-empty subset of G . Then the following holds:*

- 1) Γ is regular of degree $|S|$.
- 2) Γ is connected if and only if $G = \langle S \rangle$.
- 3) If $1 \in S$ then Γ has a loop at every vertex.
- 4) Γ is undirected if and only if $S = S^{-1}$.

In this thesis we only consider undirected graphs. In the light of the previous theorem, we will always assume that S is a symmetric subset of G , i.e. $S = S^{-1}$. In the study of integral Cayley graphs, the usual assumption of $1 \notin S$ is not necessary. This is because including 1 in S will add one unit to every eigenvalues of the graph and that does not change the integrality of the graph spectrum. However, we will always assume that S is identity free. If for every g in G , we define $r_g : G \rightarrow G$ given by $r_g(h) = hg$, then one can check that r_g is an automorphism of $\Gamma = \text{Cay}(G, S)$. The *right regular permutation* representation of G is the set $R(G) = \{r_g \mid g \in G\}$. One can check that $R(G)$ is a group with function composition and $R(G) \simeq G$. If $\text{Aut}(G, S) = \{\alpha \in \text{Aut}(G) \mid \alpha(S) = S\}$, then we have $\text{Aut}(G, S) = \text{Aut}(\Gamma) \cap \text{Aut}(G)$.

Let α be an automorphism of the group G . We have $\alpha r_g \alpha^{-1} = r_{\alpha(g)}$, and so

$$R(G)\text{Aut}(G, S) \leq N_{\text{Aut}(\Gamma)}(R(G)).$$

Theorem 3.1.2. *If $\Gamma = \text{Cay}(G, S)$, then $\text{Aut}(\Gamma)$ acts transitively on G , and so Γ is a vertex-transitive graph.*

Suppose $\Gamma = \text{Cay}(G, S)$. The linear operator A_Γ (associated with Γ) on $\mathbb{C}G$, is defined by its action on the basis G according to $A_\Gamma(h) = \sum_{s \in S} sh$. The matrix of A_Γ with respect to the basis G is the adjacency matrix of Γ . It is clear from the definition of the left regular representation ρ_{reg} that $A_\Gamma = \sum_{s \in S} \rho_{reg}(s)$.

Theorem 3.1.3 (Diaconis and Shahshahani [25]). *Let G be a group and let $S \subseteq G$ be a multiset of elements of G . Let $\text{IRR}(G) = \{\rho_1, \dots, \rho_k\}$. For $t = 1, \dots, k$, let d_t be the degree of ρ_t , and let Λ_t be the multiset of eigenvalues of the matrix $\sum_{g \in S} \mu_S(g)\rho_t(g)$. Then the following holds:*

- (1) *The set of eigenvalues of $\text{Cay}(G, S)$ equals $\cup_{t=1}^k \Lambda_t$.*
- (2) *If the eigenvalue λ occurs with multiplicity $m_t(\lambda)$ in $\sum_{g \in S} \mu_S(g)\rho_t(g)$ ($1 \leq t \leq k$), then the multiplicity of λ in $\text{Cay}(G, S)$ is $\sum_{t=1}^k d_t m_t(\lambda)$.*

Remark 3.1.4. *Theorem 3.1.3 suggests that integrality of a Cayley graph $\text{Cay}(G, S)$ is equivalent to integrality of the matrices $\rho(S) = \sum_{s \in S} \rho(s)$ for every representation (reducible or irreducible) ρ of G .*

Theorem 3.1.5 ([48]). *Let G be a finite group of order n and $\text{Irr}(G) = \{\chi_1, \dots, \chi_h\}$ with $\chi_i(1) = n_i$ ($i = 1 \dots h$). Suppose S is a symmetric subset of G which is a union of conjugacy classes. Then the spectrum of the Cayley graph $\text{Cay}(G, S)$ can be arranged as $\Lambda = \{\lambda_{ijk} \mid i = 1, \dots, h; j, k = 1, \dots, n_i\}$ such that $\lambda_i = \lambda_{ijk}$ for $1 \leq j, k \leq n_i$, where λ_i is an eigenvalue corresponding to χ_i that can be expressed as:*

$$\lambda_i = \frac{\sum_{s \in S} \chi_i(s)}{n_i}.$$

Theorem 3.1.6 (Babai [13]). *Let G be a finite group of order n , $\text{Irr}(G) = \{\chi_1, \dots, \chi_h\}$ with $\chi_i(1) = n_i$ ($i = 1, \dots, h$). Suppose also that S is a symmetric subset of G . Then the spectrum of the Cayley graph $\text{Cay}(G, S)$ can be arranged as $\Lambda = \{\lambda_{ijk} \mid i = 1, \dots, h; j, k = 1, \dots, n_i\}$ such that $\lambda_{ij1} = \dots = \lambda_{ijn_i}$ (this common value is denoted by λ_{ij}). Furthermore, for any natural number t we have:*

$$\lambda_{i1}^t + \dots + \lambda_{in_i}^t = \sum_{s_1, \dots, s_t \in S} \chi_i\left(\prod_{l=1}^t s_l\right).$$

Theorems 3.1.3 and 3.1.6 are served as bridges between spectral graph theory and representations and characters of finite groups.

Theorem 3.1.7. *Let $\Gamma = \text{Cay}(G, S)$, where G is a finite group and S is a symmetric generating subset of G . Then, Γ is bipartite if and only if G has a linear character which maps each element s of S to -1 .*

Proof. We know by Theorem 3.1.1 that Γ is a connected graph and $\lambda_1 = |S|$ is a simple eigenvalue. Thus Γ is bipartite if and only if $-|S|$ is a simple eigenvalue of Γ . According to Theorem 3.1.3, each non-linear representation produce multiple eigenvalues. This implies that linear representations (characters) of G are the one which will produce $-|S|$ as an eigenvalue. Now it is clear from Theorem 1.1.8 that Γ is bipartite if any only if there is a character θ of G such that $\theta(s) = -1$ for every s in S . \square

Corollary 3.1.8. *Let $\Gamma = \text{Cay}(G, S)$, where S is a symmetric generating subset of a group G . If S contains an element of odd order then Γ is not bipartite.*

A group G is *perfect* if it is equal to its derived subgroup, i.e. $G = G'$. The index $[G : G']$ of the derived subgroup G' counts the number of linear characters of G .

Corollary 3.1.9. *If G is a perfect group, then there is no bipartite Cayley graph over G .*

Proof. Since G is perfect, the only linear character of G is the trivial character which maps each element of G to 1. Thus according to Theorem 3.1.7, for any subset S of G , $\text{Cay}(G, S)$ is not bipartite. \square

3.2 Character and representation integrality

We say a subset S of G is *representation integral* if for every matrix representation ρ of G , the matrix $\rho(S) = \sum_{s \in S} \rho(s)$ is an integral matrix. In the same way, we call a subset S of G *character integral* if for every character χ of G , $\chi(S) = \sum_{s \in S} \chi(s)$ is an integer.

We will write ρ -integral for representation integrality and χ -integral for character integrality. We notice that the group algebra $\mathbb{C}G$ is a semi-simple algebra. Therefore, to check a subset S of G is ρ -integral (χ -integral), it is sufficient to consider the irreducible representations (characters). We denote the collection of subgroups, normal subgroups, χ -integral and ρ -integral subsets of G by \mathcal{G}_G , \mathcal{N}_G , \mathcal{I}_χ^G and \mathcal{I}_ρ^G , respectively. When we consider a single group or when the group G is clear from the context, we will omit the letter G from the notation.

Remark 3.2.1. *The union of two χ -integral subsets of G is not generally a χ -integral subset, whereas disjoint union of χ -integral subsets of G is always a χ -integral subset.*

The situation for ρ -integral subsets is quite different from χ -integral sets, the fact that “eigenvalues of a sum of two matrices are not the sums of the eigenvalues of the terms” has made the situation quite undecidable. However, we have the following lemma.

Lemma 3.2.2. *If S and T are disjoint ρ -integral subsets of G and $ST = TS$ as multisets, then $S \cup T$ is a ρ -integral subset of G .*

Proof. It is easy to see that,

$$ST = TS \quad \Leftrightarrow \quad \left(\sum_{s \in S} s \right) \left(\sum_{t \in T} t \right) = \left(\sum_{t \in T} t \right) \left(\sum_{s \in S} s \right).$$

If ρ is any matrix representation of G , then this is equivalent with the fact that $\rho(S)$ and $\rho(T)$ are commuting matrices. Theorem 1.1.2 implies that eigenvalues of the matrix $\rho(S \cup T) = \rho(S) + \rho(T)$ are the sum of the eigenvalues of $\rho(S)$ and $\rho(T)$. Since S and T are ρ -integral subsets of G , we conclude that $\rho(S \cup T)$ is ρ -integral as well. \square

Remark 3.2.3. We notice that for two subsets S and T of a finite group G , $ST = TS$ (multiset equality) if $S \subseteq N_G(T)$.

Lemma 3.2.4. If ρ is a matrix representation of G then $\rho(G) = \sum_{g \in G} \rho(g)$ is an integral matrix, that is to say $G \in \mathcal{I}_\rho$.

Proof. For every h in G we have:

$$\rho(G) = \sum_{g \in G} \rho(g) = \sum_{g \in G} \rho(hg) = \rho(h) \left(\sum_{g \in G} \rho(g) \right) = \rho(h) \rho(G).$$

Thus if there is a h in G such that $\rho(h) \neq I$, then $\rho(G) = 0$ otherwise, $\rho(G) = |G|I$. In both cases $\rho(G)$ is an integral matrix. \square

From the above lemma, we deduce that the complement of a ρ -integral (χ -integral) subset is again a ρ -integral (χ -integral) subset of G . Recall the equivalence relation \sim in a group G , for g_1 and g_2 in G , we have $g_1 \sim g_2$ if and only if the subgroup $\langle g_1 \rangle$ generated by g_1 , is equal to the subgroup $\langle g_2 \rangle$ generated by g_2 . This is equivalent to $g_1 = g_2^k$ for some integer k relatively prime with respect to the common order of g_1 and g_2 .

Theorem 3.2.5. Let G be a finite group, and $\mathbf{x} = \sum_{g \in G} c_g g$ an element in $\mathbb{Q}G$. Suppose \mathbf{x} has the property that $g_1 \sim g_2$ implies $\sum_{h \in \text{cl}(g_1)} c_h = \sum_{h \in \text{cl}(g_2)} c_h$. Then $\chi(\mathbf{x})$ is an integer for all characters χ of G .

Proof. It suffices to show that $\chi(\mathbf{x})$ is rational for any irreducible character χ of G . Take E to be the cyclotomic field of $|G|$ -th roots of unity. We know that all character values, $\chi(g)$ for g in G lie in this field.

Let σ be in $\text{Gal}(E/\mathbb{Q})$. It suffices to show that $\sigma(\chi(\mathbf{x})) = \chi(\mathbf{x})$. Now if ω is a primitive $|G|$ -th root of unity, then $\sigma(\omega) = \omega^k$ for some integer k co-prime to $|G|$. It follows for g in G that $\sigma(\chi(g)) = \chi(g^k)$ (Theorem 1.1.8). Assume that L is a set of representatives of conjugacy classes in G . Since characters are class functions, so for $h \in \text{cl}(g)$ we have $\chi(g) = \chi(h)$. Thus,

$$\sigma(\chi(\mathbf{x})) = \sum_{g \in L} \left(\sum_{h \in \text{cl}(g)} c_h \right) \sigma(\chi(g)) = \sum_{g \in L} \left(\sum_{h \in \text{cl}(g)} c_h \right) \chi(g^k).$$

We also know that $\text{ord}(g)$ and k are relatively prime, because $\text{ord}(g) \mid |G|$. Consequently, g and g^k generate the same cyclic subgroup and so $g \sim g^k$. Since $\sum_{h \in \text{cl}(g)} c_h = \sum_{h \in \text{cl}(g^k)} c_h$, and

we notice that $\{g^k \mid g \in L\}$ is a complete set of representatives of conjugacy classes as well. This yields

$$\sigma(\chi(\mathbf{x})) = \sum_{g \in L} \left(\sum_{h \in \text{cl}(g^k)} c_h \right) \chi(g^k) = \sum_{g \in G} c_g \chi(g) = \chi(\mathbf{x}).$$

It follows that $\chi(\mathbf{x})$ is rational and thus integer. \square

The converse of the previous theorem is true and we have the following result:

Theorem 3.2.6. *Let G be a finite group, and let $\mathbf{x} = \sum_{g \in G} c_g g$ be an element in $\mathbb{Q}G$ with the property that for all irreducible characters λ of G , $\lambda(\mathbf{x}) \in \mathbb{Q}$. With these given, if $g_1 \sim g_2$ ($g_1, g_2 \in G$), then we have $\sum_{h \in \text{cl}(g_1)} c_h = \sum_{h \in \text{cl}(g_2)} c_h$.*

Proof. Since $g_1 \sim g_2$, we have $\text{ord}(g_1) = \text{ord}(g_2) = n$ for an integer n . Suppose $g_2 = g_1^r$, where r is co-prime to n . Let F be the field $\mathbb{Q}(\omega)$, where ω is a primitive n -th root of unity. There exists σ in $\text{Gal}(F/\mathbb{Q})$ such that $\sigma(\omega) = \omega^r$. Note that for all $\lambda \in \text{Irr}(G)$, we have $\sigma(\lambda(g_1)) = \lambda(g_1^r)$.

Now $\mathbf{x} = \sum_{t \in G} c_t t$, where c_t in \mathbb{Q} for every t in G . For t in G let $\theta_t = \sum_{\lambda \in \text{Irr}(G)} \lambda(t) \bar{\lambda}$, where $\bar{\lambda}$ is the complex-conjugate of λ . By character orthogonality we have:

$$\theta_t(u) = \begin{cases} |C_G(t)| & \text{if } u \text{ and } t \text{ are conjugate} \\ 0 & \text{otherwise} \end{cases}$$

We have $\theta_t(\mathbf{x}) = |C_G(t)| \sum_{g \in \text{cl}(t)} c_g$. Since this is rational, $\sigma(\theta_t(\mathbf{x})) = \theta_t(\mathbf{x})$ for all t in G . Also, by hypothesis, $\sigma(\lambda(\mathbf{x})) = \lambda(\mathbf{x})$ for all λ in $\text{Irr}(G)$.

We have

$$\begin{aligned} |C_G(g_1)| \sum_{h \in \text{cl}(g_1)} c_h &= \theta_{g_1}(\mathbf{x}) = \sigma(\theta_{g_1}(\mathbf{x})) = \\ &= \sum \sigma(\lambda(g_1)) \sigma(\bar{\lambda}(\mathbf{x})) = \sum \lambda(g_1^r) \bar{\lambda}(\mathbf{x}) = \\ &= \theta_{g_1^r}(\mathbf{x}) = \theta_{g_2}(\mathbf{x}) = |C_G(g_2)| \sum_{h \in \text{cl}(g_2)} c_h. \end{aligned} \tag{3.1}$$

Since $g_1 \sim g_2$ we have $C_G(g_1) = C_G(g_2)$ and so $\sum_{h \in \text{cl}(g_1)} c_h = \sum_{h \in \text{cl}(g_2)} c_h$, as wanted. \square

Theorem 3.2.7. *A subset S of G is χ -integral if and only if for all elements g_1 and g_2 in G , such that $g_1 \sim g_2$ we have:*

$$|\text{cl}(g_1) \cap S| = |\text{cl}(g_2) \cap S|.$$

Proof. We take $\mathbf{x} = \sum_{s \in S} s = \sum_{g \in G} c_g g$ where

$$c_g = \begin{cases} 1 & \text{if } g \in S \\ 0 & \text{otherwise} \end{cases}$$

Then using theorem 3.2.5 and 3.2.6 we have the desired result. □

Theorem 3.2.8. *Let G be a finite group. The following statements are true:*

- 1) $\mathbb{B}(\mathcal{G}) \subseteq \mathcal{I}_\chi$.
- 2) $\mathbb{B}(\mathcal{N}) \subseteq \mathcal{I}_\rho$.
- 3) $\mathcal{I}_\rho \subseteq \mathcal{I}_\chi$.
- 4) $\mathcal{G} \subseteq \mathcal{I}_\rho$.
- 5) $\mathbb{B}(\mathcal{N}) \subseteq \mathbb{B}(\mathcal{G})$.
- 6) $\mathbb{B}(\mathcal{G}) = \mathcal{I}_\chi$ if and only if G is an abelian group.
- 7) If $H \leq G$, then $\mathcal{I}_\rho^H \subseteq \mathcal{I}_\rho^G$.
- 8) Each atom of $\mathbb{B}(\mathcal{G})$ belongs to \mathcal{I}_ρ .
- 9) If $G = H \times K$, then $\mathcal{I}_\rho^H \times \mathcal{I}_\rho^K \subseteq \mathcal{I}_\rho^G$.
- 10) If $G = H \times K$ and $S \in \mathcal{I}_\rho^G$, then $\pi_H(S) \in \mathcal{I}_\rho^H$ and $\pi_K(S) \in \mathcal{I}_\rho^K$.

Proof. 1) \mathcal{I}_χ is closed under disjoint union. Thus it suffices to prove that for every atom $[a]_{\mathcal{G}}$ of $\mathbb{B}(\mathcal{G})$ we have $[a]_{\mathcal{G}} \subseteq \mathcal{I}_\chi$. We know that $[a]_{\mathcal{G}} = \{b \in G \mid \langle b \rangle = \langle a \rangle\}$. According to Theorem 3.2.7, we need to prove, for g_1 and g_2 in G with $g_1 \sim g_2$, that:

$$|\text{cl}(g_1) \cap [a]_{\mathcal{G}}| = |\text{cl}(g_2) \cap [a]_{\mathcal{G}}|.$$

If $a^k \in \text{cl}(g_1) \cap [a]_{\mathcal{G}}$, then we have $\gcd(\text{ord}(a), k) = 1$ and $\text{ord}(a) = \text{ord}(a^k) = \text{ord}(g_1)$. Then $\gcd(k, \text{ord}(g_1)) = 1$. Since $g_1 \sim g_2$, so $g_2 = g_1^m$ for a m relatively prime with respect to $\text{ord}(g_2) = \text{ord}(g_1) = \text{ord}(a)$. We have $a^{km} \in \text{cl}(g_2)$ and $\text{ord}(a)$ is relatively prime with respect to k and m , and so with respect to km . Then $a^{km} \in [a]_{\mathcal{G}} \cap \text{cl}(g_2)$. This shows that $|\text{cl}(g_1) \cap [a]_{\mathcal{G}}| \leq |\text{cl}(g_2) \cap [a]_{\mathcal{G}}|$. By symmetry we have $|\text{cl}(g_1) \cap [a]_{\mathcal{G}}| \geq |\text{cl}(g_2) \cap [a]_{\mathcal{G}}|$ as required.

2) Let $\mathcal{X} = \{\text{Cay}(G, H) : H \triangleleft G\}$. By Lemma 2.3.3, the adjacency matrices of all graphs in \mathcal{X} commute and hence they share a common orthogonal set B of eigenvectors. For every $X \in \mathcal{X}$ we have that X has B as a basis of eigenvectors, and X is a disjoint union of cliques (with loops at every vertex), so X is B -integral. It now follows from Lemma 2.3.2 that $\mathbb{B}(\mathcal{X}) = \{\text{Cay}(G, S) : S \in \mathbb{B}(\mathcal{N})\}$ is B -integral. Thus, for every representation ρ of G and $S \in \mathbb{B}(\mathcal{N})$ we have by the remark after Theorem 3.1.3 that $\rho(S)$ is integral. Thus $S \in \mathcal{I}_{\rho}$. This completes the proof.

3) If $S \in \mathcal{I}_{\rho}$ then $\rho(S)$ is an integral matrix for every representation ρ of G . If λ is a character of G then λ is afforded by a representation ρ_{λ} of G . This implies $\lambda(S) = \text{tr}(\rho_{\lambda}(S))$. Since trace of a square matrix is the sum of eigenvalues, the integrality of $\lambda(S)$ follows from the integrality of $\rho_{\lambda}(S)$.

4) Suppose $H \in \mathcal{G}$, and $h \in H$. We have,

$$\rho(H) = \sum_{g \in H} \rho(g) = \sum_{g \in H} \rho(gh) = \rho(h) \left(\sum_{g \in H} \rho(g) \right) = \rho(h) \rho(H).$$

If there is an h in H such that $\rho(h) \neq I$, then $\rho(H) = 0$ otherwise $\rho(H) = |H|I$. In both cases, $\rho(H)$ is an integral matrix and so $H \in \mathcal{I}_{\rho}$.

5) This is obvious since $\mathcal{N} \subseteq \mathcal{G}$.

6) If G is abelian, then from Theorem 2.4.4 in Chapter 2, we have that $\mathbb{B}(\mathcal{G}) = \mathcal{I}_{\chi}$. We prove that for a non-abelian group G , $\mathbb{B}(\mathcal{G}) \neq \mathcal{I}_{\chi}$. We suppose G is non-abelian and $\mathbb{B}(\mathcal{G}) = \mathcal{I}_{\chi}$. We will prove that if $a \notin Z(G)$, then $\text{ord}(a) = 2$. Suppose that $a \notin Z(G)$ and $\text{ord}(a) \neq 2$. If $[a]$ denote the atom of $\mathbb{B}(\mathcal{G})$ containing a , then we know that $|[a]| = \phi(\text{ord}(a)) > 1$. If $g \in G$ and b in $[a]$, we claim that $b^g = g^{-1}bg \in [a]$. Otherwise, if $A = \left([a] - \{b\} \right) \cup \{b^g\}$, then clearly for every $\chi \in \text{Irr}(G)$ we have $\chi(A) = \chi([a]) \in \mathbb{Z}$. This implies that $[a] \setminus A \in \mathbb{B}(\mathcal{G}) = \mathcal{I}_{\chi}$. That is to say $\{b\} \in \mathbb{B}(\mathcal{G})$, which is impossible

since the minimal set in $\mathbb{B}(\mathcal{G})$ containing b is the atom $[a]$ which has more than one element. Thus $[a]$ is a union of conjugacy classes all of the same size. Let $\{a_1, \dots, a_k\}$ and $l = |\text{cl}(a_i)|$ be, respectively, the set of distinct representatives and the common size of these classes. Because $[a] \in \mathbb{B}(\mathcal{G}) = \mathcal{I}_\chi$, we have

$$\chi([a]) = \sum_{b \in [a]} \chi(b) = \sum_{i=1}^k l \chi(a_i) = l \sum_{i=1}^k \chi(a_i) \in \mathbb{Z}.$$

We know the values of characters are algebraic integers, thus this implies $\sum_{i=1}^k \chi(a_i) \in \mathbb{Z}$. This proves that $\{a_1, \dots, a_k\} \subseteq [a]$ is a character integral set and thus an element in $\mathbb{B}(\mathcal{G})$. As $[a]$ is an atom this implies that $\{a_1, \dots, a_k\} = [a]$, $l = 1$ and so $a \in Z(G)$. We know prove that $G = Z(G)$. If $g_1, g_2 \notin Z(G)$, then $\text{ord}(g_1 g_2) = 2$ because otherwise

$$g_1 g_2 \in Z(G) \Rightarrow g_1(g_1 g_2) = (g_1 g_2)g_1 \Rightarrow g_1 g_2 = g_2 g_1 \Rightarrow \text{ord}(g_1 g_2) = 2.$$

On the other hand, $g_1, g_2 \notin Z(G)$ implies that $\text{ord}(g_1) = \text{ord}(g_2) = \text{ord}(g_1 g_2) = 2$, which implies that $g_1 g_2 = g_2 g_1$. We have shown that if $g_1 \notin Z(G)$, then g_1 commutes with all elements inside and outside of $Z(G)$. By definition of $Z(G)$ this implies that $g_1 \in Z(G)$. This contradiction implies that there are no elements outside of $Z(G)$ and thus $G = Z(G)$ and so G is abelian.

- 7) If ρ is a representation of G , then by restriction to H we will get a representation ρ_H of H . If $S \subseteq H$, we have

$$\rho(S) = \sum_{s \in S} \rho(s) = \sum_{s \in S} \rho_H(s) = \rho_H(S).$$

Clearly, if $S \in \mathcal{I}_\rho^H$, then $S \in \mathcal{I}_\rho^G$.

- 8) Let a be an element in G and $[a]$ the atom of $\mathbb{B}(\mathcal{G})$ containing a . If ρ is a matrix representation of G , then the restriction of ρ to the cyclic group $H = \langle a \rangle$ is a representation of $H = \langle a \rangle$. We have also $\mathcal{I}_\rho^H \subseteq \mathcal{I}_\rho^G$ and hence it is no loss of generality to assume $G = \langle a \rangle$. This implies that G is abelian, and so $\mathcal{I}_\chi = \mathcal{I}_\rho$. Since for an abelian group we have $\mathbb{B}(\mathcal{G}) = \mathcal{I}_\chi$, it follows that $[a] \in \mathbb{B}(\mathcal{G}) \subseteq \mathcal{I}_\rho$.
- 9) Every irreducible representation of $H \times K$ is the tensor product of an irreducible representation of H with an irreducible representation of K . Notice that H and K commute

element-wise. Assume $\rho_1 \in \text{IRR}(H)$ and $\rho_2 \in \text{IRR}(K)$. If $S_1 \in \mathcal{I}_\rho^H$ and $S_2 \in \mathcal{I}_\rho^K$, then we have;

$$(\rho_1 \otimes \rho_2)(S_1 \times S_2) = \sum_{(s_1, s_2) \in S_1 \times S_2} \rho_1(s_1) \otimes \rho_2(s_2) = \sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \rho_1(s_1) \otimes \rho_2(s_2) = \rho_1(S_1) \otimes \rho_2(S_2).$$

This proves, that $S_1 \times S_2$ is in \mathcal{I}_ρ^G .

10) Let $\mathbf{1}_K$ denote the principal representation of K . If $\rho \in \text{IRR}(H)$, Then $\rho \otimes \mathbf{1}_K$ is a representation of $H \times K$. Since $(\rho \otimes \mathbf{1}_K)(S) = \rho(\pi_H(S))$, we have $\pi_H(S) \in \mathcal{I}_\rho^H$. □

If we define $a \equiv_{\mathcal{N}} b$ if and only if $\langle \text{cl}(a) \rangle = \langle \text{cl}(b) \rangle$ then one can easily check that the classes of this equivalence relation are the atoms of $\mathbb{B}(\mathcal{N})$. It is interesting if one can find an easy way to describe an atom $[a]_{\mathcal{N}}$ in this algebra. If D is an integral domain, then we say a character χ of a group G is *realized over D* if all character values $\chi(g)$ ($g \in G$) are in D .

Theorem 3.2.9. *Suppose $P(G)$ denotes the power set of the group G . The following are equivalent;*

- 1) $\mathcal{I}_\chi = P(G)$
- 2) If $g_1 \sim g_2$ then $\text{cl}(g_1) = \text{cl}(g_2)$.
- 3) Every character of G is realized over \mathbb{Q} .

Proof. (**1** \Rightarrow **2**), If we take $S = \text{cl}(g_1)$ in theorem 3.2.7, then we have $|\text{cl}(g_1)| = |\text{cl}(g_1) \cap \text{cl}(g_2)|$. Since $\text{cl}(g_1) \cap \text{cl}(g_2) \subseteq \text{cl}(g_1)$, this implies that $\text{cl}(g_1) \subseteq \text{cl}(g_2)$. By symmetry we have; $\text{cl}(g_1) \subseteq \text{cl}(g_2)$ as well and so 2 is obtained.

(**2** \Rightarrow **1**) Another application of theorem 3.2.7 will imply that every subset S of G is character integral and so $\mathcal{I}_\chi = P(G)$.

(**1** \Leftrightarrow **3**) We notice that character values are algebraic integers, and so they are rational if and only if they are integral. □

If a finite group G satisfies one and therefore all the conditions in the theorem 3.2.9 then G is called a *rational group* or a \mathbb{Q} -group. There is no classification of rational groups, and the list of rational groups contains lots of interesting groups. For further studies of rational

groups and their structures we suggest the interesting book “Structure and Representations of \mathbb{Q} -Groups” by Dennis Kletzing (see [37]). We call a group G , *Cayley integral group* if $\mathcal{I}_\rho = P(G)$. In Chapter 4, we will classify all Cayley integral groups. Interestingly, there are just a few classes of Cayley integral groups. This proves once more that the notion of representation integrality is more restrictive than character integrality.

3.3 Hamiltonian groups

In this section and next, we investigate to what extent theorem 2.4.4 would hold in some other groups. As a natural candidate, we have decided to consider *Dedekind groups*, i.e. groups whose every subgroup is normal. Every abelian group is Dedekind; non-abelian Dedekind groups are also called *Hamiltonian groups*, and they have a simple characterization that is due to Baer, cf. [30, Theorem 12.5.4].

Theorem 3.3.1. *A finite group is Hamiltonian if and only if it can be written as a direct product $Q_8 \times A$, where Q_8 is the group of quaternions and A is an abelian group without elements of order 4.*

We provide sufficient and necessary conditions for integrality of the spectra of Cayley multigraphs over such groups (Theorem 3.3.2). By using this characterization, we show that integrality of Cayley graphs over Hamiltonian groups is easy to decide in certain special cases, while it leads to challenging combinatorial problems in some other special cases.

Throughout this section, by boolean algebra we mean the boolean algebra generated by subgroups, i.e. $\mathbb{B}(\mathcal{G})$. We use the simplified notation $\mathbb{B}(H)$ instead of $\mathbb{B}(\mathcal{G}_H)$ to denote the boolean algebra generated by subgroups of H . Let \mathcal{H} be the family of groups of the form $Q_8 \times A$ where A is a finite abelian group and Q_8 is the quaternion group represented as follows:

$$Q_8 = \langle -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

Let us recall that a finite group G is *Hamiltonian* if it is non-abelian and every subgroup of G is normal. By Baer’s result (Theorem 3.3.1), every Hamiltonian group is in \mathcal{H} .

In this section, we obtain a necessary and sufficient condition for a multigraph $\text{Cay}(G, S)$ to be integral, where $G \in \mathcal{H}$ and $S \subseteq G$ is a symmetric multiset of elements of G .

The table below is the character table of Q_8 .

$g \in Q_8$	1	-1	i	j	k
$\text{cl}(g)$	{1}	{-1}	{ $i, -i$ }	{ $j, -j$ }	{ $k, -k$ }
$\mathbb{1}_{Q_8}$	1	1	1	1	1
λ_i	1	1	1	-1	-1
λ_j	1	1	-1	1	-1
λ_k	1	1	-1	-1	1
ε	2	-2	0	0	0

where ε is the character afforded by the representation ρ_ε defined below:

$$\rho_\varepsilon(1) = I, \quad \rho_\varepsilon(i) = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}, \quad \rho_\varepsilon(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho_\varepsilon(k) = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}$$

where the value \mathbf{i} appearing in the matrices is the complex imaginary unit $\sqrt{-1}$. Also note that $\rho_\varepsilon(-g) = -\rho_\varepsilon(g)$ for every $g \in Q_8$ and that $\text{IRR}(Q_8) = \{\mathbb{1}_{Q_8}, \lambda_i, \lambda_j, \lambda_k, \rho_\varepsilon\}$.

Let $G = Q_8 \times A$, where A is an abelian group, and let $S \subseteq G$ be a symmetric multiset of elements of G . For every $q \in Q_8$, let B_q be the multiset

$$B_q = \{a \in A \mid (q, a) \in S\} \tag{3.2}$$

in which the multiplicity of $a \in B_q$ is equal to the multiplicity of (q, a) in S .

Since S is symmetric, we have $B_1 = B_1^{-1}$, $B_{-1} = B_{-1}^{-1}$, and $B_{-q} = B_q^{-1}$ for every $q \in Q_8 \setminus \{1, -1\}$. In particular, this implies that $\lambda(B_{-q}) = \overline{\lambda(B_q)}$, for every $\lambda \in \text{Irr}(A)$. For every multiset D of elements of A , we define

$$\widehat{\lambda}(D) = \lambda(D) - \lambda(D^{-1}) = \sum_{g \in D} \mu_D(g)(\lambda(g) - \lambda(g^{-1})) = \sum_{g \in D} \mu_D(g)(\lambda(g) - \overline{\lambda(g)}).$$

In particular, for every $q \in Q_8$, $\widehat{\lambda}(B_q) = \lambda(B_q) - \lambda(B_{-q})$. The following is the main result of this section.

Theorem 3.3.2. *Let $G = Q_8 \times A$, where A is an abelian group, and let S be a symmetric multiset of elements of G . Then $\text{Cay}(G, S)$ is integral if and only if the following holds:*

- (i) $B_1, B_{-1} \in \mathcal{C}(\mathcal{G}_A)$.
- (ii) *The multiset union $B_q \cup B_{-q} \in \mathcal{C}(\mathcal{G}_A)$, for every $q \in Q_8 \setminus \{-1, 1\}$.*
- (iii) $\widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2$ *is a negative square of an integer, for every $\lambda \in \text{Irr}(A)$.*

Proof. Lemma 3.1.3 shows that $\text{Cay}(G, S)$ is integral if and only if the matrix $\sum_{s \in S} \mu_S(s) \phi(s)$ is integral for every $\phi \in \text{IRR}(G)$. Since ϕ is an irreducible representation of the direct product $Q_8 \times A$, it can be written in the form $\phi = \rho \times \lambda$ for some $\rho \in \text{IRR}(Q_8)$ and $\lambda \in \text{Irr}(A)$ (where we identify $\text{Irr}(A)$ and $\text{IRR}(A)$ since all irreducible representations of A are 1-dimensional). In other words, $\phi(q, a) = \lambda(a)\rho(q)$ for every $(q, a) \in Q_8 \times A$. Consequently, $\text{Cay}(G, S)$ is integral if and only if the matrices

$$A^{(\rho, \lambda)} = \sum_{(q, a) \in S} \mu_S((q, a)) (\rho \times \lambda)(q, a) = \sum_{(q, a) \in S} \mu_S((q, a)) \lambda(a) \rho(q)$$

are integral for every $\rho \in \text{IRR}(Q_8)$ and every $\lambda \in \text{Irr}(A)$. By definition of B_q we can write the matrix $A^{(\rho, \lambda)}$ in the following form:

$$A^{(\rho, \lambda)} = \sum_{(q, a) \in S} \mu_S((q, a)) \lambda(a) \rho(q) = \sum_{q \in Q_8} \lambda(B_q) \rho(q). \quad (3.3)$$

Integrality of the matrix in (3.3) (with $\rho = \rho_\varepsilon$ and $\lambda \in \text{Irr}(A)$ arbitrary) together with the fact that the trace of a matrix is equal to the sum of its eigenvalues implies that

$$\text{tr} \left(\sum_{q \in Q_8} \lambda(B_q) \rho_\varepsilon(q) \right) = \sum_{q \in Q_8} \lambda(B_q) \varepsilon(q) = 2(\lambda(B_1) - \lambda(B_{-1})) \in \mathbb{Z}.$$

It follows that

$$\lambda(B_1) - \lambda(B_{-1}) \in \mathbb{Q}. \quad (3.4)$$

Let $\rho \in \{\mathbb{1}_{Q_8}, \lambda_i, \lambda_j, \lambda_k\}$ be a degree-one representation of Q_8 and let $\lambda \in \text{Irr}(A)$. Define $\lambda^+(B_q) = \lambda(B_q) + \lambda(B_{-q})$. Observe that $\rho(q) = \rho(-q)$ for every $q \in Q_8$. Therefore, integrality of the matrices $A^{(\rho, \lambda)}$ in (3.3) implies by the same argument as above that

$$\rho(1)\lambda^+(B_1) + \rho(i)\lambda^+(B_i) + \rho(j)\lambda^+(B_j) + \rho(k)\lambda^+(B_k) \in \mathbb{Z}.$$

This yields the following four conditions (one for each $\rho \in \{1, \lambda_i, \lambda_j, \lambda_k\}$):

$$\begin{aligned} \lambda^+(B_1) + \lambda^+(B_i) + \lambda^+(B_j) + \lambda^+(B_k) &\in \mathbb{Z} \\ \lambda^+(B_1) + \lambda^+(B_i) - \lambda^+(B_j) - \lambda^+(B_k) &\in \mathbb{Z} \\ \lambda^+(B_1) - \lambda^+(B_i) + \lambda^+(B_j) - \lambda^+(B_k) &\in \mathbb{Z} \\ \lambda^+(B_1) - \lambda^+(B_i) - \lambda^+(B_j) + \lambda^+(B_k) &\in \mathbb{Z} \end{aligned} \quad (3.5)$$

Since the matrix of coefficients of the linear system (3.5) is invertible, this implies that $\lambda^+(B_q) \in \mathbb{Q}$ for every $q \in Q_8$. In particular, since $\lambda^+(B_1) = \lambda(B_1) + \lambda(B_{-1}) \in \mathbb{Q}$, we

conclude by using (3.4) that $\lambda(B_1) \in \mathbb{Q}$ and $\lambda(B_{-1}) \in \mathbb{Q}$, while for $q \in Q_8 \setminus \{1, -1\}$, we have $\lambda(B_q) + \lambda(B_{-q}) \in \mathbb{Q}$.

Rationality of $\lambda(X)$ for every $\lambda \in \text{Irr}(A)$ has been discussed in the proof of Lemma 2.4.2, where it was proved that this is equivalent to the condition that $X \in \mathcal{C}(\mathcal{G}_A)$. Therefore, the conclusions stated in the previous paragraph imply (i) and (ii).

Conversely, notice that by Theorem 2.4.4, (i) and (ii) imply integrality of the matrices in (3.3), where ρ is any degree-one representation of Q_8 and $\lambda \in \text{Irr}(A)$.

For (iii), we consider the degree-two representation ρ_ε . As observed above, $\rho_\varepsilon(-q) = -\rho_\varepsilon(q)$ for every $q \in Q_8$, and hence

$$\sum_{q \in Q_8} \lambda(B_q) \rho_\varepsilon(q) = \widehat{\lambda}(B_1)I + \widehat{\lambda}(B_i) \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} + \widehat{\lambda}(B_j) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \widehat{\lambda}(B_k) \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix}.$$

As mentioned above, (3.4) implies that $\widehat{\lambda}(B_1) \in \mathbb{Z}$. Therefore, $\sum_{q \in Q_8} \lambda(B_q) \rho_\varepsilon(q)$ is integral if and only if the matrix

$$M = \begin{pmatrix} \mathbf{i}\widehat{\lambda}(B_i) & \widehat{\lambda}(B_j) + \mathbf{i}\widehat{\lambda}(B_k) \\ -\widehat{\lambda}(B_j) + \mathbf{i}\widehat{\lambda}(B_k) & -\mathbf{i}\widehat{\lambda}(B_i) \end{pmatrix}.$$

is integral. By considering the characteristic polynomial of M , it is easy to see that M is integral if and only if $\widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2$ is the negative square of an integer. Hence, integrality of $\text{Cay}(G, S)$ implies (iii), and conversely, (iii) implies integrality of the matrices $A^{(\rho, \lambda)}$. This completes the proof. \square

3.4 Some special cases

In this section we consider some special cases of Hamiltonian groups by applying Theorem 3.3.2. This result gives a simple characterization in some cases, and leads to interesting combinatorial problems in some other cases.

3.4.1 Simple Cayley graphs of $Q_8 \times C_p$, where $p \neq 3$

As the first special case of using Theorem 3.3.2 we consider Hamiltonian groups $G = Q_8 \times C_p$, where $p \neq 3$ is a prime and C_p is the cyclic group of order p . In analogy with the abelian case, we obtain the following complete characterization for integrality of *simple* Cayley graphs over this group. The multigraph version is different and is treated in a separate section.

Theorem 3.4.1. *Let $p \neq 3$ be a prime and let S be a symmetric subset of $Q_8 \times C_p$. The Cayley graph $\text{Cay}(Q_8 \times C_p, S)$ is integral if and only if $S \in \mathbb{B}(\mathcal{G}_{Q_8 \times C_p})$.*

This result is a direct consequence of the following:

Theorem 3.4.2. *Let $G = Q_8 \times C_p$, for a prime $p \neq 3$. Let $S \subseteq G$ be a symmetric subset of G , and let B_q ($q \in Q_8$) be defined as in (3.2). Then $\text{Cay}(G, S)$ is integral if and only if the following conditions hold:*

$$(P1) \quad B_1, B_{-1} \in \mathbb{B}(\mathcal{G}_{C_p}).$$

$$(P2) \quad \text{For every } q \in Q_8 \setminus \{1, -1\}, B_q = B_{-q} \in \mathbb{B}(\mathcal{G}_{C_p}).$$

Proof. By Theorem 3.3.2, it suffices to show that (P2) holds if and only if conditions (ii) and (iii) in Theorem 3.3.2 hold. The “only if” part is trivial, since (P2) implies that $\widehat{\lambda}(B_i) = \widehat{\lambda}(B_j) = \widehat{\lambda}(B_k) = 0$. For the “if” part suppose that conditions (ii) and (iii) of Theorem 3.3.2 hold. By condition (iii), for every $\lambda \in \text{Irr}(C_p)$ there is an integer α_λ so that

$$\widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2 = -\alpha_\lambda^2. \quad (3.6)$$

Let e be the unit in C_p and let $E_1 = \{e\}$ and $E_2 = C_p \setminus E_1$ be the two equivalence classes of C_p . Let $q \in Q_8 \setminus \{1, -1\}$. Recall that since S is symmetric we have $B_q^{-1} = B_{-q}$.

If $B_q \in \mathbb{B}(\mathcal{G}_{C_p})$ then $B_{-q} = B_q$. This is true because $B_q^{-1} = B_{-q}$, and the sets E_1 and E_2 are symmetric. Hence in this case $B_q = B_{-q}$ and $\widehat{\lambda}(B_q) = 0$. If $p = 2$, then every subset of C_p is in $\mathbb{B}(\mathcal{G}_{C_p})$, so (P2) holds in this case, and we may henceforth assume that $p \geq 5$.

If $B_q \notin \mathbb{B}(\mathcal{G}_{C_p})$, then by condition (ii) and the fact that $B_q^{-1} = B_{-q}$, we conclude that $E_2 \subseteq B_q \Delta B_{-q}$, thus the support of $B_q - B_{-q}$, viewed as an element of the group algebra $\mathbb{C}C_p$, contains $p - 1$ distinct elements (that is, the whole class E_2), where an element and its inverse appear with opposite signs. In particular, the sum of coefficients of elements of $B_q - B_{-q}$ is 0.

Let us write $B'_q = B_q \setminus B_{-q}$, and observe that for every $q \in Q_8$, either $B'_q = \emptyset$ or

$|B'_q| = \frac{1}{2}(p-1)$. Now, (3.6) can be written as follows

$$\begin{aligned}
 -\alpha_\lambda^2 &= \widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2 \\
 &= \widehat{\lambda}(B'_i)^2 + \widehat{\lambda}(B'_j)^2 + \widehat{\lambda}(B'_k)^2 \\
 &= \lambda((B'_i - B'_{-i})^2) + \lambda((B'_j - B'_{-j})^2) + \lambda((B'_k - B'_{-k})^2) \\
 &= \lambda((B'_i - B'_{-i})^2 + (B'_j - B'_{-j})^2 + (B'_k - B'_{-k})^2) \\
 &= \lambda\left(-2(|B'_i| + |B'_j| + |B'_k|)e + \sum_{g \in E_2} a_g g\right) \\
 &= -2(|B'_i| + |B'_j| + |B'_k|) + \lambda\left(\sum_{g \in E_2} a_g g\right) \tag{3.7}
 \end{aligned}$$

where $a_g \in \mathbb{Z}$ for every $g \in E_2$. Since the sum of coefficients in $B_q - B_{-q}$ is zero, it follows that the sum of coefficients in $(B_q - B_{-q})^2$ is also zero. Thus, (3.7) implies that

$$\sum_{g \in E_2} a_g = 2(|B'_i| + |B'_j| + |B'_k|). \tag{3.8}$$

By (3.7), $\lambda(\sum_{g \in E_2} a_g g) \in \mathbb{Q}$ for every $\lambda \in \text{Irr}(C_p)$. It follows by Lemma 2.4.2, that all coefficients a_g are equal, and from (3.8) we conclude that for every $g \in E_2$:

$$a_g = \frac{2(|B'_i| + |B'_j| + |B'_k|)}{p-1}.$$

We also know that for each non-principal character $\lambda \in \text{Irr}(C_p)$ we have $\sum_{g \in C_p} \lambda(g) = 0$. Thus, $\sum_{g \in E_2} \lambda(g) = -1$, and we can rewrite (3.7) as follows:

$$-\alpha_\lambda^2 = -2(|B'_i| + |B'_j| + |B'_k|) - \frac{2(|B'_i| + |B'_j| + |B'_k|)}{p-1}.$$

This gives the following conclusion:

$$\alpha_\lambda^2 = 2(|B'_i| + |B'_j| + |B'_k|) \frac{p}{p-1}. \tag{3.9}$$

We know that for every $q \in Q_8$, $|B'_q|$ is either 0 or $\frac{1}{2}(p-1)$. By (3.9), $p-1$ divides $2(|B'_i| + |B'_j| + |B'_k|)$. Let β denote the number of elements $q \in \{i, j, k\}$ such that $|B'_q| = \frac{p-1}{2}$. Then we conclude from (3.9) that $\alpha_\lambda^2 = \beta p$. Since $0 \leq \beta \leq 3$ and $p \geq 5$, this is possible only when $\alpha = 0$. However, in that case (P2) holds. \square

3.4.2 $Q_8 \times C_3$

The conclusion of Theorem 3.4.2 does not hold for $p = 3$. An example is provided in the next observation.

Observation 3.4.3. *Let $G = Q_8 \times C_3$, and $S = \{(i, 1), (-i, 2), (j, 1), (-j, 2), (k, 1), (-k, 2)\}$. Then $\text{Cay}(G, S)$ is integral but $S \notin \mathbb{B}(\mathcal{G})$.*

To see this, we verify conditions (i)–(iii) of Theorem 3.3.2. Conditions (i) and (ii) are obvious; (iii) is left to the reader.

This graph is indeed a very interesting vertex-transitive graph whose properties are discussed below. Let us remark at this point that the proof of the Theorem 3.4.2 shows that the example in Observation 3.4.3 is the only integral simple Cayley graph of $Q_8 \times C_3$ (up to Cayley graph isomorphisms and up to choice of $B_1, B_{-1} \in \mathbb{B}(\mathcal{G}_{C_3})$) that fails to satisfy the conclusion of Theorem 3.4.2.

This graph has a natural tripartition according to the first coordinate, and the bipartite graphs obtained from it by removing one of these tripartite classes is the Möbius-Kantor graph. The Möbius-Kantor graph is the unique double-cover of the cube of girth 6 and it sits naturally as a subgraph of the 4-cube. The graph of the 24-cell is also tripartite with classes of size 8, and deleting any one yields a 4-cube.

3.4.3 Cayley multigraphs of $Q_8 \times C_p$

Theorem 3.4.2 does not hold for the multigraph case. In this section we shall provide infinitely many examples confirming this. We let $C_p = \{a^t \mid 0 \leq t < p\}$, the cyclic group of order p generated by a . We consider the multisets B_q ($q \in Q_8 \setminus \{1, -1\}$) defined as in (3.2), and we set $B_1 = B_{-1} = \emptyset$. In order to satisfy conditions (i)–(iii) of Theorem 3.3.2, we need that $B_q \cup B_{-q} \in \mathcal{C}(\mathcal{G}_{C_p})$ and $\widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2$ is a negative square of an integer, for every $\lambda \in \text{Irr}(C_p)$. As before, for every $q \in Q_8 \setminus \{1, -1\}$ we define $B'_q = B_q \setminus (B_q \cap B_{-q})$, where $B_q \cap B_{-q}$ is the multiset in which the multiplicity of any $x \in C_p$ is equal to the minimum of multiplicities of x in B_q and in B_{-q} . Thus, in particular, $\widehat{\lambda}(B_q) = \widehat{\lambda}(B'_q)$. Note that B'_q and B'_{-q} are disjoint and the condition that generating multiset is symmetric is equivalent to the requirement that the multiplicity of a^t ($0 \leq t < p$) in B'_q is the same as the multiplicity of a^{-t} in B'_{-q} . The following is a well-known result from number theory.

Lemma 3.4.4. *If p is a prime number and $p \equiv 1 \pmod{4}$, then the Diophantine equation $x^2 + y^2 = pz^2$ has infinitely many solutions satisfying $\gcd(x, y, z) = 1$.*

A solution of the Diophantine equation $x^2 + y^2 = pz^2$ is *primitive* if $\gcd(x, y, z) = 1$. Clearly, every integral multiple of (x, y, z) is also a solution. The solution $(0, 0, 0)$ is called the *trivial solution*.

Lemma 3.4.5. *Let (r, s, t) be a non-trivial solution for the Diophantine equation $x^2 + y^2 = 5z^2$. Let $D_1 = ra + sa^2$, $D_2 = ra + sa^3$ and $D_3 = 0$, be elements of $\mathbb{C}C_5$, where a is a generator of C_5 . Then*

$$\widehat{\lambda}(D_1)^2 + \widehat{\lambda}(D_2)^2 + \widehat{\lambda}(D_3)^2 = -(5t)^2.$$

Proof. For any x and y in \mathbb{R} , we have the following equation in $\mathbb{C}C_5$:

$$(x(a - a^4) + y(a^2 - a^3))^2 = -2(x^2 + y^2) + (y^2 - 2xy)(a + a^4) + (x^2 + 2xy)(a^2 + a^3).$$

Thus,

$$\widehat{\lambda}(D_1)^2 = -2(r^2 + s^2) + (s^2 - 2rs)\lambda(a + a^4) + (r^2 + 2rs)\lambda(a^2 + a^3),$$

$$\widehat{\lambda}(D_2)^2 = -2(r^2 + s^2) + (r^2 + 2rs)\lambda(a + a^4) + (s^2 - 2rs)\lambda(a^2 + a^3).$$

Clearly, $\widehat{\lambda}(D_3)^2 = 0$. We notice also that for each non-principal character $\lambda \in \text{Irr}(C_5)$ we have $\sum_{i=1}^4 \lambda(a^i) = -1$. Therefore, $\widehat{\lambda}(D_1)^2 + \widehat{\lambda}(D_2)^2 + \widehat{\lambda}(D_3)^2 = -5(r^2 + s^2) = -(5t)^2$. \square

Corollary 3.4.6. *There are infinitely many multisets S (none of which is a multiple of another) such that $\text{Cay}(Q_8 \times C_5, S)$ is integral but $S \notin \mathcal{C}(\mathcal{G})$.*

Proof. Let us start with a primitive solution (m, n, α) of the Diophantine equation $x^2 + y^2 = 5z^2$. Since $(2m, 2n, 2\alpha)$ is a solution of the Diophantine equation $x^2 + y^2 = 5z^2$, we can construct D_1 , D_2 and D_3 as in the previous lemma, i.e., $D_1 = 2ma + 2na^2$, $D_2 = 2na + 2ma^3$ and $D_3 = 0$. Suppose without loss of generality that $n \leq m$. Let us take $B_i = \{2ma, (m+n)a^2, (m-n)a^3\}$, $B_j = \{(m+n)a, (m-n)a^4, 2ma^3\}$, $B_{-i} = B_i^{-1}$, $B_{-j} = B_j^{-1}$, and $B_k = B_{-k} = \emptyset$ (where the coefficients of a^t in the the set notation denote multiplicities). Then $B_i + B_{-i} \in \mathcal{C}(\mathcal{G}_{C_5})$, $B_j + B_{-j} \in \mathcal{C}(\mathcal{G}_{C_5})$, and $B_k + B_{-k} \in \mathcal{C}(\mathcal{G}_{C_5})$. We also have $B'_i = D_1$, $B'_j = D_2$ and $B'_k = D_3$. From the previous lemma we get

$$\widehat{\lambda}(B_i)^2 + \widehat{\lambda}(B_j)^2 + \widehat{\lambda}(B_k)^2 = \widehat{\lambda}(B'_i)^2 + \widehat{\lambda}(B'_j)^2 + \widehat{\lambda}(B'_k)^2 = -(10\alpha)^2.$$

So, clearly conditions (i)–(iii) of Theorem 3.3.2 are satisfied for the generating multiset S arising from B_i , B_j and B_k , but $B_i, B_j \notin \mathcal{C}(\mathcal{G}_{C_5})$. Thus $S \notin \mathcal{C}(\mathcal{G}_{Q_8 \times C_5})$, while according to Theorem 3.3.2 the Cayley graph $\text{Cay}(Q_8 \times C_5, S)$ is integral. \square

The case $p = 7$ is similar. First, we observe that there are infinitely many primitive solutions for Diophantine equation $x^2 + y^2 + z^2 = 7\alpha^2$. If we assume (m, n, l, α) is one of these solutions, then we can define

$$B'_i = ma + na^2 + la^3, \quad B'_j = la + ma^2 + na^3, \quad B'_k = na + la^2 + ma^3.$$

It is easy to see that condition (iii) of Theorem 3.3.2 holds. As in Corollary 3.4.6, we can define B_i , B_j and B_k using correspondence with B'_i , B'_j and B'_k such that conditions (i)–(iii) of Theorem 3.3.2 are satisfied. This gives rise to integral Cayley multigraphs of $Q_8 \times C_7$ whose generating multiset is not in the lattice $\mathcal{C}(\mathcal{G}_{Q_8 \times C_7})$.

3.4.4 Simple Cayley graphs of $Q_8 \times C_p^d$

As the last special case we consider the group $G = Q_8 \times C_p^d$, where p is a prime and $d \geq 2$. Here the abelian direct factor of G is an elementary abelian p -group, thus every non-identity element has order p . If $[a]$ denotes the equivalence class containing a with respect to the relation \sim in C_p^d and if $a \neq e$ (where e is the identity element of C_p^d), then $[a] = \{a^t \mid 1 \leq t \leq p-1\}$. We also know that $[e] = \{e\}$; we call this the trivial equivalence class. Since each non-identity element in C_p^d has order p , each non-trivial class is of order $p-1$, and the number of non-trivial classes is equal to $n_d = \frac{p^d-1}{p-1}$. Label these classes as A_r for $1 \leq r \leq n_d$. If λ is a non-principal character of C_p^d , then $|\text{Im}(\lambda)| = p$ and therefore $\ker(\lambda)$ is a subgroup of order p^{d-1} .

Let us assume that $\text{Cay}(G, S)$ is integral. Then we derive in the same way as in the case of $Q_8 \times C_p$ that there is an integer α_λ such that

$$-\alpha_\lambda^2 = \widehat{\lambda}(B'_i)^2 + \widehat{\lambda}(B'_j)^2 + \widehat{\lambda}(B'_k)^2 = -2(|B'_i| + |B'_j| + |B'_k|) + \lambda\left(\sum_{g \in C_p^d \setminus \{e\}} a_g g\right). \quad (3.10)$$

Since (3.10) holds for every $\lambda \in \text{Irr}(C_p^d)$, we conclude by Lemma 2.4.2 that the coefficients a_g

are constant on each equivalence class A_r . Let b_r be the common value for a_g , $g \in A_r$. Then

$$\begin{aligned} -\alpha_\lambda^2 &= -2(|B'_i| + |B'_j| + |B'_k|) + \lambda\left(\sum_{r=1}^{n_d} \sum_{g \in A_r} b_r g\right) \\ &= -2(|B'_i| + |B'_j| + |B'_k|) + \sum_{r=1}^{n_d} b_r \lambda(A_r). \end{aligned} \quad (3.11)$$

Since each $A_r \cup \{e\}$ is a subgroup of order p , we have

$$\lambda(A_r) = \sum_{g \in A_r} \lambda(g) = \begin{cases} p-1, & A_r \subseteq \ker(\lambda) \\ -1, & A_r \not\subseteq \ker(\lambda). \end{cases} \quad (3.12)$$

We also notice that for $q \in \{i, j, k\}$ the element $B_q - B_{-q}$ of the group algebra has the sum of the coefficients equal to zero. By using this fact in combination with (3.11) and (3.12) for the case when λ is the principal character and noting that $\alpha_\lambda = 0$ in that case, we obtain the following analogue of (3.9):

$$2(|B'_i| + |B'_j| + |B'_k|) = (p-1) \sum_{r=1}^{n_d} b_r. \quad (3.13)$$

Using (3.13), we have for every non-principal character λ :

$$\alpha_\lambda^2 = 2(|B'_i| + |B'_j| + |B'_k|) - \sum_{r=1}^{n_d} b_r \lambda(A_r) = \sum_{r=1}^{n_d} b_r (p-1 - \lambda(A_r)). \quad (3.14)$$

The equality (3.12) shows that a non-zero contribution in the sum on the right side of (3.14) arises only when $A_r \not\subseteq \ker(\lambda)$. Let $I_\lambda \subseteq \{1, \dots, n_d\}$ be the set of values r for which $A_r \not\subseteq \ker(\lambda)$. Then we have:

$$\alpha_\lambda^2 = \sum_{r \in I_\lambda} b_r (p-1 - \lambda(A_r)) = p \sum_{r \in I_\lambda} b_r. \quad (3.15)$$

There is a natural geometric setting for these equations. View C_p^d as a vector space over C_p and consider the projective geometry $PG(d-1, p)$ consisting of all subspaces of C_p^d . The points in our projective geometry are the 1-dimensional subspaces of C_p^d which are in correspondence with A_1, A_2, \dots, A_{n_d} , and we label the point associated with A_i by b_i . The kernels of the non-principal characters of C_p^d correspond to the hyperplanes in our projective geometry (i.e. subspaces of dimension $d-1$ of C_p^d). So, equation 3.15 implies that the sum of the labels on the complement of every hyperplane is an integer of the form a^2/p . Although this is a meaningful consequence, it is not difficult to find labellings of the points in a projective geometry which satisfy this property, so a more complicated analysis will be required to understand the integrality of such Cayley graphs.

3.5 Dihedral groups

In this section, we will study the integrality of Cayley graphs over dihedral groups. Suppose S is a symmetric generating set of D_n . We know that $\text{Cay}(D_n, S)$ is integral if and only if for every ρ in $\text{IRR}(D_n)$, $\rho(S) = \sum_{s \in S} \rho(s)$ is an integral matrix.

We have the following presentation for D_n , which we will be using throughout this chapter.

$$D_n = \langle a, b \mid a^n = b^2 = 1, \quad ab = ba^{-1} \rangle$$

Here, we list some basic properties of D_n :

- $|D_n| = 2n$.
- $D_n = \{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$.
- For $1 \leq i \leq n$ we have $\text{cl}(a^i) = \{a^i, a^{-i}\}$.
- If n is odd, then $\text{cl}(ba^i) = \{ba^j \mid 1 \leq j \leq n\}$.
- If n is even, then:

$$\text{cl}(ba^{2i}) = \{ba^{2j} \mid 1 \leq j \leq n/2\} \quad \text{and} \quad \text{cl}(ba^{2i-1}) = \{ba^{2j-1} \mid 1 \leq j \leq n/2\}.$$

- For $1 \leq i \leq n$, a^i is called a *rotation* and $ba^i = a^{n-i}b$ a *reflection*.

Suppose S is a subset of D_n . Let us introduce the following notation;

$$S_{rot} = S \cap \{a^i \mid 1 \leq i \leq n\}, \quad S_{ref} = S \cap \{ba^i \mid 1 \leq i \leq n\}.$$

$$\hat{S}_{rot} = \{i \mid a^i \in S_{rot}\}, \quad \hat{S}_{ref} = \{i \mid ba^i \in S_{ref}\}.$$

S_{rot} is the set of all rotations in S , and S_{ref} is the set of all reflections in S . We will show that $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$, where $C_n = \langle a \rangle$ is the cyclic subgroup of D_n generated by the rotations.

3.5.1 Irreducible representations of D_n

In what will follow, ω_n will denote a primitive n -th root of unity.

- If $n = 2k + 1$, then $\text{IRR}(D_n) = \{\lambda_0, \lambda_1\} \cup \{\rho_i \mid 1 \leq i \leq k\}$, where the representations are determined by the following values:

$$\begin{aligned} \lambda_0 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_0(g) &= \begin{cases} 1 & g = a \\ 1 & g = b \end{cases} \\ \lambda_1 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_1(g) &= \begin{cases} 1 & g = a \\ -1 & g = b \end{cases} \\ \rho_i : D_n &\rightarrow GL_2(\mathbb{C}) & \rho_i(g) &= \begin{cases} \begin{pmatrix} \omega_n^i & 0 \\ 0 & \omega_n^{-i} \end{pmatrix} & g = a \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & g = b. \end{cases} \end{aligned}$$

- If $n = 2k$, then $\text{IRR}(D_n) = \{\lambda_0, \lambda_1, \lambda_2, \lambda_3\} \cup \{\rho_i \mid 1 \leq i \leq k - 1\}$, where the representations are determined by the following values:

$$\begin{aligned} \lambda_0 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_0(g) &= \begin{cases} 1 & g = a \\ 1 & g = b \end{cases} \\ \lambda_1 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_1(g) &= \begin{cases} 1 & g = a \\ -1 & g = b \end{cases} \\ \lambda_2 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_2(g) &= \begin{cases} -1 & g = a \\ 1 & g = b \end{cases} \\ \lambda_3 : D_n &\rightarrow GL_1(\mathbb{C}) & \lambda_3(g) &= \begin{cases} -1 & g = a \\ -1 & g = b \end{cases} \\ \rho_i : D_n &\rightarrow GL_2(\mathbb{C}) & \rho_i(g) &= \begin{cases} \begin{pmatrix} \omega_n^i & 0 \\ 0 & \omega_n^{-i} \end{pmatrix} & g = a \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & g = b. \end{cases} \end{aligned}$$

Notice the 2-dimensional representations ρ_i are well-defined for $1 \leq i \leq n$, but to obtain a complete set of irreducible 2-dimensional representations one needs to restrict to $1 \leq i \leq \lfloor \frac{n-1}{2} \rfloor$.

A subset A of \mathbb{Z}_n is called *admissible* if $|\sum_{a \in A} \omega_n^{ak}|$ is an integer, for every k such that $1 \leq k < n$. A subset $T = \{ba^i \mid i \in \hat{T}\}$ of reflections in D_n , is called *admissible* if \hat{T} is an admissible subset of \mathbb{Z}_n .

Theorem 3.5.1. *Cay(D_n, S) is integral if and only if $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$ and S_{ref} is an admissible set of reflections.*

Proof. We notice that by Theorem 3.1.3, integrality of $\text{Cay}(D_n, S)$ is equivalent to ρ -integrality of S . If S is ρ -integral, then it is χ -integral as well. If $S_{rot} \subseteq \{1\}$, then $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$. Thus, suppose $a^i \in S_{rot}$, where $1 \leq i \leq n$. Since S is a symmetric subset, we have $\text{cl}(a^i) = \{a^i, a^{-i}\} \subseteq S_{rot}$. Theorem 3.2.7 implies that $[a^i] \subseteq S_{rot}$. Therefore, S_{rot} is a union of atoms of $\mathbb{B}(\mathcal{G}_{C_n})$, and so it belongs to $\mathbb{B}(\mathcal{G}_{C_n})$. If we invoke to the 2-dimensional representations ρ_k (for $1 \leq k < n$), then $|\sum_{i \in \hat{S}_{ref}} \omega_n^{ik}|$ should be integer. This implies that S_{ref} is an admissible set of reflections. Conversely, suppose $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$, and S_{ref} is an admissible set of reflections. By Theorem 2.4.4, $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$ implies that $\lambda(S)$ is integer for any linear representation λ of D_n . We have $\rho_k(S) = \begin{pmatrix} u & \bar{v} \\ v & \bar{u} \end{pmatrix}$, where $u = \sum_{i \in \hat{S}_{rot}} \omega_n^{ik}$ and $v = \sum_{i \in \hat{S}_{ref}} \omega_n^{ik}$. Since $S_{rot} \in \mathbb{B}(\mathcal{G}_{C_n})$, we have $u \in \mathbb{Z}$. We may write $\rho_k(S)$ as:

$$\rho_k(S) = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} + \begin{pmatrix} 0 & \bar{v} \\ v & 0 \end{pmatrix} = uI + \begin{pmatrix} 0 & \bar{v} \\ v & 0 \end{pmatrix}.$$

This implies that $\rho_k(S)$ is integral if and only if $\begin{pmatrix} 0 & \bar{v} \\ v & 0 \end{pmatrix}$ is integral. The eigenvalues of $\begin{pmatrix} 0 & \bar{v} \\ v & 0 \end{pmatrix}$ are $\pm|v|$. Since S_{ref} is an admissible set $|v|$ is an integer, and therefore $\rho_k(S)$ is integral for $1 \leq k < n$. This completes the proof. \square

When n is a given small number, this theorem provides a good tool to decide about integrality of $\text{Cay}(D_n, S)$. However in the general case, it does not give us an easy explicit criterion to decide if $\text{Cay}(D_n, S)$ is integral or not. Clearly, one needs to classify all admissible subsets of reflections to be able to reach at such a criterion. We will see in the reminder, this is possible when n is a prime number and quite a challenging problem in general.

3.5.2 The case D_p where p is a prime number

In the reminder of this chapter, we assume S is a symmetric generating set of D_n , and S_{ref} will denote the set of all reflections in S . We will need the following results.

Theorem 3.5.2. (Kronecker) *Let $\alpha \neq 0$ be an algebraic integer. If α is not a root of unity, then at least one of conjugates of α has absolute value strictly greater than 1.*

Corollary 3.5.3. *Let τ be any root of unity and $\alpha \in \mathbb{Q}[\tau]$ with $|\alpha| = 1$. Then, α is a root of unity.*

Lemma 3.5.4. *Suppose S_{ref} is an admissible set, $\hat{S}_{ref} = \{i \mid ba^i \in S_{ref}\}$ and $|\sum_{i \in \hat{S}_{ref}} \omega_n^i| = c$, where c is an integer. If $\gcd(j, n) = 1$, then we have $|\sum_{i \in \hat{S}_{ref}} \omega_n^{ij}| = c$.*

Proof. Since $\gcd(j, n) = 1$, $\sigma_j(\omega_n) = \omega_n^j$ determines an automorphism σ_j in the $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega_n))$. Complex conjugation is in the center of the Galois extension $\mathbb{Q}(\omega_n)$ of \mathbb{Q} . It follows that complex conjugation preserves absolute values. If σ is in $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\omega_n))$, then we have $|z^\sigma| = |z|^\sigma$, where $z \in \mathbb{Q}(\omega_n)$. Then, applying σ_j , we get:

$$c = \sigma_j(c) = \sigma_j\left(|\sum_{i \in \hat{S}_{ref}} \omega_n^i|\right) = |\sigma_j(\sum_{i \in \hat{S}_{ref}} \omega_n^i)| = |\sum_{i \in \hat{S}_{ref}} \sigma_j(\omega_n^i)| = |\sum_{i \in \hat{S}_{ref}} \omega_n^{ij}|.$$

□

Let $P(z) = \sum_{i \in \hat{S}_{ref}} z^i \in \mathbb{Z}[z]$. Suppose $|\sum_{i \in \hat{S}_{ref}} \omega_n^i| = c$, where c is an integer. If $Q(z) = z^n(P(z)P(1/z) - c^2)$, then $Q(z) \in \mathbb{Z}[z]$. By Lemma 3.5.4, $Q(\alpha) = 0$ where α is an arbitrary primitive n -th root of unity. This implies that,

$$P(z)P(1/z) = c^2 + \Phi_n(z)q(z, 1/z).$$

where $\Phi_n(z)$ is the n -th cyclotomic polynomial and q has integer coefficients. Therefore

$$P(1)^2 = c^2 + \Phi_n(1)k \quad \Rightarrow \quad \Phi_n(1) \mid P(1)^2 - c^2.$$

We notice that $P(1) = |S_{ref}|$.

Theorem 3.5.5. *Let p be a prime and S a symmetric generating set in D_p . Then, $\text{Cay}(D_p, S)$ is integral if and only if $S_{rot} \in \mathbb{B}(C_p)$ and S_{ref} is a set of reflections of size 1, $p-1$ or p .*

Proof. The case $p = 2$ is obvious, hence in the reminder we assume that p is an odd prime. Notice that $S_{ref} \neq \emptyset$, because any generating set of D_p needs at least one reflection. By Theorem 3.5.1, we just need to show that any non-empty admissible set of reflections in D_p is of size 1, $p - 1$ or p .

Let $|\sum_{i \in \hat{S}_{ref}} \omega_p^i| = c$, where c is an integer, and $P(z) = \sum_{i \in \hat{S}_{ref}} z^i$. We have $P(1)^2 = |S_{ref}|^2 = c^2 + \Phi_p(1)k$, where k is an integer. For a prime p , we have $\Phi_p(z) = \sum_{k=0}^{p-1} z^k$, which implies that $\Phi_p(1) = p$. Notice that $c = |\sum_{i \in \hat{S}_{ref}} \omega_p^i| \leq \sum_{i \in \hat{S}_{ref}} |\omega_p^i| = |S_{ref}|$, with equality only if $|S_{ref}| = 1$.

If $k = 0$, then $c = |S_{ref}|$ and so $|S_{ref}| = 1$. Suppose now $k \neq 0$, then $p \mid |S_{ref}| - c$ or $p \mid |S_{ref}| + c$. We know $c < |S_{ref}| \leq p$, so if $p \mid |S_{ref}| - c$, then $c = 0$ and $|S_{ref}| = p$. In the case, $p \mid |S_{ref}| + c$, and $c \neq 0$ we will have $p = |S_{ref}| + c$.

From $|\sum_{i \in \hat{S}_{ref}} \omega_p^i| = c$, we have,

$$\left(\sum_{i \in \hat{S}_{ref}} \omega_p^i \right) \left(\sum_{i \in \hat{S}_{ref}} \omega_p^{-i} \right) = c^2.$$

If we define $d_i = |\{(m, n) \in \hat{S}_{ref}^2 \mid m - n \equiv i \pmod{p}\}|$ then we have;

$$|\hat{S}_{ref}| + \sum_{1 \leq i < p} d_i \omega_p^i = c^2.$$

Notice that, $\sum_{i=1}^{p-1} \omega_p^i = -1$. Since $|\hat{S}_{ref}| = |S_{ref}|$ and d_i should all be equal to a common value d , we have following set of equations:

- $p = |S_{ref}| + c$
- $(p - 1)d = |S_{ref}|^2 - |S_{ref}|$
- $-d = c^2 - |S_{ref}|$

If we replace d in the middle equation with $|S_{ref}| - c^2$ obtained from the third equation, and $|S_{ref}|$ with $p - c$ from the first equation, then the second equation becomes:

$$p(p - c) - (p - 1)c^2 = (p - c)^2.$$

Since p is an odd prime and $c < p$, this equation implies that $c = 0$ or $c = 1$, and by Kronecker's result this means that S_{ref} is a set of reflections of size $p, p - 1$ or 1. \square

3.5.3 The general case

In this section we consider dihedral group D_n , where n is a composite number. From previous section, immediately follows that we need to find all admissible subsets of \mathbb{Z}_n to characterize all ρ -integral subsets of D_n . That is to say, we need to characterize all subsets T of \mathbb{Z}_n such that the following is true:

$$\left| \sum_{t \in T} \omega_n^{tk} \right| \in \mathbb{Z}. \quad (3.16)$$

where ω_n is a primitive n -th root of unity, and $1 \leq k < n$. In the previous section, we proved that in \mathbb{Z}_p this happens if and only if $|T| \in \{0, 1, p-1, p\}$. If $T \in \mathbb{B}(\mathcal{G}_{\mathbb{Z}_n})$, then T is admissible. This is because $\sum_{t \in T} \omega_n^{tk}$ is an integer if and only if $T \in \mathbb{B}(\mathcal{G}_{\mathbb{Z}_n})$. If T is a subset of \mathbb{Z}_n such that $|T| \in \{1, n-1\}$, then T is admissible as well. An admissible subset T of \mathbb{Z}_n is called a *trivial admissible set* if $T \in \mathbb{B}(\mathcal{G}_{\mathbb{Z}_n})$ or $|T| \in \{1, n-1\}$. A primitive guess is that every admissible set in \mathbb{Z}_n is of trivial kind. Following example provides a counter-example to this primitive guess.

Example 3.5.1. If $T = \{1, 2, 3\}$ and $0 \leq k < 6$, then $\left| \sum_{t \in T} \omega_6^{tk} \right| \in \mathbb{Z}$. Therefore T is a non-trivial admissible set in \mathbb{Z}_6 .

Proof. The absolute value of $\omega_6 + \omega_6^2 + \omega_6^3$ is 2. The atoms of $\mathbb{B}(\mathcal{G}_{\mathbb{Z}_6})$ containing elements of T are; $[1] = \{1, 5\}$, $[2] = \{2, 4\}$ and $[3] = \{3\}$. Clearly T is not a union of atoms of $\mathbb{B}(\mathcal{G}_{\mathbb{Z}_6})$, and thus it is not in $\mathbb{B}(\mathcal{G}_{\mathbb{Z}_6})$. Therefore T is a non-trivial admissible set in \mathbb{Z}_6 . \square

In general, the problem of determining admissible sets in \mathbb{Z}_n is quite difficult. Indeed this problem is related to a famous open conjecture known as Circulant Hadamard Matrix Conjecture 3.5.7 given in the sequel.

Theorem 3.5.6. *If $n \geq 4$, then $\mathcal{I}_\rho^{\mathcal{D}_n}$ is not a boolean algebra.*

Proof. According to Theorem 3.2.8, part 8, each atom of $\mathbb{B}(D_n)$ is ρ -integral. We need to prove that $\mathbb{B}(D_n) \not\subseteq \mathcal{I}_\rho^{\mathcal{D}_n}$. Since each reflection is of order 2, thus any subset of reflections is in the boolean algebra of subgroups. Suppose $S = \{b, ba\}$. We have,

$$\rho_1(S) = \rho_1(b) + \rho_1(ba) = \begin{pmatrix} 0 & 1 + \omega_n \\ 1 + \bar{\omega}_n & 0 \end{pmatrix}.$$

The eigenvalues of this matrix are $\pm\lambda$, where $\lambda = |1 + \omega_n|$. We have $|1 + \omega_n| = \sqrt{2(1 + \cos(\frac{2\pi}{n}))}$, which is an integer only if $n = 2, 3$. Therefore, for $n \geq 4$, $\mathcal{I}_\rho^{\mathcal{D}_n}$ is not a boolean algebra. \square

An $n \times n$ matrix H is a Hadamard matrix if its entries are ± 1 and its rows are orthogonal. Equivalently, its entries are ± 1 and $HH^t = nI$. An $n \times n$ matrix H is *circulant* if each row is a cyclic shift of the previous row. Equivalently, $H = (h_{i-j})$, for some h_0, h_1, \dots, h_{n-1} , where indices $i - j$ are taken modulo n . The column vector $\mathbf{w}_j = (1, \omega^j, \omega^{2j}, \dots, \omega^{(n-1)j})^t$ for $0 \leq j < n$ is an eigenvector of the circulant matrix H , with the corresponding eigenvalue $\sum_{0 \leq i < n} h_i \omega^{ij}$.

Conjecture 3.5.7. *There does not exist a circulant Hadamard matrix of order $n > 4$.*

A circulant Hadamard matrix of order n could exist only if n is a square of an even integer ([57]). The circulant Hadamard matrix is uniquely determined by the positions of the $+1$ entries in the first row. Let us denote the set of positions of $+1$ in the first row by T . Since $\sum_{0 \leq i < n} \omega^i = 0$, and $HH^t = nI$, we have,

$$4\left(\sum_{t \in T} \omega^{tj}\right) \cdot \left(\sum_{t \in T} \omega^{-tj}\right) = 4\left|\sum_{t \in T} \omega^{tj}\right|^2 = n.$$

This proves that $|\sum_{t \in T} \omega^{tj}|$ should be an integer for every choice of j (notice that n is a square of an even integer). This suggests that the positions of $+1$ in the first row of a circulant Hadamard matrix should form an admissible subset of \mathbb{Z}_n . Therefore, any classification of admissible subsets of \mathbb{Z}_n will definitely be a push towards a finale of the circulant Hadamard matrix conjecture. This is the main theme of the algebraic approach towards the circulant Hadamard conjecture. This idea has recently been used as *field descent method* (see [39, 40]) to rule out many open cases of the circulant Hadamard matrix conjecture.

A *Weil number* is a complex number, all of its conjugates (over \mathbb{Q}) have the same absolute value. A *d-Weil integer* is a Weil number that is also an algebraic integer with absolute value equal to $d^{\frac{1}{2}}$. One may ask if every Weil number of absolute value 1 is necessarily a root of unity. However, this is false. For example, the roots of the polynomial $x^2 + \frac{x}{2} + 1$ are Weil numbers of absolute value 1. Though, they are not roots of unity. Kronecker Theorem implies that every Weil integer with absolute value 1 is a root of unity. There is no classification of d -Weil integers (see [27, 46]). It is clear that integrality of Cayley graphs over D_n is essentially a special case of classification of d^2 -Weil integers.

Chapter 4

CIS and Cayley integral groups

In this chapter, we solve two open problems regarding the classification of certain classes of Cayley graphs with integer eigenvalues. We first classify all finite groups that have a “non-trivial” Cayley graph with integer eigenvalues, thus solving a problem proposed by Abdollahi and Jazaeri. The notion of Cayley integral groups was introduced by Klotz and Sander. These are groups for which every Cayley graph has only integer eigenvalues. In the second part of this chapter, all Cayley integral groups are determined.

4.1 Introduction

The notion of CIS groups as groups admitting no integral Cayley graphs besides complete multipartite graphs, has been introduced by Abdollahi and Jazaeri [1], who classified all abelian CIS groups. The question which non-abelian groups are CIS remained open. A similar but more intriguing notion of Cayley integral groups was introduced by Klotz and Sander in [38], where the abelian group case has been resolved, while the general case was left open. The main results in this chapter are Theorems 4.2.2 and 4.3.2 in which we classify all CIS groups and all Cayley integral groups. The first of these two results interestingly shows that every finite non-abelian group admits a non-trivial Cayley graph whose eigenvalues are all integral. We first present some preliminary results which we will use in the rest of this chapter. A subgroup H of G is *central* if it lies inside the center of the group, i.e $H \subseteq Z(G)$.

Lemma 4.1.1. *Suppose H is a central normal subgroup of a group G . If G/H is cyclic, then G is an abelian group.*

Proof. Suppose $G/H = \langle Hx \rangle$. If $g_1, g_2 \in G$, then there are integers m and n such that $Hg_1 = Hx^m$ and $Hg_2 = Hx^n$. Thus, there exist $h_1 \in H$ and $h_2 \in H$ such that $g_1 = h_1x^m$ and $g_2 = h_2x^n$. Notice that $h_1, h_2 \in Z(G)$ (since H is central). We have;

$$g_1g_2 = (h_1x^m)(h_2x^n) = h_1h_2x^{m+n} = (h_2x^n)(h_1x^m) = g_2g_1.$$

□

Lemma 4.1.2. *Suppose G is a p -group, where p is a prime number. If N is a normal subgroup of G , then $N \cap Z(G) \neq 1$.*

Thus, the center of any p -group is non-trivial. We often use this fact without mentioning it.

Theorem 4.1.3 (Miller and Moreno [42]). *Let G be a non-abelian group with the property that every proper subgroup is abelian. Then $|G|$ has at most two prime divisors and there is some prime p dividing the order of G such that the Sylow p -subgroup of G is normal.*

If H is a subgroup of G , then G is a disjoint union of left (right) cosets of H . Suppose $G = \bigcup_{i=1}^k a_iH$, where $\{a_iH \mid 1 \leq i \leq k\}$ is a distinct set of left cosets of H in G . In this case, $\{a_i \mid 1 \leq i \leq k\}$ is called a *left transversal* of H in G . Right transversal is defined in the same way using a partition to right cosets. In general a left transversal is not a right transversal or vice versa, however for finite groups there is an interesting result:

Theorem 4.1.4. *Let H be a subgroup of a finite group G . There is a left transversal of H in G which is a right transversal as well.*

Every where in this chapter, when we pick a random transversal of a subgroup H of a finite group G , we are assuming that it is a two sided transversal. Thus we refer to it as a “transversal” of H in G .

Let N and H be groups, and $\theta : H \rightarrow \text{Aut}(N)$ be a group homomorphism. The *external semi-direct product* $N \rtimes_{\theta} H$ (or simply $N \rtimes H$ when θ is understood) of N and H with respect to θ is the group $(N \times H; \bullet)$ with $(n_1, h_1) \bullet (n_2, h_2) = (n_1\theta_{h_1}(n_2), h_1h_2)$. The identity element of $N \rtimes_{\theta} H$ is $(1_N, 1_H)$, and the inverse of $(n, h) = (\theta_{h^{-1}}(n^{-1}), h^{-1})$.

Regarding N and H as subgroups of $N \rtimes H$ via the canonical monomorphisms $\iota_N(n) = (n, 1_H)$, and $\iota_H(h) = (1_N, h)$. We have the following properties:

Proposition 4.1.1. Let $G = N \rtimes H$. Then:

- N is a normal subgroup of G .
- $G = NH$.
- $N \cap H = 1$ and $G/N \cong H$.

Let G be a group with subgroups N and H . We say that G is the *internal semi-direct product* of N and H if;

- N is a normal subgroup of G .
- $G = NH$.
- $N \cap H = 1$.

If G is the internal semi-direct product of N and H , then $G \cong N \rtimes_{\theta} H$ via the homomorphism $\theta : H \rightarrow \text{Aut}(N)$ given by $\theta_h(n) = h^{-1}nh$.

Proposition 4.1.2. If G is a group with a normal subgroup N such that $G/N \cong H$, then there exists a homomorphism $\theta : H \rightarrow \text{Aut}(N)$, such that $G = N \rtimes_{\theta} H$.

4.2 Cayley integral simple groups

In this section, we answer a question of Abdollahi and Jazaeri [1] concerning Cayley integral simple groups. Abdollahi and Jazaeri defined a *Cayley integral simple* group (CIS group for short) to be a group G with the property that the only connected integral Cayley graphs of G are complete multipartite graphs. In addition to this, they noticed that given a symmetric generating subset S of G , $\text{Cay}(G, S)$ is a complete multipartite graph if and only if S is the complement of a subgroup of G . Thus a simpler definition of a CIS group is that it is a group G with the property that for a symmetric generating set S of G , we have that $\text{Cay}(G, S)$ is an integral graph if and only if S is the complement of a subgroup of G .

As part of their study of CIS groups, Abdollahi and Jazaeri gave a complete characterization of abelian CIS groups, which we state now.

Theorem 4.2.1 (Abdollahi and Jazaeri [1]). *Let G be an abelian group. Then G is a CIS group if and only if $G \cong \mathbb{Z}_{p^2}, \mathbb{Z}_p$ for some prime number p , or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

In addition to this, they posed the following question.

Question 1. Which finite non-abelian groups are CIS groups?

We answer their question with the perhaps surprising answer that non-abelian finite CIS groups do not exist. More formally, we show the following result.

Theorem 4.2.2. *Let G be a CIS group. Then G is abelian and in particular is isomorphic to either a cyclic group of order p or p^2 for some prime p , or is isomorphic to \mathbb{Z}_2^2 .*

Our proof of Theorem 4.2.2 is essentially an induction argument on the order of the group.

Theorem 4.2.3. *Let G be a finite group and S a symmetric generating set of G such that $1 \notin S$. Then $G \setminus S$ is a subgroup of G if and only if $\text{Cay}(G, S)$ is a complete multipartite graph. In particular a complete multipartite Cayley graph has equal number of vertices in each partition and is integral*

Proof. Suppose that $H = G \setminus S$ is a subgroup of G . Let $\{a_1, a_2, \dots, a_k\}$ be a transversal of H in G , where $k = [G : H]$. We know that $a_j a_i^{-1} \in H$ if and only if $i \neq j$. Clearly, this implies that $\text{Cay}(G, S)$ is a multipartite graph with parts $\{a_i H \mid 1 \leq i \leq k\}$. Notice that each part is of size $|H|$, and thus $\text{Cay}(G, S)$ is integral. Conversely, suppose that $\text{Cay}(G, S)$ is a complete multipartite graph. Since Cayley graphs are regular, each partition of $\text{Cay}(G, S)$ has equal size. Let $1 \neq g \in G \setminus S$. Then $g \not\sim 1$ in $\text{Cay}(G, S)$, because $g = g1^{-1} \notin S$. Therefore g and 1 belong to one partition of $\text{Cay}(G, S)$. Thus, all elements outside of S belong to the same partition (the partition that 1 belongs to) and so there is no edge between them. Therefore, if $g_1, g_2 \in G \setminus S$, then $g_1 g_2^{-1} \notin S$. This implies that $G \setminus S$ is a subgroup of G . \square

We now show that the CIS property is closed under the process of taking subgroups and homomorphic images.

Lemma 4.2.4. *Let G be a CIS group. Then every subgroup and every homomorphic image of G is also a CIS group.*

Proof. Suppose H is a subgroup of G . We will show that H is a CIS group. Suppose, towards a contradiction, that H is not a CIS group. Then there is a symmetric generating subset S of H such that $1 \notin S$, $H \setminus S$ is not a subgroup of H , and such that $\text{Cay}(H, S)$ is an integral graph. We take $T = S \cup (G \setminus H)$. Then T generates G , $1 \notin T$, and $G \setminus T = H \setminus S$ is not a subgroup

of G . Then the adjacency matrix of $\text{Cay}(G, T)$ is given by $B := A_S \otimes I_k + J_n \otimes (J_k - I_k)$, where A_S is the adjacency matrix of $\text{Cay}(H, S)$, $n = |H|$, $k = [G : H]$. Since A_S is Hermitian, it is unitarily diagonalizable. In particular, we can find an orthogonal basis of eigenvectors of A_S , $\{\mathbf{w}_1, \dots, \mathbf{w}_n\}$. We may assume that $\mathbf{w}_1 = \mathbf{j}$, the vector whose coordinates are all equal to one. Thus there are integers $|\lambda_i| = \lambda_1, \dots, \lambda_n$ such that $A_S \mathbf{w}_i = \lambda_i \mathbf{w}_i$ for $i = 1, \dots, n$. Notice that since J_n has each of its columns equal to $\mathbf{j} = \mathbf{w}_1$, we have $J_n \mathbf{w}_1 = n \mathbf{w}_1$ and $J_n \mathbf{w}_i = 0$ for $i \geq 2$. Since J_k is symmetric and of rank 1, it has eigenvectors $\mathbf{u}_1, \dots, \mathbf{u}_k$ with $J_k \mathbf{u}_i = k \delta_{1,i} \mathbf{u}_i$. Then $\mathcal{S} = \{\mathbf{w}_i \otimes \mathbf{u}_j \mid 1 \leq i \leq n, 1 \leq j \leq k\}$ is a basis of $\mathbb{C}^n \otimes \mathbb{C}^k$. Observe that $B(\mathbf{w}_i \otimes \mathbf{u}_j) = (\lambda_i + \delta_{1,i} n(k \delta_{1,j} - 1)) \mathbf{w}_i \otimes \mathbf{u}_j$. In particular, \mathcal{S} is a complete set of eigenvectors of B and thus every eigenvalue of B is an integer. Thus G is not a CIS group, a contradiction.

For the second part, suppose N is a proper normal subgroup of G . We show, using a proof by contradiction, that G/N is a CIS group. If G/N is not a CIS group, then there exists a symmetric generating subset \bar{S} of G/N such that $N \notin \bar{S}$, $G/N \setminus \bar{S}$ is not a subgroup of G/N and $\text{Cay}(G/N, \bar{S})$ is an integral graph. Suppose $\bar{S} = \{Ns \mid s \in S\}$, where the set S is symmetric in G . We have $S \cap N = \emptyset$. If we define $T = \cup_{s \in S} Ns$, then clearly T is a symmetric subset of G such that $1 \notin T$. Since $G/N \setminus \bar{S}$ is not a subgroup of G/N , there are g_1 and g_2 in G such that Ng_1 and Ng_2 do not belong to \bar{S} but $Ng_1g_2 \in \bar{S}$. Thus, we get $g_1g_2 \in T$ and $\{g_1, g_2\} \cap T = \emptyset$. This proves that $G \setminus T$ is not a subgroup of G . It is easy to see that the adjacency matrix of $\text{Cay}(G, T)$ is $J_k \otimes A_{G/N}$, where $k = |N|$ and $A_{G/N}$ is the adjacency matrix of $\text{Cay}(G/N, \bar{S})$. Since J_k has eigenvalues 0 with multiplicity $k - 1$ and k with multiplicity 1, we deduce that $\text{Cay}(G, T)$ is an integral graph and thus G is not a CIS group which contradicts our assumption. Therefore, G/N is a CIS group. \square

For the sake of completeness, we present a rather short proof of Theorem 4.2.1 based on above result.

Proof of Theorem 4.2.1. Suppose p is a prime. The boolean algebra of \mathbb{Z}_p contains two atoms $[0] = \{0\}$ and $[1] = \mathbb{Z}_p \setminus \{0\}$. Clearly the only connected integral Cayley graph over \mathbb{Z}_p is $\text{Cay}(\mathbb{Z}_p, [1])$, thus \mathbb{Z}_p is a CIS group. The boolean algebra of \mathbb{Z}_{p^2} contains atoms $[0] = \{0\}$, $[p] = \{pk \mid 1 \leq k < p\}$ and $[1] = \mathbb{Z}_p \setminus \{pk \mid 0 \leq k < p\}$. In this case, $S = [1]$ or $S = [1] \cup [p]$ are the only symmetric generating sets avoiding the identity which generate integral graphs. Both are the complement of subgroups of \mathbb{Z}_{p^2} , thus \mathbb{Z}_{p^2} is a CIS group as well. In $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\{(1, 0), (0, 1), (1, 1)\}$, $\{(1, 0), (0, 1)\}$, $\{(1, 0), (1, 1)\}$, $\{(1, 1), (0, 1)\}$ are the only generating sets

which are a union of atoms of the boolean algebra. All these sets are the complement of subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$, therefore $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a CIS group as well. To prove that there are no other abelian CIS groups, suppose that G is an abelian CIS group of minimum order that is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, \mathbb{Z}_{p^2} or \mathbb{Z}_p .

Suppose first that $G = A \times \mathbb{Z}_m$, where $m > 2$ and $|A| \geq 2$. Let $S_1 = A \setminus \{0\}$, $S_2 = \mathbb{Z}_m \setminus \{0\}$ and $S = S_1 \cup S_2$. We notice that the Cayley graph $\text{Cay}(G, S)$ is isomorphic to the Cartesian product $\text{Cay}(A, S_1) \square \text{Cay}(\mathbb{Z}_m, S_2)$. Since $\text{Cay}(A, S_1)$ and $\text{Cay}(\mathbb{Z}_m, S_2)$ are complete graphs and therefore integral, their Cartesian product $\text{Cay}(G, S)$ is also integral. Since $G \setminus S$ is not a subgroup of G , we conclude that G is not a CIS group.

Since every abelian group is a direct product of cyclic subgroups whose orders are powers of primes, we conclude from the above that G is either isomorphic to \mathbb{Z}_{p^n} or to \mathbb{Z}_2^n for some $n > 2$. Since subgroup of CIS groups are CIS, and since \mathbb{Z}_{p^n} (\mathbb{Z}_2^n) contains $\mathbb{Z}_{p^{n-1}}$ (\mathbb{Z}_2^{n-1}) as a subgroup, we may assume that $n = 3$. However, \mathbb{Z}_{p^3} and \mathbb{Z}_2^3 are not CIS as evidenced by the following generating sets. For \mathbb{Z}_2^3 we take $S = \{(0, 0, 1), (0, 1, 0), (1, 0, 0)\}$ whose Cayley graph is the 3-cube having only integral eigenvalues. For $\mathbb{Z}_{p^3} = \langle a \mid a^{p^3} = 1 \rangle$, we let $Y = \{a^{tp} \mid t = 0, 1, \dots, p^2 - 1\}$ and $Z = \{a^{tp^2} \mid t = 0, 1, \dots, p - 1\}$. Now, take $S = \mathbb{Z}_{p^3} \setminus (Y \setminus Z)$ whose complement contains a^p but not a^{p^2} , and is therefore not a subgroup. The corresponding Cayley graph is easily seen to be integral. This completes the proof. \square

Our inductive proof of Theorem 4.2.2 requires considering a few base cases, which are covered by the following lemma.

Lemma 4.2.5. *Suppose that G is one of the following groups: D_4 , Q_8 , A_4 , or a non-abelian semi-direct product of two cyclic groups of prime order. Then G is not a CIS group.*

Proof. We write $D_4 = \langle x, y \mid x^4 = y^2 = 1, yxy = x^{-1} \rangle$. Then $S = \{x, x^3, y\}$ is a symmetric generating set whose complement is not a subgroup of D_4 . The Cayley graph $\text{Cay}(D_4, S)$ is isomorphic to the graph of the 3-cube which is integral. Thus D_4 is not a CIS group.

Let us now consider the group of quaternions, $Q_8 = \{\pm i, \pm j, \pm k, \pm 1\}$. We let $S = \{\pm i, \pm j, -1\}$. Then S is a symmetric generating set and its complement is not a subgroup. If θ is the element of the group algebra of Q_8 corresponding to S then θ is sent to $-I$ in the irreducible 2-dimensional representation of Q_8 ; in the one-dimensional representations it is sent to an element in $\{-3, 1, 5\}$. This implies that $\text{Cay}(Q_8, S)$ is integral, and that Q_8 is not a CIS group.

We next consider A_4 . We take $S = \{(12)(34), (123), (132), (124), (142), (234), (243), (134), (143)\} \subseteq A_4$. The complement is not a subgroup since $(13)(24)$ and $(14)(23)$ are in the complement and their product is in S . Let θ denote the element

$$(12)(34) + (123) + (132) + (124) + (142) + (234) + (243) + (134) + (143)$$

of the group algebra of A_4 corresponding to S . Since the sum of all three-cycles, which we call z , is central in A_4 , we have that $\rho(z)$ is a scalar multiple of the identity for every irreducible representation ρ of A_4 . Since all characters of A_4 are integer-valued, we see that $\rho(z)$ must be an integral multiple of the identity. Thus $\rho(\theta)$ has eigenvalues equal to the eigenvalues of $\rho((12)(34))$ shifted by an integer. The eigenvalues of $\rho((12)(34))$ are in $\{\pm 1\}$, since $(12)(34)$ has order 2. This shows that all eigenvalues of $\rho(\theta)$ are integers. Thus A_4 is not a CIS group.

Finally, let G be a non-abelian semidirect product of two groups of prime order. Since every semidirect product of \mathbb{Z}_p with \mathbb{Z}_p and every semidirect product of \mathbb{Z}_2 with \mathbb{Z}_p is abelian, we may assume that $G = \langle x \mid x^p = 1 \rangle \rtimes \langle y \mid y^q = 1 \rangle$, where $2 < p < q$ are distinct primes. Let $S = \{x, x^2, \dots, x^{p-1}, y, y^2, \dots, y^{q-1}\}$. Then S is symmetric and generates G . Since $p > 2$, $|G \setminus S| = pq - p - q + 2$ does not divide pq , thus $G \setminus S$ is not a group. Notice that the element $z = x + x^2 + \dots + x^{p-1}$ is central in the group algebra of G . It follows that if ϕ is any irreducible representation of G then $\phi(z)$ is a scalar multiple of the identity. In fact, since x has order p , all of the eigenvalues of $\phi(x)$ are p -th roots of unity and hence $\phi(z) = (p-1)I$ (if $\phi(x) = 1$), or $\phi(z) = -I$ (when $\phi(x) \neq 1$). Thus, $\phi(z)$ has eigenvalues in $\{-1, p-1\}$. Similarly, since the eigenvalues of $\phi(y)$ are q -th roots of unity, we conclude that $\phi(y) + \phi(y^2) + \dots + \phi(y^{q-1})$ has eigenvalues in $\{-1, q-1\}$. Thus $z + y + \dots + y^{q-1}$ has eigenvalues in $\{-2, q-2, p-2, p+q-2\}$. This implies that $\text{Cay}(G, S)$ is an integral graph. Thus G is not a CIS group. \square

Proof of Theorem 4.2.2. Suppose, towards a contradiction, that there exists a non-abelian CIS group. We pick such a CIS group G of minimum order. By Lemma 4.2.4, every subgroup of G is a CIS group. Thus, by minimality of G , we have that G is a non-abelian group with the property that every proper subgroup of G is abelian.

By Theorem 4.1.3, G is either a p -group or there exist distinct primes p and q such that $|G| = p^a q^b$ for some positive integers a and b and the Sylow p -subgroup of G is normal. We consider these cases separately.

Case I. G is a p -group.

Suppose that $|G| = p^k$. Since G is non-abelian, we have $k \geq 3$. Let us first assume that $k = 3$. Every p -group has a non-trivial center. Since G is not abelian, $G/Z(G)$ can not be cyclic. This implies that $|Z(G)| = p$ and $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. If G is a CIS group, then $\mathbb{Z}_p \times \mathbb{Z}_p$ should be a CIS group as well (Lemma 4.2.4). Thus by Theorem 4.2.1 we have $p = 2$. Thus $G \cong Q_8$ or D_4 , but according to Lemma 4.2.5, Q_8 and D_4 are not CIS groups. Thus no p -group of order p^3 is a CIS group. If G is a non-abelian p -group of order greater than p^3 then G has a subgroup of order p^3 and thus it is not a CIS group.

Case II. G has order $p^a q^b$, where p and q are distinct primes, $a, b \geq 1$, and G has a normal Sylow p -subgroup.

In this case the Sylow p - and Sylow q -subgroups are proper and hence must be abelian by the minimality assumption on the order of G . Let P and Q denote the Sylow p - and the Sylow q -subgroup of G , respectively. Then $G \cong P \rtimes Q$. We consider the case that $p = 2$ and $p \neq 2$ separately.

Subcase I: p is odd.

Since P is an abelian CIS group, we have $P \cong \mathbb{Z}_p$ or $P \cong \mathbb{Z}_{p^2}$. Since \mathbb{Z}_{p^2} has a characteristic subgroup of size p we see that G has a subgroup that is isomorphic to $\mathbb{Z}_p \rtimes Q$. Also, Q has a subgroup isomorphic to \mathbb{Z}_q and since this normalizes the copy of \mathbb{Z}_p we see that G has a subgroup isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_q$. Since there are no abelian CIS groups of order pq we see that $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ is non-abelian and so by minimality of G we have $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$. Since G is non-abelian we have the result from Lemma 4.2.5.

Subcase II: $p = 2$.

In this case, $|P| \in \{2, 4\}$. If P is cyclic then P has a characteristic subgroup isomorphic to \mathbb{Z}_2 and thus G contains a copy of $\mathbb{Z}_2 \rtimes Q$. Notice that \mathbb{Z}_2 has only the trivial automorphism and so $\mathbb{Z}_2 \rtimes Q \cong \mathbb{Z}_2 \times Q$, which is not a CIS group since all abelian CIS groups have order a power of a prime. Thus $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Notice that $\text{Aut}(P) \cong \mathbb{Z}_3$ and so $P \rtimes Q$ is abelian unless $q = 3$. Since G is non-abelian, we conclude that $q = 3$ and that $Q \cong \mathbb{Z}_3$ or \mathbb{Z}_9 . Notice that in either case, Q has a subgroup of size 3 that normalizes P and so G contains a subgroup isomorphic to $(\mathbb{Z}_2)^2 \rtimes \mathbb{Z}_3$. Since this group is necessarily a CIS group and since there are no abelian CIS groups of order 12, we see that $(\mathbb{Z}_2)^2 \rtimes \mathbb{Z}_3$ is a non-abelian semi-direct product

and hence isomorphic to A_4 . But A_4 is not a CIS group by Lemma 4.2.5 (iii). Thus we see that we cannot have $p = 2$.

We have obtained a contradiction in each case and so we conclude that every CIS group is abelian. \square

4.3 Cayley Integral Groups

Klotz and Sander [38] introduced the notion of a *Cayley integral group*. This is a group G with the property that for every symmetric subset S of G , $\text{Cay}(G, S)$ is an integral graph. One of their results was a characterization of abelian integral groups.

Theorem 4.3.1 (Klotz and Sander [38]). *The only abelian Cayley integral groups are*

$$\mathbb{Z}_2^n \times \mathbb{Z}_3^m, \text{ and } \mathbb{Z}_2^n \times \mathbb{Z}_4^m,$$

where m and n are arbitrary non-negative integers.

The main result of this section is a complete characterization of Cayley integral groups, which we now state.

Theorem 4.3.2. *The only Cayley integral groups are*

$$\mathbb{Z}_2^n \times \mathbb{Z}_3^m, \mathbb{Z}_2^n \times \mathbb{Z}_4^m, Q_8 \times \mathbb{Z}_2^n, S_3, \text{ and } \text{Dic}_{12},$$

where m, n are arbitrary non-negative integers, Q_8 is the quaternion group of order 8, and Dic_{12} is the dicyclic group of order 12.

We note that the dicyclic group of order 12 can be described as the non-abelian semi-direct product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$. One of the interesting features is that it has S_3 as a homomorphic image. We also point out that S_3 and Dic_{12} are the only non-nilpotent groups on the list.

Let us first describe some basic properties of Cayley integral groups.

Lemma 4.3.3. *Let G be a Cayley integral group. Then every subgroup and every homomorphic image of G is also Cayley integral.*

Proof. The claim for subgroups is obvious since for a subset S of a subgroup $H \leq G$, The Cayley graph $\text{Cay}(G, S)$ consists of $[G : H]$ copies of $\text{Cay}(H, S)$.

Next, suppose that K is a homomorphic image of G . Let $\pi : G \rightarrow K$ be a surjective homomorphism and let S be a symmetric subset of K . Let $T = \pi^{-1}(S)$. Then T is a symmetric subset of G . We let A_G denote the adjacency matrix of $\text{Cay}(G, T)$. Then $A_G = A_H \otimes J_k$, where A_H is the adjacency matrix of $\text{Cay}(H, S)$, $k = |G|/|K|$, and J_k is the $k \times k$ matrix with every entry equal to one. If \mathbf{w} is an eigenvector of A_H corresponding to an eigenvalue λ and if \mathbf{j} is the $k \times 1$ matrix whose entries are all 1, then $A_G(\mathbf{w} \otimes \mathbf{j}) = k\lambda(\mathbf{w} \otimes \mathbf{j})$. Since λ is an algebraic integer, it must indeed be an integer. This implies that K is a Cayley integral group. \square

Lemma 4.3.4. *Let G be a finite group. If G is a Cayley integral group and g is a non-identity element in G , then $\text{ord}(g) \in \{2, 3, 4, 6\}$.*

Proof. We notice that the only integral cycles are C_3, C_4 and C_6 . Thus, $\text{Cay}(\langle g \rangle, \{g, g^{-1}\})$ is not integral if $\text{ord}(g) \notin \{2, 3, 4, 6\}$. \square

Lemma 4.3.5. *Let G be a finite group and S a symmetric subset of G . If for every s in S , $\text{ord}(s) \in \{2, 3, 4, 6\}$, then $S \in \mathbb{B}(G)$.*

Proof. We show that for every s of order 2, 3, 4 or 6, we have $\{s, s^{-1}\} \in \mathbb{B}(G)$. Since S is a symmetric subset, thus this will implies $S \in \mathbb{B}(G)$. We notice that the atom containing s in $\mathbb{B}(G)$ is the set of generators of the cyclic group generated by s . If s is an element of order 2, then $[s] = \{s\}$. If s is an element of order 3, 4 or 6, then $[s] = \{s, s^{-1}\}$. Therefore in every case, we have $\{s, s^{-1}\} \in \mathbb{B}(G)$ and we are done. \square

Theorem 4.3.1 is an immediate consequence of these lemmas. We now show that the property of being Cayley integral is equivalent to a weaker property.

Proposition 4.3.1. A group G is Cayley integral if and only if every connected Cayley graph of G is integral.

Proof. One direction is obvious. Suppose now that every connected Cayley graph of G is integral, but there is a subset S of G such that $\text{Cay}(G, S)$ is not integral. Let $T = G \setminus (S \cup \{1\})$. Note that $\text{Cay}(G, S)$ is disconnected, thus its complementary graph, which is equal to $\text{Cay}(G, T)$ is connected. Thus, by the assumption, $\text{Cay}(G, T)$ is integral. It is well-known that the complement of a regular integral graph is also integral. This contradicts our assumption that $\text{Cay}(G, S)$ has non-integral eigenvalues. \square

We note that the only Cayley integral cyclic groups are \mathbb{Z}_m with $m \in \{1, 2, 3, 4, 6\}$. Thus if G is a Cayley integral group, then since subgroups of G are also Cayley integral, G can not have any elements of order p where p is a prime greater than 3. In particular, Cauchy's theorem gives that G is a $(2, 3)$ -group; i.e., the order of G is the product of a power of 2 and a power of 3. A theorem of Burnside then gives that G is necessarily a solvable group.

We summarize the important points obtained so far in the following remark.

Remark 4.3.6. *Let G be a group. Then:*

1. G is a Cayley integral group if and only if $\text{Cay}(G, S)$ is an integral graph for every symmetric generating sets S of G ;
2. if G is a Cayley integral group then so are subgroups and homomorphic images of G ;
3. if G is a Cayley integral group then its order is a product of a power of 2 and a power of 3 and all elements of G have order in $\{1, 2, 3, 4, 6\}$;
4. G is a solvable group.

We will make use of this remark often without referring to it directly.

We next give a result that will be used to characterize Cayley integral groups. It shows, roughly speaking, that if a group G has a symmetric generating set S such that $\text{Cay}(G, S)$ is an integral graph, then $|G|$ cannot be too large compared to $|S|$.

Proposition 4.3.2. *Let G be a finite group and let S be a symmetric generating set of G . If $\text{Cay}(G, S)$ is an integral Cayley graph, then the order of G divides $2(2|S| - 1)!$. If, in addition, G is perfect or S has an element of odd order, then $|G|$ divides $(2|S| - 1)!$.*

Proof. Let A_S denote the adjacency matrix of $\text{Cay}(G, S)$. For each group element $g \in G$, we let A_g denote the permutation matrix (associated with the left-regular representation of G) of g . We then have that $A_S = \sum_{s \in S} A_s$. Let $k = |S|$. Since S is a symmetric generating subset of G , $\text{Cay}(G, S)$ is a k -regular connected graph. Therefore all eigenvalues of A_S are in the set $\{-k, \dots, k-1, k\}$. A well-known consequence of the Perron-Frobenius Theorem is that the eigenspaces of the eigenvalues k and $-k$ are at most 1-dimensional since the graph is connected. Moreover, $-k$ is an eigenvalue if and only if the graph is bipartite. We now look at the cases corresponding to whether $\text{Cay}(G, S)$ is bipartite or not.

Case I. $\text{Cay}(G, S)$ is not bipartite.

In this case $-k$ is not an eigenvalue of A_S . Since A_S is a symmetric matrix, it is diagonalizable and therefore the minimal polynomial of A_S divides

$$(x - k) \prod_{i=-k+1}^{k-1} (x - i).$$

If we take $\Phi(x) = \prod_{i=-k+1}^{k-1} (x - i)$, then $B := \Phi(A_S)$ will be nonzero, since A_S has k as an eigenvalue. Let \mathbf{j} be the vector whose coordinates are all equal to one. This spans the kernel of $A_S - kI$. Since B is nonzero, there is some i such that $B\mathbf{e}_i$ is nonzero, where \mathbf{e}_i is the vector with a one as its i -th coordinate and zeros in every other coordinate. Moreover, $(A_S - kI)B = 0$ and so $B\mathbf{e}_i = c\mathbf{j}$ for some $c \in \mathbb{Z} \setminus \{0\}$. Then $\mathbf{j}^T B = \mathbf{j}^T \prod_{i=-k+1}^{k-1} (A_S - iI) = (2k - 1)! \mathbf{j}^T$. Hence,

$$(2k - 1)! = (2k - 1)! \mathbf{j}^T \cdot \mathbf{e}_i = \mathbf{j}^T B \mathbf{e}_i = c \mathbf{j}^T \cdot \mathbf{j} = c|G|.$$

It follows that $|G|$ divides $(2k - 1)!$ in this case. Notice that this case necessarily occurs if S contains an element of odd order. It also occurs when G is perfect. To see this, note that $\text{Cay}(G, S)$ being bipartite implies that there is a homomorphism ϕ from G to \mathbb{Z}_2 which sends each element in S (and all elements in the bipartite class containing S) to 1. The kernel of ϕ must contain G' since the image is abelian, and so if G is perfect then ϕ would need to be trivial.

Case II. $\text{Cay}(G, S)$ is bipartite.

We let \mathbf{u} be a nonzero integer vector with $A_S \mathbf{u} = -k\mathbf{u}$. We can take \mathbf{u} to be the vector whose coordinates are all in $\{\pm 1\}$, where we have a 1 in the g -th coordinate if and only if g is in the kernel of the homomorphism from G to \mathbb{Z}_2 that sends each element of S to 1.

As before we let $B = \Phi(A_S)$, where Φ is the polynomial described in Case I. Then $(A - kI)(A + kI)B = 0$ and so the range of B is contained in the span of \mathbf{j} and \mathbf{u} . Moreover, B is nonzero since k and $-k$ occur as eigenvalues of $|A|$. Thus there is some i such that $B\mathbf{e}_i = c\mathbf{j} + d\mathbf{u}$ for some $c, d \in \mathbb{Q}$, not both zero, with $c\mathbf{j} + d\mathbf{u}$ a vector with integer coordinates. Notice that this implies that $c + d$ and $c - d$ are integers.

Since A_S is Hermitian and \mathbf{u} and \mathbf{j} are eigenvectors from distinct eigenspaces, we see that \mathbf{u} and \mathbf{j} are orthogonal. As before, we have

$$\mathbf{j}^T B = \Phi(k) \mathbf{j}^T = (2k - 1)! \mathbf{j}^T \quad \text{and} \quad \mathbf{u}^T B = \Phi(-k) \mathbf{u}^T = -(2k - 1)! \mathbf{u}.$$

Thus

$$(2k - 1)! = (2k - 1)! \mathbf{j}^T \cdot \mathbf{e}_i = \mathbf{j}^T B \mathbf{e}_i = c \mathbf{j}^T \cdot \mathbf{j} = c|G| \quad (4.1)$$

and

$$-(2k-1)! = -(2k-1)! \mathbf{u}^T \cdot \mathbf{e}_i = d \mathbf{u}^T \cdot \mathbf{u} = d|G|. \quad (4.2)$$

By summing up (4.1) and (4.2), we see that $(c+d)|G| = 0$, thus $d = -c$. By taking the difference, we obtain $2c|G| = 2(2k-1)!$. Since $2c = c - d$ is an integer, we conclude that $|G|$ divides $2(2k-1)!$. \square

We now classify all Cayley integral groups. During the course of giving our classification, it will be useful to understand whether some groups of small order are Cayley integral or not.

Lemma 4.3.7. *The following groups are Cayley integral groups:*

- (a) S_3 ,
- (b) the dicyclic group Dic_{12} (the non-trivial semi-direct product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$),
- (c) $Q_8 \times \mathbb{Z}_2^d$ for every $d \geq 0$.

Proof. Notice that (a) follows from (b) since Dic_{12} has S_3 as homomorphic image. We note that Dic_{12} has $\langle x, y \mid x^3 = y^4 = 1, xy^{-1} = x^{-1} \rangle$ as a presentation. Any symmetric subset S of Dic_{12} is a union of sets from $\{1\}$, $\{x, x^2\}$, $\{y, y^3\}$, $\{y^2\}$, $\{xy, xy^3\}$, $\{x^2y, x^2y^3\}$, and $\{xy^2, x^2y^2\}$. Moreover, y^2 is central and hence gets mapped to either the identity or to the negative of the identity by any irreducible representation. We consider these cases separately. If y^2 is sent to $-I$ then each of $y + y^3$, $xy + xy^3$, and $x^2y + x^2y^3$ is sent to zero; and each of $xy^2 + x^2y^2$, y^2 , $x + x^2$, and 1 is sent to an integer scalar matrix. Thus each symmetric set S has the property that the corresponding element of the group algebra is sent to an integer scalar multiple of the identity and hence has integer eigenvalues. If, on the other hand, y^2 is sent to I then our representation factors through $\text{Dic}_{12}/\langle y^2 \rangle \cong S_3$. Notice that if we let π denote the isomorphism from $\text{Dic}_{12}/\langle y^2 \rangle$ to S_3 , in which the image of x is sent to (123) and the image of y is sent to (12) , then we see that the symmetric set S becomes a multi-set in which we have at most two copies of $\{\text{id}\}$, at most three copies of $\{(123), (132)\}$, and either zero or two copies of each of $\{(12)\}$, $\{(13)\}$, and $\{(23)\}$.

Both id and $(123) + (132)$ are central in the group algebra and since the characters of S_3 are integer-valued we see that these elements are sent to integer multiples of the identity in any irreducible representation of S_3 . Thus these sets have no affect on whether we obtain a matrix with integer eigenvalues. Thus we may assume that the multi-set is a union consisting of either 0 or 2 copies of each of $\{(12)\}$, $\{(13)\}$, $\{(23)\}$. Notice that these

elements each have order 2 and so if the multi-set has size 2 (i.e., we have two copies of a single transposition) then we obtain a matrix with eigenvalues in $\{\pm 2\}$. Next, observe that $(12) + (13) + (23)$ is central and since the characters of S_3 are integer-valued, we see that if S has size 6 then we again obtain a matrix with integer eigenvalues. Finally, if our multi-set has size 4 then by applying an inner automorphism we may assume that it is given by $\{(12), (12), (13), (13)\}$. Then $(12) + (13)$ maps to 2 under the trivial representation; to -2 under the alternating representation; and has the same image as $-(23)$ in the irreducible 2-dimensional representation of S_3 . Thus we see that in each case we obtain a matrix with integer eigenvalues. This establishes (a) and (b).

To show (c), let $G = Q_8 \times \mathbb{Z}_2^d$ and let z be the central element of order 2 in Q_8 . If ϕ is an irreducible representation of G then z must either be sent to the identity or to the negative of the identity. If z is sent to the identity then ϕ in fact factors through $G/\langle z \rangle$, which is an elementary abelian 2-group and thus ϕ is one-dimensional and clearly any symmetric set will be sent to an integer. If, on the other hand, $\phi(z) = -I$, then notice that if u is an element of order 4 then $u^2 = z$ and so the natural extension of ϕ to the group algebra of G sends $u + u^{-1} = u(1 + z)$ to 0. Consequently, we only need to consider symmetric sets consisting of elements of order 2. But all elements of order 2 are central in G and hence are mapped to either I or $-I$ by ϕ . It follows that $\text{Cay}(G, S)$ is an integer Cayley graph for each symmetric subset S of G , giving (c). \square

Lemma 4.3.8. *The following groups are not Cayley integral groups:*

- (1) any dihedral group D_n with $n \geq 4$;
- (2) any non-abelian group of order 12 that is not isomorphic to Dic_{12} ;
- (3) any non-abelian group of order 18;
- (4) any non-abelian group of order 24;
- (5) $Q_8 \times \mathbb{Z}_4$.

Proof. We first show (1). If $n \geq 4$ and $n \notin \{4, 6\}$ then D_n contains an element that is of order $r \notin \{1, 2, 3, 4, 6\}$ and thus D_n is not Cayley integral (since the subgroup isomorphic to \mathbb{Z}_r is not). Thus we only need to worry about $n \in \{4, 6\}$. Notice that D_n has the presentation

$\langle x, y \mid x^2 = y^n = 1, xyx = y^{-1} \rangle$. We have a 2-dimensional representation θ of D_n given by

$$x \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} \omega_n & 0 \\ 0 & \omega_n^{-1} \end{pmatrix},$$

where ω_n is the primitive n -th root of unity. Then if we use the symmetric generating set $S = \{x, xy\}$ we see that $\theta(x) + \theta(xy)$ is given by

$$\begin{pmatrix} 0 & 1 + \omega_n \\ 1 + \omega_n^{-1} & 0 \end{pmatrix},$$

which has eigenvalues $\pm\sqrt{2 + \omega_n + \omega_n^{-1}}$. We note that if $n = 4$ then this gives eigenvalues $\pm\sqrt{2}$ and if $n = 6$ this gives eigenvalues $\pm\sqrt{3}$. Thus we have (1).

We now consider (2). Notice that the only non-abelian groups of order 12 are, up to isomorphism, Dic_{12} , A_4 , and D_6 . By (1), we only need to consider A_4 . For A_4 notice that if we use the 4-dimensional representation ρ which associates to a permutation in A_4 its corresponding permutation matrix and if we use the symmetric set $S = \{(13)(24), (14)(23), (123), (132)\}$, then by extending ρ to the group algebra of A_4 via linearity, we see that $(13)(24) + (14)(23) + (123) + (132)$ is represented by the matrix

$$\begin{pmatrix} 0 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 2 & 0 & 0 \\ 1 & 1 & 0 & 2 \end{pmatrix},$$

which has eigenvalues $4, -1, \frac{-1 \pm \sqrt{17}}{2}$. Thus A_4 is not Cayley integral.

To prove (3), we note that up to isomorphism there are only three non-abelian groups of order 18: D_9 , $S_3 \times \mathbb{Z}_3$, and the group $E_9 \cong \mathbb{Z}_3^2 \rtimes_{\theta} \mathbb{Z}_2$, where θ is the map that sends every element of \mathbb{Z}_3^2 to its inverse. The group D_9 is not Cayley integral by (1). For $S_3 \times \langle x \mid x^3 = 1 \rangle$, we take the representation that sends $(\sigma, x^j) \mapsto \omega^j P(\sigma)$, where ω is the primitive third-root of unity and P is the (reducible) 3-dimensional representation of S_3 that associates to $\sigma \in S_3$ the 3×3 permutation matrix $P(\sigma)$ of σ . If we extend this to the group algebra via linearity, then the symmetric element $((12), x) + ((12), x^2) + ((13), 1)$ is represented by the matrix

$$\begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 0 \\ 1 & 0 & -1 \end{pmatrix},$$

which has eigenvalues $0, \pm\sqrt{3}$. Thus $S_3 \times \mathbb{Z}_3$ is not Cayley integral. The group E_9 has presentation $\langle x, y \mid x^3 = y^3 = [x, y] = 1 \rangle \rtimes \langle z \mid z^2 = 1 \rangle$, where the automorphism of $\langle x, y \rangle$ determining the semidirect product is $x \mapsto x^{-1}, y \mapsto y^{-1}$. Notice that xz, yz , and z all have order 2. Thus we may consider the symmetric set $S = \{xz, z, yz\}$. We claim that the element $xz + z + yz$ in the group algebra has some representation with eigenvalues that are not all integers. To see this, observe that $\langle x \rangle$ is a normal subgroup of E_9 and when we mod out by this group we have a group isomorphic to S_3 with isomorphism given by $\bar{y} \mapsto (123), \bar{z} \mapsto (12)$. Then the image of $xz + z + yz$ in the group algebra of S_3 under the composition of maps described above is $2(12) + (13)$. Notice that the 3-dimensional permutation representation of S_3 sends this element to

$$\begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix},$$

which has eigenvalues $\{3, \pm\sqrt{3}\}$. Notice that this representation lifts to a representation of E_9 and thus we see that E_9 is not Cayley integral.

To prove (4), we note that up to isomorphism there are 15 groups of order 24, 3 of which are abelian. Of the remaining 12 there are only two that do not have any elements of order 8 or 12, do not contain a copy of D_4 , and do not contain a copy of a non-abelian group of order 12 that is not isomorphic to Dic_{12} . (These are necessary properties to be Cayley integral by (1) and (2).) These two groups are $\text{SL}_2(\mathbb{Z}_3)$ and $\text{Dic}_{12} \times \mathbb{Z}_2$, up to isomorphism. Notice that S_3 is a homomorphic image of Dic_{12} and so $S_3 \times \mathbb{Z}_2$ is a homomorphic image of $\text{Dic}_{12} \times \mathbb{Z}_2$. But $S_3 \times \mathbb{Z}_2$ is not Cayley integral by (2) and so neither is $\text{Dic}_{12} \times \mathbb{Z}_2$. Note that A_4 is isomorphic to $\text{PSL}_2(\mathbb{Z}_3)$ and hence A_4 is a homomorphic image of $\text{PSL}_2(\mathbb{Z}_3)$. This shows that $\text{PSL}_2(\mathbb{Z}_3)$ is not Cayley integral by (2). This establishes (4).

Finally, to prove (5), we note that $Q_8 = \langle x, y, z \mid x^2 = y^2 = [x, y] = z, z^2 = 1 \rangle$ has a representation π determined by

$$x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Thus $Q_8 \times \langle t \mid t^4 = 1 \rangle$ has a 2-dimensional representation ρ given by $\rho((a, t^j)) = i^j \pi(a)$ for $a \in Q_8$ and $j \in \mathbb{Z}$, where i is a primitive fourth root of unity. If we use the symmetric set $S = \{(x, t), (x^{-1}, t^{-1}), (y, t), (y^{-1}, t^{-1})\}$, we see that ρ sends the element $(x, t) + (x^{-1}, t^{-1}) +$

$(y, t) + (y^{-1}, t^{-1})$ from the group algebra to

$$\begin{pmatrix} -2 & 2i \\ -2i & 2 \end{pmatrix},$$

which has eigenvalues $\pm 2\sqrt{2}$ and hence $Q_8 \times \mathbb{Z}_4$ is not Cayley integral, giving us (5). \square

Corollary 4.3.3. Let $H \leq S_4$ be a Cayley integral subgroup of S_4 that acts transitively on $\{1, 2, 3, 4\}$. Then H has order 4.

Proof. We note that if H has order in $\{8, 12, 24\}$ then H is isomorphic to one of D_4 , A_4 , or S_4 and hence is not Cayley integral by Lemma 4.3.8 (1), (2), and (4). Each subgroup of order 6 is equal to the set of permutations that fix some element $i \in \{1, 2, 3, 4\}$ and hence does not act transitively on $\{1, 2, 3, 4\}$. Thus H has order in $\{1, 2, 3, 4\}$. It is straightforward to check that a subgroup of order 1, 2, or 3 cannot act transitively on $\{1, 2, 3, 4\}$ and thus H has order 4. \square

We now start the classification of Cayley integral groups by first classifying the Cayley integral 2-groups.

Lemma 4.3.9. Let Q be a Cayley integral 2-group. Then the following statements hold:

- (i) Every element of order 2 is central.
- (ii) If Q is non-abelian then any two elements that do not commute generate a subgroup that is isomorphic to Q_8 .

Proof. Let N denote the set of elements in Q of order at most 2. We claim that N is a group. To see this, it is sufficient to show that if $x, y \in N$ then $xy = yx$ since this implies that $(xy)^2 = x^2y^2 = 1$. This will show that the set of elements of order at most 2 is closed under multiplication and hence forms a group. Moreover, it follows that N is abelian. Let $x, y \in N$ and let E denote the subgroup of N generated by x and y . Then E is a Cayley integral group and applying Proposition 4.3.2 to the symmetric set $S = \{x, y\}$, we see that $|E|$ divides 12. Since E is in Q and Q is a 2-group, we see that E has order at most 4 and thus is abelian. This means that x and y commute and since they were arbitrary elements of N , we thus have that N is an abelian group as claimed. We note that N is normal, since the set of elements of order at most 2 is closed under conjugation.

To complete the proof of (i), we must show that N is a central subgroup of Q . Suppose, towards a contradiction, that N is not central. Then there is some $u \in Q$ such that conjugation by u induces a non-trivial automorphism of N . Note that every element of Q has order dividing 4. Therefore $u^2 \in N$ and so this automorphism must have order 2. Hence there are $x, y \in N$ with $x \neq y$ such that $uxu^{-1} = y$ and $uyu^{-1} = x$. Let Q_1 denote the subgroup of Q generated by x, y , and u . Then Q_1 is non-abelian and has order 8 or 16. Notice that Q_1 has at least four elements of order 4 and hence must be isomorphic to D_4 if it has order 8; but D_4 is not Cayley integral by Lemma 4.3.8 and so we see Q_1 must have order 16. In particular, u has order 4 and $\langle u \rangle$ intersects $\langle x, y \rangle$ trivially. Thus $Q_1/\langle u^2 \rangle$ is a Cayley integral group of order 8 and, as before, we see that it is isomorphic to D_4 , a contradiction. It follows that each element of N is indeed central, which establishes (i).

We now prove (ii). Suppose that $x, y \in Q$ and that they do not commute. By (i), x and y must both have order at least 4. But since $\langle x \rangle$ and $\langle y \rangle$ are Cayley integral, their order is equal to 4. Notice that since the square of every element is central, Q/N is elementary abelian and so $Q' \subseteq N$. In particular, $[x, y] = z$, where $z \in Q$ is a central element of order 2. We claim that $x^2 = y^2 = z$. To see this, suppose that $x^2 \neq z$ and let H denote the subgroup of Q generated by x and y . Then $E := H/\langle x^2 \rangle$ is a Cayley integral 2-group and the image of x in E now has order 2 and so it must be central. But the image of $[x, y] = z$ in E is non-trivial, a contradiction since by (i) we have that every element of order 2 in E is central. It follows that $x^2 = y^2 = z$ and so H is a non-abelian homomorphic image of the group with presentation

$$\langle s, t, u \mid s^4 = t^4 = u^2 = 1, s^2 = t^2 = [s, t] = u, [s, u] = [t, u] = 1 \rangle.$$

We note that this is just a presentation of Q_8 and since H is non-abelian, we see that $H \cong Q_8$. \square

Proposition 4.3.4. Let Q be a non-abelian Cayley integral 2-group. Then $Q \cong Q_8 \times \mathbb{Z}_2^d$ for some $d \geq 0$.

Proof. By Lemma 4.3.9, every element of order 2 in Q is central and any pair of non-commuting elements of Q generate a subgroup that is isomorphic to Q_8 . Moreover, every element is of order 1, 2, or 4. Let u, v be elements of order 4 that generate a copy of Q_8 . Then there is a central element z of order 2 such that $u^2 = v^2 = [u, v] = z$. We claim that if w is another element of order 4 then $w^2 = z$. To see this, note that if $w^2 \neq z$ then w

and u must commute since otherwise by Lemma 4.3.9 (ii) they generate a copy of Q_8 with $w^2 = [u, w] = u^2 = z$. Similarly, $[w, v] = 1$ and since w^2 is central and not in $\{1, u^2\}$, we see that the group generated by u, v , and w is isomorphic to $Q_8 \times \mathbb{Z}_4$, which is not Cayley integral by Lemma 4.3.8 (5). It follows that all elements of order 4 in Q have the same square.

Let Z denote the central subgroup of Q consisting of elements of order at most 2. By assumption, there exist u and v that do not commute and hence there is some $z \in Z$ such that $u^2 = v^2 = [u, v] = z$. We claim that Q is generated by u, v , and Z . To see this, let Q_0 denote the subgroup of Q generated by u, v , and Z and suppose that there is some $w \in Q \setminus Q_0$. Then w has order 4 and so $w^2 = z$. If u and w commute then $(uw)^2 = u^2w^2 = z^2 = 1$ and so $uw \in Z$, which gives that $w \in Q_0$, a contradiction. Thus u and w do not commute, which gives that $u^2 = w^2 = [u, w] = z$ by Lemma 4.3.9 (ii). Similarly, we have $v^2 = w^2 = [v, w] = z$. Notice that $(uvw)^2 = 1$ and so $uvw \in Z$, which gives that $w \in v^{-1}u^{-1}Z \subseteq Q_0$, a contradiction. Thus $Q = Q_0$ and so Q is generated by u, v and Z . Now let H be the subgroup of Q generated by u and v . Then $H \cong Q_8$ and $H \cap Z = \langle z \rangle$. Note that Z is an elementary abelian 2-group and so there is an elementary abelian subgroup Z_1 such that $Z_1 \oplus \langle z \rangle = Z$. Then we see that $Q \cong H \times Z_1 \cong Q_8 \times \mathbb{Z}_2^d$ for some $d \geq 0$. \square

We now classify Cayley integral 3-groups. As it turns out, the classification in this case is simpler.

Proposition 4.3.5. Every Cayley integral 3-group is elementary abelian.

Proof. Let x and y be two elements of a Cayley integral group P and let P_0 denote the subgroup of P generated by x and y . Then P_0 is Cayley integral and so applying Proposition 4.3.2 to the symmetric set $S = \{x, x^{-1}, y, y^{-1}\}$ gives that the order of P_0 divides $7!$. Since P_0 is a 3-group, we see that $|P_0|$ divides 9. In particular P_0 is abelian and so x and y commute. Since all elements of P commute, we see that P is abelian. Since every element of P has order 1 or 3, we see that P is an elementary abelian 3-group. \square

Corollary 4.3.6. Let G be a nilpotent Cayley integral group. Then G is either abelian or $G \cong Q_8 \times \mathbb{Z}_2^d$ for some $d \geq 0$.

Proof. If G is nilpotent then G must be a direct product of a Cayley integral 2-group and a Cayley integral 3-group. Thus by Propositions 4.3.4 and 4.3.5, if G is non-abelian then

$G \cong (Q_8 \times \mathbb{Z}_2^d) \times \mathbb{Z}_3^e$ for some $d, e \geq 0$. Note that if $e \geq 1$ then G contains a copy of $Q_8 \times \mathbb{Z}_3$ which is not Cayley integral by Lemma 4.3.8 (4). Hence $e = 0$ and the result follows. \square

We now begin to study non-nilpotent Cayley integral groups. We first show that such groups necessarily have a unique Sylow 3-subgroup. To do this, we first require a few lemmas.

Lemma 4.3.10. *Let G be a Cayley integral group. If G has a normal Sylow 2-subgroup then G is nilpotent.*

Proof. Suppose that this is not the case. Then we can pick a non-nilpotent Cayley integral group G of smallest order with respect to having a normal Sylow 2-subgroup.

Let Q denote the Sylow 2-subgroup of G and let Z denote the center of Q . Let P be a Sylow 3-subgroup of G . Then G is a semi-direct product $P \rtimes Q$. Since Z is a characteristic subgroup of Q and Q is normal in G , we see that if $x \in P$ then $xZx^{-1} = Z$. Pick $z \in Z$ of order 2. We claim that z commutes with every element of P . To see this, suppose towards a contradiction, that there is some $x \in P$ such that $xz \neq zx$. Then $z_1 := xzx^{-1}$ and $z_2 := x^2zx^{-2}$ have the property that the subgroup of Z generated by z, z_1, z_2 is an elementary abelian 2-group of order either 4 or 8 and hence the group generated by x and z must have order 12 or 24. By Lemma 4.3.8, the only non-abelian Cayley integral group of order either 12 or 24 is isomorphic to the dicyclic group of order 12, but this one does not have a normal Sylow 2-subgroup, a contradiction.

Thus we see that $xz = zx$ for every $z \in Z$ and $x \in P$. This means that the centralizer of z contains both P and Q and thus must contain all of G . Notice that $H := G/\langle z \rangle$ is a Cayley integral group with the property that it has a normal Sylow 2-subgroup. By minimality of the order of G we see that H is nilpotent. It follows that G is nilpotent, since we obtained H by taking the quotient of G with a central subgroup. \square

Lemma 4.3.11. *Let G be a Cayley integral group generated by two elements of order 3. Then G is isomorphic to \mathbb{Z}_3 or to $\mathbb{Z}_3 \times \mathbb{Z}_3$.*

Proof. Let x and y be elements of order 3 in G that generate G as a group. Notice that the set $S = \{x, x^{-1}, y, y^{-1}\}$ has size 4 and since x has odd order we see from Proposition 4.3.2 that the order of G divides $7!$. Since G is a $(2, 3)$ -group, we see that the order of G in fact divides 144.

We let n_3 denote the number of Sylow 3-subgroups of H . It is known that $n_3 \equiv 1 \pmod{3}$ and that n_3 divides the index of the Sylow subgroup in G . Since $|G|$ divides 144, the index is 2^t , where $0 \leq t \leq 4$, thus $n_3 \in \{1, 4, 16\}$.

If $n_3 = 1$, then G has a unique Sylow 3-subgroup, which is elementary abelian by 4.3.5. Hence x and y commute and so they generate a group of order 3 or 9. This yields the conclusion of the lemma.

In the rest of the proof we argue by contradiction, considering the cases $n_3 = 4$ and $n_3 = 16$ separately.

Suppose that $n_3 = 4$. Then G acts on the Sylow 3-subgroups by conjugation, which gives us a non-trivial homomorphism π from G to S_4 . Let G_0 denote the image of G under π . Since the collection of Cayley integral groups is closed under the process of taking subgroups and homomorphic images, G_0 is a Cayley integral subgroup of S_4 . Moreover, by construction G_0 acts transitively on $\{1, 2, 3, 4\}$ since G acts transitively on the set of Sylow 3-subgroups under conjugation. By Corollary 4.3.3, G_0 has order 4. Let N denote the kernel of π . Then N has order dividing 36 and by construction it contains all Sylow 3-subgroups and in particular contains x and y . But this means that the group generated by x, y is contained in N , a contradiction since N is a proper subgroup of G . We conclude that $n_3 = 4$ cannot occur.

Suppose next that $n_3 = 16$. Suppose first that $|G| \neq 144$. Since $n_3 = 16$, we know that 16 divides the order of G and since G is a proper divisor of 144 and 3 divides the order of G , we see that $|G| = 48$. Then each pair of distinct Sylow 3-subgroups must intersect trivially since they are all cyclic groups of order 3. Thus there are $16 \cdot 2 = 32$ elements of order 3. This leaves 16 unaccounted elements, which necessarily make up a normal Sylow 2-subgroup. By Lemma 4.3.10, we see that G is nilpotent and thus $n_3 = 1$, a contradiction.

Suppose now that $|G| = 144$. If each pair of distinct Sylow 3-subgroups intersect trivially then G has $8 \cdot n_3 = 128$ elements of order 3. This leaves 16 unaccounted for elements in G , which must make up a normal Sylow 2-subgroup. By Lemma 4.3.10, G is nilpotent, which gives that $n_3 = 1$, a contradiction.

Thus G has distinct Sylow 3-subgroups P and Q such that $P \cap Q = \langle u \rangle$ is a group of order 3. Notice that P and Q both have order 9 and hence are abelian. It follows that $C_G(u)$, the centralizer of u in G , contains the groups P and Q . It follows that its order is a multiple of 9 and since it contains two distinct Sylow 3-subgroups it must have at least four Sylow subgroups and so its order must in fact be in $\{36, 72, 144\}$.

Our next step is to show that $C_G(u)$ is normal in G . If $C_G(u)$ has order 72 or 144, this is

automatic, so we may assume that $|C_G(u)| = 36$. Then G acts on the left cosets of $C_G(u)$, giving a homomorphism ρ to S_4 . Let E denote the image of ρ in S_4 . By assumption the image of ρ is a Cayley integral group that acts transitively on $\{1, 2, 3, 4\}$ and hence E must have order 4 by Corollary 4.3.3. Thus the kernel of ρ has size 36 and since the kernel of ρ is contained in $C_G(u)$, we see that $C_G(u)$ is normal in this case.

We now show that $C_G(u) = G$. Since G is generated by x and y , it is sufficient to show that u commutes with y . Let Z_1 denote the Sylow 3-subgroup of the center of $C_G(u)$. Note that Z_1 is characteristic in $C_G(u)$ and hence normal in G . Moreover, Z_1 is non-trivial since $u \in Z_1$. Notice that if Z_1 has order 9 then it is a Sylow subgroup of G and since all Sylow subgroups are conjugate and $C_G(u)$ is normal we see that x and y are in $C_G(u)$, which gives that $G = C_G(u)$ since x and y are generators of G . Thus $Z_1 = \langle u \rangle$. Notice that $xZ_1x^{-1} = Z_1$ and so $xux^{-1} \in \{u, u^{-1}\}$. If $xu = u^{-1}x$ then $u = x^3u = u^{-1}x^3 = u^{-1}$, a contradiction. Thus $xu = ux$. Similarly, $yu = uy$, which gives that $x, y \in C_G(u)$ and so $C_G(u) = G$.

Now $H := G/\langle u \rangle = C_G(u)/\langle u \rangle$ is a Cayley integral group of order 48 and is generated by two elements of order 3. Since we already proved the lemma for groups whose order is less than 144, we can apply the lemma to the group H . It follows that H has order 3 or 9. This gives a contradiction and completes the proof by showing that $n_3 \neq 16$ when $|G| = 144$. \square

Proposition 4.3.7. Let G be a Cayley integral group. Then G has a normal abelian Sylow 3-subgroup.

Proof. By Lemma 4.3.11 any two elements of order 3 generate a group of order 3 or 9. Since groups of orders 3 and 9 are abelian, it follows that any two elements of order 3 commute. Thus the product of two elements of order 3 has order 1 or 3. This shows that elements of order dividing 3 are closed under multiplication in G and hence form a group. This group is necessarily the unique Sylow 3-subgroup of G and so G has a normal Sylow 3-subgroup. By Proposition 4.3.5, this group must be abelian. \square

Corollary 4.3.8. Let G be a non-nilpotent Cayley integral group. Then G is isomorphic to either S_3 or Dic_{12} .

Proof. By Proposition 4.3.7, G has a normal Sylow 3-subgroup, $P \cong \mathbb{Z}_3^d$. Moreover, $d \geq 1$ since G is not nilpotent. Let Q be a Sylow 2-subgroup of G . Then $G = P \rtimes Q$.

We first claim that if $x \in P$ and if $y \in Q$ has order 2, then $xyx^{-1} \in \{x, x^{-1}\}$. To see this, suppose that $xyx^{-1} = u \notin \{x, x^{-1}\}$. Then u is of order 3 and x and u generate a group of

order 9 by Lemma 4.3.11. Consequently, x, y, u generate a non-abelian subgroup of G of order 18. But this contradicts Lemma 4.3.8 (3), since a non-abelian group of order 18 cannot be Cayley integral.

We next claim that if $|P| \geq 9$ and if $y \in Q$ has order 2, then $yx = xy$ for every $x \in P$. To see this suppose that there is some $x \in P$ such that $yx \neq xy$. As shown above, we have $xyx^{-1} = x^{-1}$. Let $u \in P$ be such that $\langle x, u \rangle$ has order 9. Then since $yuy^{-1} \in \{u, u^{-1}\}$, we see that u, x, y generate a non-abelian group of order 18. But this is a contradiction, since Lemma 4.3.8 says that no such group can be Cayley integral. Thus we have shown that either $|P| = 3$ or we have $yx = xy$ whenever $y \in Q$ has order 2 and $x \in P$.

We next claim that if $|P| \geq 9$ and $w \in Q$ then $wxw^{-1} \in \{x, x^{-1}\}$ for every $x \in P$. To see this, suppose that this is not the case. Then $wxw^{-1} = u \notin \{x, x^{-1}\}$. By the above, the order of w is greater than 2 and since G is Cayley integral and $w \in Q$, its order must be 4. Thus w^2 has order 2 and hence $w^2x = xw^2$. This implies that $wuw^{-1} = x$ and so the group generated by u, x, w is a non-abelian group of order 36 and w^2 is central. Notice that the quotient of the group generated by u, x, w by $\langle w^2 \rangle$ is a non-abelian group of order 18 and hence it cannot be Cayley integral by Lemma 4.3.8 (3). This is a contradiction and so we conclude that if $|P| \geq 9$ then whenever $x \in P$ we have that $\langle x \rangle$ is normal in G since its normalizer contains both P and Q .

We now claim that $|P| \leq 3$. If $|P| \geq 9$, then notice that P cannot be central in G since G is not nilpotent. Thus there is some $y \in Q$ and some $x \in P$ such that $xy \neq yx$. We have just shown that we must have $xyx^{-1} = x^{-1}$. Pick $u \in P$ such that u and x generate a subgroup of P of order 9. Then $\langle u, x \rangle$ is normal in G , the group E generated by y, u, x has order 36, and y^2 is central in E . But by construction, $E/\langle y^2 \rangle$ is a non-abelian group of order 18 and hence cannot be Cayley integral. It follows that $|P| \leq 3$, as claimed. Moreover, since G is not nilpotent, $|P| = 3$.

We next claim that Q is abelian. If not, then Q contains a copy of Q_8 . Then G contains a copy of $P \rtimes Q_8$, which is not Cayley integral by Lemma 4.3.8 (4), since $P \rtimes Q_8$ is a non-abelian group of order 24. Thus Q is abelian.

Finally, we claim that Q has order at most 4. To see this, suppose that $|Q| \geq 8$. By assumption, G is non-nilpotent and so there is some $u \in Q$ such that conjugation by u induces a non-trivial automorphism of P . Since Q is an abelian 2-group of order at least 8, there is a subgroup Q_0 of Q of order 8 that contains u . Then $P \rtimes Q_0$ is a non-abelian group of order 24 and so by Lemma 4.3.8 (4) is not Cayley integral, a contradiction. Thus Q has

order at most 4 and since G is not nilpotent it must have order at least 2. Hence $G = P \rtimes Q$ has order 6 or 12. Since G is not nilpotent, we see by Lemma 4.3.8 that $G \cong S_3$ if $|G| = 6$, and $G \cong \text{Dic}_{12}$ if $|G| = 12$. This completes the proof. \square

We are now ready to give the proof of the classification result for Cayley integral groups.

Proof of Theorem 4.3.2. If G is not nilpotent, then by Corollary 4.3.8 we have that $G \cong \text{Dic}_{12}$ or $G \cong S_3$. If G is nilpotent and non-abelian then by Corollary 4.3.6 we see that $G \cong Q_8 \times \mathbb{Z}_2^d$ for some $d \geq 0$. If G is abelian then by Theorem 4.3.1 we have that $G \cong \mathbb{Z}_3^d \times \mathbb{Z}_2^e$ or $G \cong \mathbb{Z}_2^d \times \mathbb{Z}_4^e$ for some $d, e \geq 0$. By Lemma 4.3.7 all of these groups are Cayley integral. \square

Chapter 5

Integral Cayley graphs of small degree

The study of integral Cayley graphs of small degree began with [2] by Abdollahi and Vatandoost. They used a result of Schwenk [51] and classified all cubic integral Cayley graphs. Essentially their method was to recognize Cayley graphs among the famous 13 cubic integral graphs which was found by Schwenk. In another paper, Abdollahi and Vatandoost (see [3]) attempted to classify all 4-regular integral Cayley graphs over abelian groups. They found a list of possible orders of abelian groups which admit 4-regular integral Cayley graphs. Their list is incomplete and more than half of the possible sizes do not admit any abelian group with an associated integral Cayley graph. Minchenko and Wanless [44] investigated the 4-regular integral vertex-transitive graphs. They used the data provided by Cvetković, Stevanović and others in [24, 54, 53, 55]. They managed to find all 4-regular bipartite integral Cayley graphs and their associated groups. These results are derived primarily from computer computations. In this chapter we characterize groups which admit connected integral Cayley graphs of small degrees. All of our results are based on theoretical arguments. In the first section, we characterize abelian groups which admit connected 3, 4 or 5-regular integral Cayley graphs. We will find some general bounds and for a given fixed degree, we explain a general approach to find all abelian groups for which there are connected integral Cayley graphs of that degree. In the next section, we classify all non-abelian groups for which there are connected cubic integral Cayley graphs. We explain the current state of non-abelian groups which admit connected 4-regular integral Cayley graphs.

5.1 Abelian groups admitting integral Cayley graphs of small degree

In this section, we will determine abelian groups G which admit a connected integral Cayley graph. We notice that if $\text{Cay}(G, S)$ is a connected Cayley graph, then $|G|$ divides $2(2|S| - 1)!$ (see Theorem 4.3.2). In most cases, this bound is a lot bigger than the actual group order. In this section, we provide a stronger bound in the case of abelian groups. It turns out that this bound is sharp as well. We conjecture that in general $|G| \leq (|S| + 1)!$ holds whenever $\text{Cay}(G, S)$ is integral and S is a symmetric generating set.

Lemma 5.1.1. *For every positive integer n such that $n \neq 6$, we have:*

$$2^{\phi(n)} \geq n.$$

Equality happens only if $n = 2$ or $n = 4$.

Proof. It is known (see page 9 in [45]) that for $n \neq 2, 6$, $\phi(n) \geq \sqrt{n}$. One can see that $\phi(2) = 1 = \log_2 2$, while $\phi(6) = 2 < 2.584 \approx \log_2 6$. Function $f(x) = \sqrt{x} - \log_2 x$ is strictly increasing for $x > 9$, and $f(16) = 0$. Hence, for $n > 16$ we have $\phi(n) \geq \sqrt{n} > \log_2 n$. This implies for $n > 16$ that $2^{\phi(n)} > n$. Through direct calculation for $2 \leq n \leq 16$, we have the desired result, with equality just when $n = 2$ or $n = 4$. \square

Lemma 5.1.2. *Let G be an abelian group and S a symmetric generating set of G such that there is no element of order 6 in S . If $\text{Cay}(G, S)$ is integral, then $|G| \leq 2^{|S|}$. Equality happens only if S is a minimal symmetric generating set such that all elements in S are of order 2 or 4.*

Proof. We prove this by induction on the number of non-involution elements in S . We notice that if S is a generating set of G , then $|G| \leq \prod_{s \in S} \text{ord}(s)$ with equality only when S is a minimal generating set. If all elements in S are involutions, then we are done. Suppose the assertion is true for symmetric generating sets with at most d non-involutions, where d is a non-negative integer. Let G be an abelian group and S a symmetric generating set in G with $d + 1$ non-involutions such that $\text{Cay}(G, S)$ is integral. Suppose $s \in S$ is a non-involution element in S . By Theorem 2.4.4, the integrality of $\text{Cay}(G, S)$ implies that S is a union of distinct atoms of the group algebra $\mathbb{B}(G)$. Thus $[s] \subseteq S$ ($[s]$ denotes the atom containing s). Let $S_1 = S \setminus [s]$. If $H = \langle S_1 \rangle$, then $\text{Cay}(H, S_1)$ is integral and S_1 has less

than d non-involutions. By the induction hypothesis $|H| \leq 2^{|S_1|}$, with equality only if S_1 is a minimal symmetric generating set of elements of orders 2 or 4. We have $|\langle s \rangle| = \phi(k)$, where $k = \text{ord}(s) \geq 2$. Since $|G| \leq |H||\langle s \rangle| = k|H|$, we have $|G| \leq 2^{|S_1| - \phi(k)}k \leq 2^{|S_1|}$. Equality happens if and only if $|G| = |H||\langle s \rangle|$, $|H| = 2^{|S_1|}$ and $2^{\phi(k)} = k$. From group theory, we have $|G| = |H\langle s \rangle| = \frac{|H||\langle s \rangle|}{|H \cap \langle s \rangle|}$. Thus $|G| = |H||\langle s \rangle|$ if and only if $|H \cap \langle s \rangle| = 1$. Therefore, s is not a redundant generator in S . By induction hypothesis, $|H| = 2^{|S_1|}$ if and only if S_1 is a minimal generating set consisting of elements of orders 2 or 4. Finally, Lemma 5.1.1 gives that $2^{\phi(k)} = k$ if and only if $k = 2$ or $k = 4$. This completes the proof. \square

It is interesting that if $G = \mathbb{Z}_2^n$ and S is a generating set of G consisting of n involutions, then $\text{Cay}(G, S) = Q_n$ is integral. Therefore the inequality in Lemma 5.1.2 is sharp.

Theorem 5.1.3. *Let G be an abelian group and S a symmetric generating set of G . Let α denote the number of elements of order 6 in S and $\beta = |S| - \alpha$. If $\text{Cay}(G, S)$ is integral, then $|G| \leq 2^\beta 6^{\frac{\alpha}{2}}$.*

Proof. Let S_1 denote the subset of all elements of order 6 in S , and $S_2 = S \setminus S_1$. We have $G = \langle S_1 \rangle \langle S_2 \rangle$. Thus $|G| \leq |\langle S_1 \rangle| |\langle S_2 \rangle|$. By Theorem 2.4.4, S is a symmetric subset of G which is a disjoint union of atoms of $\mathbb{B}(G)$. Therefore, S_1 and S_2 are also symmetric and they are unions of disjoint atoms. This implies that $|\langle S_1 \rangle| \leq 6^{\frac{\alpha}{2}}$. We notice that $\text{Cay}(\langle S_2 \rangle, S_2)$ is integral graph satisfying the conditions of Lemma 5.1.2. Therefore $|\langle S_2 \rangle| \leq 2^{|S_2|}$. Combining these two together, we have $|G| \leq 2^\beta 6^{\frac{\alpha}{2}}$. \square

Corollary 5.1.4. *Let G be an abelian group and S a symmetric generating set of G . If $\text{Cay}(G, S)$ is integral, then we have;*

- $|G| \leq 2^{|S| + \frac{\alpha}{2}}$, where α is the number of elements of order 6 in S .
- $|G| \leq 3^{|S|}$.

The following lemma is easy to prove.

Lemma 5.1.5. *Suppose G_1 and G_2 are two finite groups with symmetric generating sets S_1 and S_2 , respectively. Then the following statements hold:*

- $\text{Cay}(G_1, S_1) \square \text{Cay}(G_2, S_2) = \text{Cay}(G_1 \times G_2, S)$, where $S = (S_1 \times \{1_{G_2}\}) \cup (\{1_{G_1}\} \times S_2)$.
- $\text{Cay}(G_1, S_1) \times \text{Cay}(G_2, S_2) = \text{Cay}(G_1 \times G_2, S_1 \times S_2)$.

Notice that $\text{Cay}(G_1, S_1) \square \text{Cay}(G_2, S_2)$ is $(|S_1| + |S_2|)$ -regular, and $\text{Cay}(G_1, S_1) \times \text{Cay}(G_2, S_2)$ is $|S_1||S_2|$ -regular.

We say that there is a r -regular integral Cayley graph over a group G , if G has a symmetric generating set S such that $\text{Cay}(G, S)$ is an r -regular integral graph.

Theorem 5.1.6. *Suppose G is a cyclic group of even order and k a non-negative integer. There is a connected $(2k + 1)$ -regular integral Cayley graph over G if and only if there is a connected $2k$ -regular integral Cayley graph over G .*

Proof. Since G is cyclic of even order, there is a unique involution in G . Let S be a symmetric generating set of G . Notice that S contains the involution of G if and only if $|S|$ is odd. Suppose $|S| = 2k + 1$ and a is the involution in S . We have $G = \langle S \setminus \{a\} \rangle \langle a \rangle$, and $|G| = \frac{|S \setminus \{a\}| |\langle a \rangle|}{|\langle S \setminus \{a\} \rangle \cap \langle a \rangle|}$. We know $|\langle a \rangle| = 2$, thus $|\langle S \setminus \{a\} \rangle \cap \langle a \rangle|$ is either 1 or 2. We have $|\langle S \setminus \{a\} \rangle \cap \langle a \rangle| = 1$ only if $\langle S \setminus \{a\} \rangle = G$, and $|\langle S \setminus \{a\} \rangle \cap \langle a \rangle| = 2$ in the case of $G \cong \langle S \setminus \{a\} \rangle \times \langle a \rangle$.

If $\langle S \setminus \{a\} \rangle = G$, then $S \setminus \{a\}$ determines a connected $2k$ -regular integral Cayley graph over G .

If $G \cong \langle S \setminus \{a\} \rangle \times \langle a \rangle$, then $\langle S \setminus \{a\} \rangle$ is of odd order, because the product of two cyclic group is cyclic if and only if they are of co-prime orders. We have $\text{Cay}(G, T) \cong \text{Cay}(\langle S \setminus \{a\} \rangle, S \setminus \{a\}) \times \text{Cay}(\langle a \rangle, \{a\})$, where $T = S \setminus \{a\} \times \{a\}$. Notice that $\text{Cay}(\langle S \setminus \{a\} \rangle, S \setminus \{a\})$ and $\text{Cay}(\langle a \rangle, \{a\}) \cong K_2$ are integral graphs. Since $\langle S \setminus \{a\} \rangle$ has a odd order, Corollary 3.1.8 implies that $\text{Cay}(\langle S \setminus \{a\} \rangle, S \setminus \{a\})$ is a connected non-bipartite Cayley graph. Therefore, $\text{Cay}(G, T)$ is connected, because it is a tensor product of a connected non-bipartite graph with K_2 . Since $|T| = 2k$, we have a $2k$ -regular Cayley graph over G .

Conversely, suppose $\text{Cay}(G, S)$ is a $2k$ -regular integral graph. Assume a is the involution in G . Notice that $a \notin S$, and $\text{Cay}(G, S \cup \{a\})$ is integral. Thus, there is a $2k + 1$ -regular integral Cayley graph over G as well. \square

Theorem 5.1.7. *Suppose G is an abelian group. If there is a connected cubic integral Cayley graph over G , then G is isomorphic with one of the following groups:*

$$\mathbb{Z}_2^2, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_3, \mathbb{Z}_2^3, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2^2 \times \mathbb{Z}_3.$$

Furthermore, each of these groups admits a cubic integral Cayley graph.

Proof. We notice that $|G|$ is even and at least four. If G is cyclic, then according to Theorem 5.1.6 there should be an integral 2-regular graph (cycle) over G . This implies that $|G| = 4, 6$.

Thus, if G is cyclic, then $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. It is easy to see that $\text{Cay}(\mathbb{Z}_4, \mathbb{Z}_4 \setminus \{0\}) = K_4$, $\text{Cay}(\mathbb{Z}_2 \times \mathbb{Z}_3, \{(0, 1), (0, 2), (1, 0)\}) = K_2 \square K_3$ and $\text{Cay}(\mathbb{Z}_2 \times \mathbb{Z}_3, \{(1, 1), (1, 2), (1, 0)\}) = K_{3,3}$. Thus, these groups admit cubic integral Cayley graphs.

If G is non-cyclic, then Lemma 5.1.2 and Theorem 5.1.3 imply $|G| \leq 12$. The set S is either consists of three involutions, or an involution and an element of order 4 or 6 along with its inverse. This implies that $|G| \in \{4, 8, 12\}$. The case $|G| = 12$ happens only when S consists of an involution and an element of order 6 and its inverse. In this case, G is necessarily in the form $G = \mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2^2 \times \mathbb{Z}_3$. We have $\text{Cay}(\mathbb{Z}_2^2 \times \mathbb{Z}_3, \{(1, 0, 1), (1, 0, 2), (1, 1, 0)\}) = K_2 \square C_6$, which gives a cubic integral Cayley graph over this group. If there is no element of order 6 in S , then $|G| \leq 8$, with equality just in the case that S is a symmetric generating set of three involutions, or an involution and an element of order 4 and its inverse. Groups \mathbb{Z}_2^3 and $\mathbb{Z}_2 \times \mathbb{Z}_4$ are the only non-cyclic abelian groups of order 8 with such minimal generating sets. Both are Cayley integral groups:

$$\text{Cay}(\mathbb{Z}_2 \times \mathbb{Z}_4, \{(1, 0), (0, 1), (0, 3)\}) = K_2 \square C_4 = Q_3$$

$$\text{Cay}(\mathbb{Z}_2^3, \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}) = Q_3.$$

The only non-cyclic group of order 4 is \mathbb{Z}_2^2 . Clearly, in this case S can be just $\mathbb{Z}_2^2 - \{0\}$. We have $\text{Cay}(\mathbb{Z}_2^2, \mathbb{Z}_2^2 - \{0\}) = K_4$, which is a cubic integral Cayley graph. \square

Corollary 5.1.8. *If G is a cyclic group and $\Gamma = \text{Cay}(G, S)$ is a connected cubic integral graph, then $G \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_3$, and $\Gamma \cong K_4, K_2 \square K_3$ or $K_{3,3}$.*

Proof. We proved in the previous lemma that \mathbb{Z}_4 and $\mathbb{Z}_2 \times \mathbb{Z}_3$ are the only cyclic groups which admit a cubic integral Cayley graph. We also showed that $K_4, K_2 \square K_3$ and $K_{3,3}$ are connected cubic integral Cayley graphs over cyclic groups. The only cubic integral graph on 4 vertices is K_4 . Thus, if $G \cong \mathbb{Z}_4$, then $\Gamma = K_4$ is the only cubic integral graph over G . Suppose $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. If $\text{Cay}(G, S)$ is cubic integral graph, then Theorem 2.4.4 implies that S is a generating set of G consisting of elements of order 2, 3 or 6. We know a cyclic group has $\phi(k)$ elements of order k . Therefore, there is a unique involution in G which should be in S . All other non-identity elements in G are of orders 3 or 6. Thus, we have just two choices for S . First choice is, $S = \{a, b, b^{-1}\}$, where a is the involution of G , and $\{b, b^{-1}\}$ the set of all elements of order 3 in G . In this case, $\text{Cay}(G, S)$ is isomorphic to $K_2 \square K_3$. Second choice is, $S = \{a, c, c^{-1}\}$, where a is the involution of G , and $\{c, c^{-1}\}$ the set of all elements of order 6 in G . In this case, $\text{Cay}(G, S)$ is isomorphic to $K_{3,3}$. This completes the proof. \square

Corollary 5.1.9. *If Γ is a connected cubic integral Cayley graph of an abelian group, then $\Gamma \cong K_4, K_2 \square K_3, K_{3,3}, Q_3, K_2 \square C_6$.*

Proof. By theorem 2.4.4, if $\text{Cay}(G, S)$ is a connected cubic integral graph over the abelian group G , then S should be a disjoint union of atoms in the Boolean algebra $\mathbb{B}(G)$ of G . Since $|S| = 3$, thus S is either consisting of three involutions, or is in the form $\{a, b, b^{-1}\}$, where a is an involution and b an element of order in $\{3, 4, 6\}$. We have already showed that these graphs are all Cayley graph of an abelian group. It is easy to see that the only Cayley graphs of order 4 or 6 are $K_4, K_2 \square K_3, K_{3,3}$.

Suppose G is an abelian group of order 12 which admits a connected cubic integral Cayley graph. Let $\text{Cay}(G, S)$ be a connected cubic integral Cayley graph over G . From the proof of Theorem 5.1.7 is clear that $S = \{a, b, b^{-1}\}$, where a is an involution and b an element of order 6. Since $G = \langle a \rangle \langle b \rangle$ and $|G| = |\langle a \rangle| |\langle b \rangle|$, we have $G = \langle a \rangle \times \langle b \rangle$. This implies that $\text{Cay}(G, S) = \text{Cay}(\langle a \rangle, \{a\}) \square \text{Cay}(\langle b \rangle, \{b, b^{-1}\}) = K_2 \square C_6$. Thus, $K_2 \square C_6$ is the only connected cubic integral Cayley graph over an abelian group of order 12.

Now, suppose G is an abelian group of order 8, and $\text{Cay}(G, S)$ a connected cubic integral Cayley graph over G . Lemma 5.1.2 implies that S is a minimal generating set of G consisting of elements of orders 2 or 4. If all elements of S are of order 2, then $G \cong \mathbb{Z}_2^3$, and clearly in this case $\text{Cay}(G, S) = Q_3$. Suppose $S = \{a, b, b^{-1}\}$, where a is an involution and b an element of order 4. Since $G = \langle a \rangle \langle b \rangle$ and $|G| = |\langle a \rangle| |\langle b \rangle|$, we have $G = \langle a \rangle \times \langle b \rangle$. This implies that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_4$, and $\text{Cay}(G, S) = \text{Cay}(\langle a \rangle, \{a\}) \square \text{Cay}(\langle b \rangle, \{b, b^{-1}\}) = K_2 \square C_4$. We notice that $K_2 \square C_4 = Q_3$. This completes the proof. \square

Theorem 5.1.10. *Let G be an abelian group. If there is a connected 4-regular integral Cayley graph over G , then G is isomorphic to one of the following groups:*

cyclic groups $\mathbb{Z}_5, \mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_{10}, \mathbb{Z}_{12}$, or any abelian non-cyclic group of order 8, 9, 12, 16, 18, 24, 36, other than $\mathbb{Z}_2^2 \times \mathbb{Z}_9$ and $\mathbb{Z}_2 \times \mathbb{Z}_8$.

Proof. Suppose $\text{Cay}(G, S)$ is an integral 4-regular connected Cayley graph. We notice that S should be in the Boolean algebra of the subgroups, thus it is a union of disjoint atoms. Each atom $[g]$ in $\mathbb{B}_G(G)$ contains $\phi(\text{ord}(g))$ elements. This implies that S cannot contain any element g with $\phi(\text{ord}(g)) > 4$. If $g \in S$ and $\phi(\text{ord}(g)) = 4$, then $S = [g]$ and $G = \langle g \rangle$ is a cyclic group.

We now first classify all the cyclic groups which admit a connected 4-regular integral Cayley graph. We know that $\phi(n) = 4$ if and only if $n \in \{5, 8, 10, 12\}$. Suppose $G = \langle g \rangle$ is a

cyclic group, which admits a connected 4-regular integral Cayley graph $\text{Cay}(G, S)$. Each atom $[a]$ in the boolean algebra, has $\phi(\text{ord}(a))$ elements. This implies that if a is not an involution, then $[a]$ is of even size. We also notice that in a cyclic group, we have at most one involution, and so S cannot contain an involution. By Theorem 2.4.4, S is either one single atom $[s]$, or a union of two atoms $[s_1]$ and $[s_2]$, where $\text{ord}(s_1) \neq \text{ord}(s_2) \in \{3, 4, 6\}$. Notice that if $S = [s_1] \cup [s_2]$, then $|G| \in \{6, 12\}$. If S consist of a single atom $[s]$, then $G = \langle s \rangle$ and $|G| \in \{5, 8, 10, 12\}$. Notice that if $G = \langle g \rangle$ is a cyclic group of order in $\{5, 8, 10, 12\}$, then we take S to be the atom containing the generator g . Clearly, S is a symmetric generator set of G which belongs to the Boolean algebra $\mathbb{B}(G)$ of G . Thus, cyclic groups $\mathbb{Z}_5, \mathbb{Z}_8, \mathbb{Z}_{10}, \mathbb{Z}_{12}$ admit connected 4-regular integral Cayley graphs. If $G = \mathbb{Z}_6$, then the only choice for S is $[1] \cup [2] = \{1, 2, 4, 5\}$. Notice that we have,

$$\begin{aligned} \text{Cay}(\mathbb{Z}_5, \mathbb{Z}_5 \setminus \{0\}) &= K_5, & \text{Cay}(\mathbb{Z}_6, \{1, 2, 4, 5\}) &= \overline{3K_2} = K_{2,2,2}, & \text{Cay}(\mathbb{Z}_8, \{1, 3, 5, 7\}) &= K_{4,4} \\ \text{Cay}(\mathbb{Z}_{10}, \{1, 3, 7, 9\}) &= \overline{K_5 \square K_2}, & \text{Cay}(\mathbb{Z}_{12}, \{1, 5, 7, 11\}) &= \overline{3C_4}. \end{aligned}$$

Now suppose G is a non-cyclic abelian group of order at least five. Then S is a disjoint union of at least two atoms of $\mathbb{B}(G)$. Since $|S| = 4$, S should be the union of two, three or four atoms.

Suppose S is the disjoint union of two 2-element atoms $[g_1]$ and $[g_2]$. Then $G = \langle g_1 \rangle \langle g_2 \rangle$, and $|G|$ divides $|\langle g_1 \rangle| |\langle g_2 \rangle|$. Since $[g_1]$ and $[g_2]$ are atoms of size 2, thus $\text{ord}(g_1)$ and $\text{ord}(g_2)$ are 3, 4 or 6. This implies $|G| \in \{6, 8, 9, 12, 16, 18, 24, 36\}$. Suppose S is the disjoint union of three atoms $[g_1]$, $[g_2]$ and $[g_3]$. Then, we may assume g_1 and g_2 are involutions and g_3 an element of order 3, 4 or 6. We have that $G = \langle g_1 \rangle \langle g_2 \rangle \langle g_3 \rangle$, and $|G|$ divides $|\langle g_1 \rangle| |\langle g_2 \rangle| |\langle g_3 \rangle|$. This case implies that $|G| \in \{6, 8, 12, 16, 24\}$. If S is a disjoint union of four atoms $[g_1]$, $[g_2]$, $[g_3]$ and $[g_4]$. Then g_1, g_2, g_3 and g_4 are necessarily involutions. Thus, $|G| \mid 16$. Since $|G| \geq 5$, we have $|G| \in \{8, 16\}$.

All abelian groups of order 6, 8, 9, 12 and 18 are Cayley integral groups (see Theorem 4.3.2) containing 4-element symmetric generating sets. Thus we need to check the case where G is a group of order 16, 24 or 36.

If $|G| = 16$, then G contains no element of order 6. Thus, Lemma 5.1.2 implies that S is a set of elements of orders 2 or 4. If $G = \mathbb{Z}_2^4$ or \mathbb{Z}_4^2 , then G contains a generating set of four involutions. Since $G = \mathbb{Z}_2 \times \mathbb{Z}_8$ has three involutions, and cannot be generated by a set of elements of order 2 and 4, there is no connected 4-regular integral Cayley graph over $\mathbb{Z}_2 \times \mathbb{Z}_8$.

Suppose now $|G| = 24$. Lemma 5.1.2 implies that $S = [g_1] \cup [g_2]$, where $\text{ord}(g_1) = 6$ and $\text{ord}(g_2) = 4$, or $S = [g_1] \cup [g_2] \cup [g_3]$, where $\text{ord}(g_1) = 6$ and $\text{ord}(g_2) = \text{ord}(g_3) = 2$. Thus $G \cong \mathbb{Z}_6 \times \mathbb{Z}_4$ or $\mathbb{Z}_6 \times \mathbb{Z}_2^2$. We have $\text{Cay}(\mathbb{Z}_6 \times \mathbb{Z}_4, \{(1, 0), (5, 0), (0, 1), (0, 2)\}) = C_6 \square C_4$. We notice that $\mathbb{Z}_6 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_2^3 \times \mathbb{Z}_3$ is a Cayley integral group (see Theorem 4.3.2) which has a symmetric generating set of four elements, $\text{Cay}(\mathbb{Z}_2^3 \times \mathbb{Z}_3, \{(1, 0, 1), (0, 1, 1), (1, 0, 5), (1, 1, 5)\}) \cong C_4 \square C_6$.

If $|G| = 36$, then $S = [g_1] \cup [g_2]$, where $\text{ord}(g_1) = \text{ord}(g_2) = 6$. We have $G = \langle g_1 \rangle \times \langle g_2 \rangle$, thus $G \cong \mathbb{Z}_6 \times \mathbb{Z}_6$. We have $\text{Cay}(\mathbb{Z}_6 \times \mathbb{Z}_6, \{(1, 1), (1, 5), (5, 1), (5, 5)\}) = C_6 \square C_6$. Notice that $\mathbb{Z}_2^2 \times \mathbb{Z}_9 \not\cong \mathbb{Z}_6 \times \mathbb{Z}_6$, thus $\mathbb{Z}_2^2 \times \mathbb{Z}_9$ cannot have a connected 4-regular integral Cayley graph. This completes the proof. \square

Theorem 5.1.11. *Let G be an abelian group of even order. There is a connected $(2k + 1)$ -regular integral Cayley graph over G if and only if G admits a connected $2k$ -regular integral Cayley graph or $G = H \times \mathbb{Z}_2$, where H is a group admitting a connected $2k$ -regular integral Cayley graph.*

Proof. Suppose G is a group of even order, and G admits a connected $2k$ -regular integral Cayley graph. Suppose S is a symmetric generating set of G of size $2k$ such that $\text{Cay}(G, S)$ is integral. We know that S is in the Boolean algebra of the subgroups. Each atom in the boolean algebra of subgroups, has even size unless it is a singleton atom consisting of an involution. Since $|S| = 2k$, the number of involutions in S is even. We notice also any group of even order has odd number of involutions. Therefore G has an involution which is not a member of S . Suppose a is an involution that $a \notin S$. Now $\text{Cay}(G, S \cup \{a\})$ is a connected $(2k + 1)$ -regular integral Cayley graph over G .

Suppose H is a group which admits a connected $2k$ -regular integral Cayley graph Γ . Lemma 5.1.5 implies that $\Gamma \square K_2$ is a $(2k + 1)$ -regular integral Cayley graph over $H \times \mathbb{Z}_2$.

Conversely, suppose G is an even group which admits a connected $(2k + 1)$ -regular integral graph $\text{Cay}(G, S)$. Since $|S| = 2k + 1$, S contains an involution. Suppose a is an involution in S , then we have $G = \langle S \setminus \{a\} \rangle \langle a \rangle$. There are two cases to consider. First suppose $a \in \langle S \setminus \{a\} \rangle$, then clearly $G = \langle S \setminus \{a\} \rangle$. In this case, we have $\text{Cay}(G, \langle S \setminus \{a\} \rangle)$ which is a connected $2k$ -regular integral graph. The second case corresponds to $a \notin \langle S \setminus \{a\} \rangle$. In this case, $G = \langle S \setminus \{a\} \rangle \times \mathbb{Z}_2$. Suppose $H = \langle S \setminus \{a\} \rangle$. Then, H admits a connected $2k$ -regular integral graph $\text{Cay}(H, S \setminus \{a\})$. \square

Corollary 5.1.12. *Suppose $\{G_j\}_{j \in J} \cup \{H_i\}_{i \in I}$ is the collection of all abelian groups admitting connected $2k$ -regular integral Cayley graphs (I and J are the index sets), where H_i for $i \in I$ is*

of odd order and G_j for $j \in J$ of even order. Then the collection of abelian groups admitting connected $(2k + 1)$ -regular integral Cayley graphs is:

$$\{G_j\}_{j \in J} \cup \{G_j \times \mathbb{Z}_2\}_{j \in J} \cup \{H_i \times \mathbb{Z}_2\}_{i \in I}.$$

Therefore, classification of all abelian groups admitting connected integral Cayley graphs of odd degree is essentially reduced to the even degree case. The method used in the proof of Theorem 5.1.10, can be employed to classify all abelian groups admitting connected s -regular integral Cayley graphs for $s = 6, 8, \dots$. However, it is not easy to classify all abelian groups admitting connected s -regular integral Cayley graphs, when s is a big number. This is due to the fact that there is not an easy classification of the solutions of the equation $\phi(x) = a$, for a given positive even integer a .

5.2 Non-abelian groups admitting cubic integral Cayley graphs

The following Theorem due to Schwenk has been proved in [51].

Theorem 5.2.1 (Schwenk). *If Γ is a connected cubic integral graph, then Γ is isomorphic to one of the graphs $\Gamma_1, \Gamma_2, \dots, \Gamma_{13}$ in Figures 5.1 and 5.2.*

Lemma 5.2.2. *Suppose n is odd, and S is a symmetric generating set of D_n . If $\text{Cay}(D_n, S)$ is bipartite, then S is a set of involutions.*

Proof. To have $\text{Cay}(D_n, S)$ bipartite, we need to have a linear character which sends each element of S to -1 . When n is odd, D_n has only one non-principal linear character, which assign -1 to each reflection and 1 to each rotation. Thus S should be a set of reflections, and consequently a set of involutions. \square

Lemma 5.2.3. *Suppose $G = H \times K$ with $|H| \notin \{1, 2, 3, 4, 6\}$. If there is a connected cubic integral Cayley graph over G , then there is a connected cubic integral Cayley graph over H .*

Proof. Part 10 of Theorem 3.2.8 implies that $\text{Cay}(H, \pi_H(S))$ is integral. If $|\pi_H(S)| = 1$, then $H = \langle h \rangle$ is a cyclic group, where $\pi_H(S) = \{h\}$. Because $\text{Cay}(H, \pi_H(S))$ is integral, each character of the group maps h to a rational number. This implies that $|H| = 1$ or 2 , which contradicts the hypothesis. If $|\pi_H(S)| = 2$, then $\text{Cay}(H, \pi_H(S))$ is a connected integral 2-regular graph. This implies that $|H| \in \{3, 4, 6\}$, which again contradicts the hypothesis. Therefore, the only possible case is that $|\pi_H(S)| = 3$, and so $\text{Cay}(H, \pi_H(S))$ is a connected cubic integral graph over H . \square

Lemma 5.2.4. *Graphs $\Gamma_3, \Gamma_6, \Gamma_{10}$ and Γ_{11} , in Figures 5.1 and 5.2 are not Cayley graphs.*

Proof. Graph Γ_6 is not vertex-transitive, and so not a Cayley graph. There is no integral Cayley graph on \mathbb{Z}_{10} , and \mathbb{Z}_{10} is the only abelian group of order 10. There is just one non-abelian group of order 10, namely the dihedral group D_5 . Suppose S is a symmetric generating set of D_5 . If $\text{Cay}(D_5, S)$ is integral, then Theorem 3.5.5 implies that $|S| \geq 4$. Hence, there is no connected cubic integral Cayley graph over D_5 . Therefore, graphs Γ_{10} and Γ_{11} which each has 10 vertices, cannot be integral Cayley graphs. Suppose Γ_3 is a Cayley graph of a group G . Then G is isomorphic to $D_{15}, \mathbb{Z}_3 \times D_5$ or $\mathbb{Z}_5 \times D_3$. From character table of D_{15} is clear that all non-simple eigenvalues are of even multiplicity. Graph Γ_3 has eigenvalue 2 with multiplicity 9, thus Γ_3 is not a Cayley graph of D_{15} . If Γ_3 was a Cayley graph of $\mathbb{Z}_3 \times D_5$, then Lemma 5.2.3 implies that there is a connected cubic integral Cayley graph over D_5 , which is not possible. Suppose $G \cong \mathbb{Z}_5 \times D_3$. Lemma 5.2.3 implies that there is a connected cubic integral Cayley graph over \mathbb{Z}_5 , which is not possible by Theorem 5.1.7. Then Γ_3 is not a Cayley graph and this completes the proof. \square

Lemma 5.2.5. *Graphs Γ_4 and Γ_5 , in Figures 5.1 and 5.2 are not Cayley graphs.*

Proof. The girth of both Γ_4 and Γ_5 is 6. This implies that if one of these graphs is in the form $\text{Cay}(G, S)$, then S cannot have any element of order 4 or 5. Non-abelian groups of order 20 are $D_{10} = D_5 \times \mathbb{Z}_2, \mathbb{Z}_5 \times \mathbb{Z}_4$ and the Frobenius group with presentation $\langle s, t \mid s^4 = t^5 = 1, ts = st^2 \rangle$. The Frobenius group cannot be generated by involutions, and it has no element of order 10, thus there is no bipartite connected cubic graph over it. Group $\mathbb{Z}_5 \times \mathbb{Z}_4$ has no symmetric generating set with three elements avoiding elements of order 4 and 5. If $G = D_{10} = D_5 \times \mathbb{Z}_2$, then $\text{Cay}(D_5, \pi_{D_5}(S))$ is integral. This is not possible by Lemma 5.2.3. \square

Theorem 5.2.6. *If G is a non-abelian group, then there is a connected cubic integral Cayley graph over G if and only if G is one of the following groups;*

$$D_3, D_4, D_6, A_4, S_4, A_4 \times \mathbb{Z}_2, D_4 \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_4.$$

Furthermore, each of these groups has a connected cubic integral Cayley graph.

Proof. By Schwenk's Theorem, possible connected integral Cayley graphs are of orders:

$$4, 6, 8, 9, 10, 12, 20, 24, 30.$$

By Lemmas 5.2.4 and 5.2.5 and the fact that we are considering non-abelian groups, the possible orders reduce to 6, 8, 12, 24. The only non-abelian group of order 6 is $D_3 = S_3$, which is a Cayley integral group. Clearly, D_3 has symmetric generating sets of size three.

If $|G| = 8$, then $G = D_4$ or $G = Q_8$. We showed in Lemma 4.2.5 that $\text{Cay}(D_4, \{x, x^3, y\})$ is the 3-cube. The quaternion group Q_8 has a unique involution, and all other non-identity elements are of order 4. Since Q_8 cannot be generated by an involution and an element of order 4, thus Q_8 has no cubic integral Cayley graph.

If G is a non-abelian group of order 12, then $G \cong D_6, A_4, \text{Dic}_{12}$. Group Dic_{12} has a unique involution. Since this involution is central, Dic_{12} cannot be generated by an involution and an element of order less than 12. Since Dic_{12} is non-abelian, it has no element of order 12. Consequently, it has no cubic integral Cayley graph. For $G \cong D_6$, we have $\text{Cay}(D_6, \{x, x^5, y\}) = K_2 \square C_6$. If $G \cong A_4$ and $S = \{(12)(34), (123), (132)\}$, then $\text{Cay}(A_4, S)$ is isomorphic to the graph Γ_{13} in the Figure 5.2. This completes the proof for non-abelian groups of order 12.

Now, suppose G is a non-abelian group of order 24. There are 12 such groups:

$$S_4, A_4 \times \mathbb{Z}_2, D_4 \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_4, \mathbb{Z}_3 \times Q_8, \mathbb{Z}_3 \rtimes Q_8, \mathbb{Z}_3 \rtimes \mathbb{Z}_8, \text{SL}_2(\mathbb{Z}_3), \\ D_{12}, \text{Dic}_{12} \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times S_3 = D_6 \times \mathbb{Z}_2, (\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2.$$

To analyze this case, all necessary information about non-abelian groups of order 24 has been provided in Appendix A. We show that from this list, groups $S_4, A_4 \times \mathbb{Z}_2, D_4 \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_4$ admit connected cubic integral Cayley graphs, while the rest of the groups in the list do not admit such Cayley graphs. Note that by Schwenk's theorem, the only possible connected cubic integral Cayley graph on 24 vertices is Γ_8 .

If $G = S_4$, then $S = \{(12), (13), (14)\}$ is a generating set. One can easily check that $\text{Cay}(S_4, S) = \Gamma_8$. If $G = A_4 \times \mathbb{Z}_2$, then since Γ_{13} is a Cayley graph over A_4 , we have $\Gamma_8 = \Gamma_{13} \times K_2$ is a Cayley graph over $A_4 \times \mathbb{Z}_2$ (see Lemma 5.1.5). If $G = D_4 \times \mathbb{Z}_3$, then $\text{Cay}(G, \{(x, 1), (x^3, 2), (y, 0)\})$ is a connected cubic integral. If $G = D_3 \times \mathbb{Z}_4$, then $\text{Cay}(G, \{(x, 1), (x^2, 2), (y, 0)\})$ is a connected cubic integral graph over this group.

In the groups $\mathbb{Z}_3 \times Q_8, \mathbb{Z}_3 \rtimes Q_8, \mathbb{Z}_3 \rtimes \mathbb{Z}_8$ and $\text{SL}_2(\mathbb{Z}_3)$ there is a unique involution, and it belongs to the center of the group. Therefore, these groups can not be generated by an involution and an element of order less than 24. Since these groups are non-abelian, there is no element of order 24 in any of them. Consequently, there is no connected cubic integral Cayley graph over any of these groups.

For all other non-abelian groups of order 24, we look for a symmetric generating set of size three containing no element of order 3 or 4 (since Γ_8 has girth 6). Because Γ_8 is bipartite, we notice that each element of the generating set should be mapped to -1 by an irreducible linear character of the group.

The only rotation of order 2 in D_{12} is a^6 (see 3.5). This element will map to 1 by all linear representations of D_{12} (see 3.5.1). Therefore, if $\text{Cay}(D_{12}, S)$ is a connected cubic integral graph, then S should consist of three reflections of D_{12} . Using the linear character of D_{12} (see 3.5.1), this implies that 3 and -3 have multiplicities greater than 1 which is not possible. That is to say, there is no connected cubic integral Cayley graph over D_{12} .

By Lemma 5.2.3, if there is a connected cubic integral Cayley graph $\text{Cay}(D_6 \times \mathbb{Z}_2, S)$, then $\text{Cay}(D_6, \pi_{D_6}(S))$ should be a connected cubic integral Cayley graph as well. It is easy to see that $\text{Cay}(D_6, \pi_{D_6}(S))$ should be bipartite, but this implies that $\text{Cay}(D_6 \times \mathbb{Z}_2, S)$, which is a tensor product (see Lemma 5.1.5) of two bipartite graphs is disconnected. This contradiction implies that $\text{Cay}(D_6 \times \mathbb{Z}_2, S)$ does not admit a connected cubic integral Cayley graph.

We can apply Lemma 5.2.3 once more to eliminate $\text{Dic}_{12} \times \mathbb{Z}_2$, because Dic_{12} does not admit a connected cubic integral Cayley graph.

The only remaining group is the group $(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ which is a solvable group with 9 conjugacy classes. One can check with character table and corresponding representations that from all symmetric generating sets of size 3 of this group, the obtained Cayley graph is not an integral graph. All the calculations for this group has been done in Appendix B.3. \square

5.3 Non-abelian groups admitting 4-regular integral Cayley graphs

Now, we explain a method which was originally used by A.J. Schwenk in proving Theorem 5.2.1. While he used no computer help to prove his theorem, the adopted method for the 4-regular graphs needs lots of computations, and therefore computer help seems inevitable.

If Γ is a non-bipartite connected 4-regular integral graph, then the product $\Gamma \times K_2$ is connected, bipartite, 4-regular and integral. Therefore, in determining 4-regular integral graphs we can consider bipartite graphs only, and later extract non-bipartite graphs from the decompositions of bipartite ones in the form $\Gamma \times K_2$. Suppose that Γ is a 4-regular bipartite integral graph with $2n$ vertices. We may write the spectrum of Γ in the form

$[4, 3^x, 2^y, 1^z, 0^{2w}, -1^z, -2^y, -3^x, -4]$. Cvetković et al. [24] found quadruples $[x, y, z, w]$ that give candidates for the spectrum of a bipartite 4-regular connected integral graph. They called these “possible spectra”. Research activities regarding the set of possible spectra fall into two streams: eliminate possible spectra based on new information and/or techniques, or find graphs that realize a possible spectrum. Useful tools include an identity by Hoffman [31] and equations relating the spectral moments to the closed walks of length $l \leq 6$. All bipartite 4-regular connected integral graph that avoid eigenvalues of ± 3 and realize a possible spectrum are found in [54]. Stevanović [53] eliminates spectra using equations arising from graph angles. In the same paper he determines that the possible values for n are between 4 and 630, but for 5 exceptions. For a subgraph X of a graph Γ , suppose $[X]$ denotes the number of copies of X in Γ . The number of closed walks of length k in a 4-regular graph is expressible in terms of n , $[C_i]$ and some other subgraphs of Γ . The Diophantine equations below are well-known:

$$\frac{1}{2} \sum_i \lambda_i^0 = 1 + x + y + z + w = n,$$

$$\frac{1}{2} \sum_i \lambda_i^2 = 16 + 9x + 4y + z = 4n,$$

$$\frac{1}{2} \sum_i \lambda_i^4 = 256 + 81x + 16y + z = 28n + 4[C_4],$$

$$\frac{1}{2} \sum_i \lambda_i^6 = 4096 + 729x + 64y + z = 232n + 72[C_4] + 6[C_6].$$

Minchenko and Wanless [43] extended these equations to higher moments.

$$\begin{aligned} \frac{1}{2} \sum_i \lambda_i^8 = & 65536 + 6561x + 256y + z = 2092n + 1012[C_4] + 144[C_6] + 8[C_8] + 16[C_{4.4}] \\ & + 48[\Theta_{2,2,2,2}] + 24[\Theta_{2,2,2}] + 8[\Theta_{3,3,1}] \end{aligned}$$

In the equation above, $C_{i,j}$ denotes an i -cycle and a j -cycle sharing a vertex, and $\Theta_{i_1, i_2, \dots, i_k}$ denotes two vertices joined by internally disjoint paths of lengths i_j for $j = 1, \dots, k$. A vertex-transitive graph has the same number of k -cycles incident with each vertex, so the number of vertices divides $k[C_k]$. This idea has been implemented in some computer programs by Minchenko and Wanless [44] to eliminate those spectra among the possible spectra (of 4-regular bipartite connected integral graphs) which cannot be realized by a vertex-transitive graph. As a consequence, they managed to find all 4-regular bipartite connected Cayley integral graphs.

Theorem 5.3.1. *Suppose G is a finite group and S a generating symmetric set of size 4 in G . If $\text{Cay}(G, S)$ is integral, then G is a group such that:*

$$|G| \in \{5, 6, 8, 9, 10, 12, 16, 18, 20, 24, 30, 32, 36, 40, 48, 60, 72, 120\}.$$

Furthermore, there are precisely 17 isomorphism classes of connected 4-regular bipartite Cayley integral graphs.

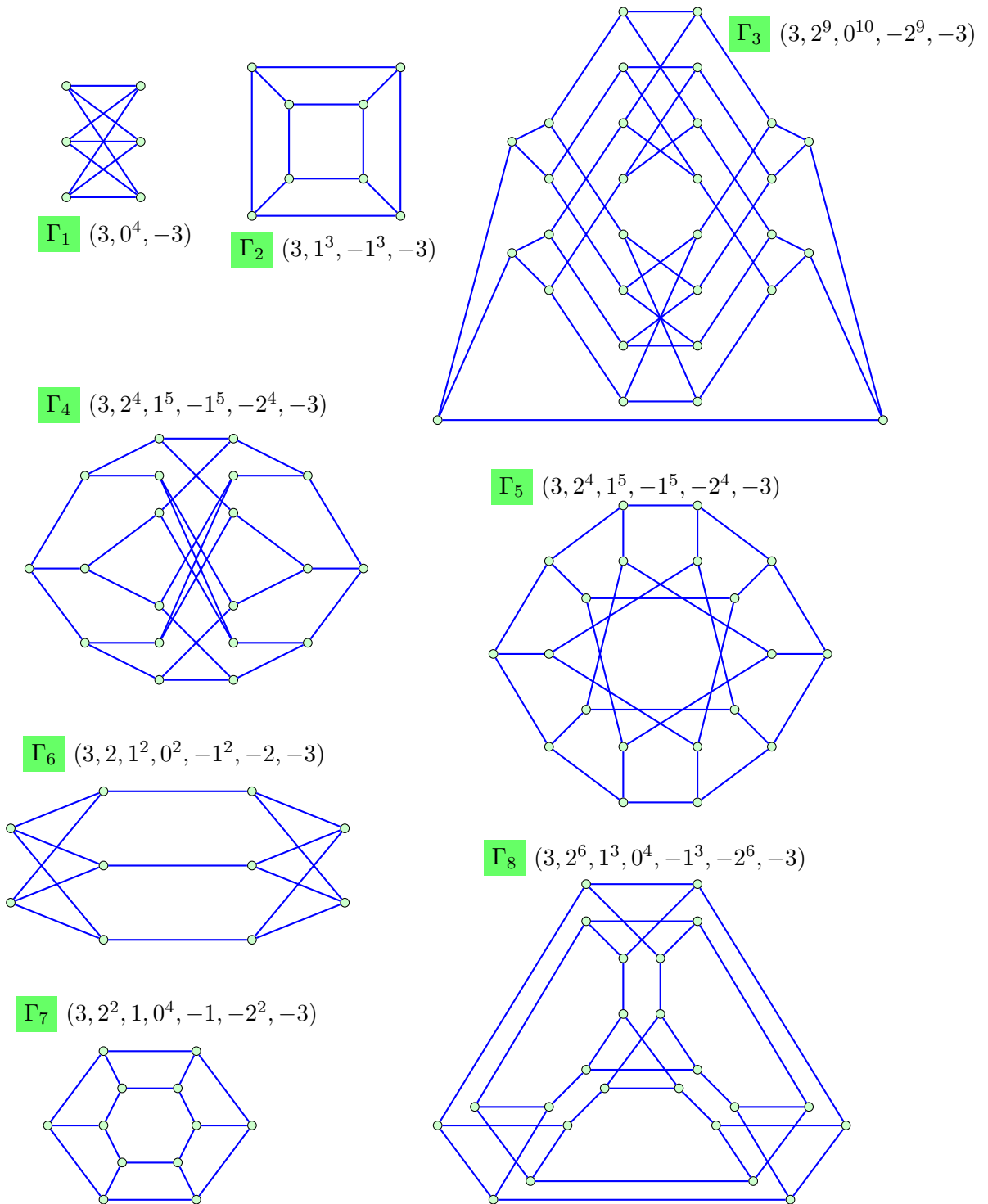


Figure 5.1: Connected cubic bipartite integral graphs.

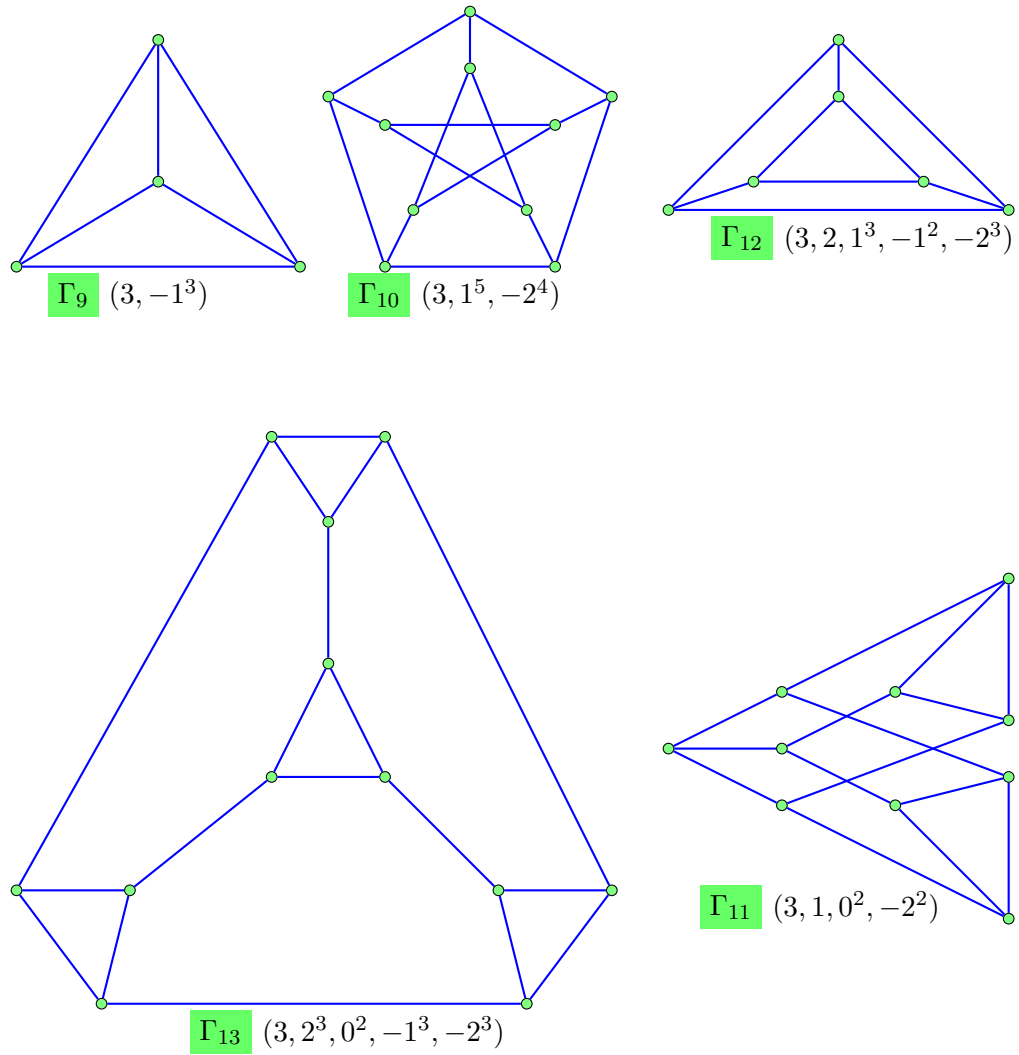


Figure 5.2: Connected cubic non-bipartite integral graphs.

Chapter 6

Miscellaneous results

In the first section of this chapter, we will study graphs with a small number of distinct eigenvalues. In the second section, we will study simple eigenvalues in Cayley graphs. In the last section, we propose some open problems and two conjectures.

6.1 Cayley graphs with small number of distinct eigenvalues

If Γ is a connected graph with exactly two distinct eigenvalues, then Γ is a complete graph (see Theorem 2.1.3). The situation is not trivial for more than two distinct eigenvalues. Let Γ be a graph which is neither empty nor complete. Then Γ is said to be a *strongly regular graph* with parameters (n, k, λ, μ) if Γ is a k -regular graph on n vertices in which every pair of adjacent vertices have λ common neighbors and every pair of non-adjacent vertices have μ common neighbors. The cycle C_4 is a (bipartite) strongly regular graph with parameters $(4, 2, 0, 2)$. The cycle C_5 is a (non-bipartite) strongly regular graph with parameters $(5, 2, 0, 1)$. It is easily seen that for any $n \geq 6$ the cycle C_n is not a strongly regular graph. The Petersen graph and the cocktail party graphs are two other examples of strongly regular graphs. Note that the complement of a strongly regular graph is also strongly regular.

Theorem 6.1.1. *For a simple graph Γ of order n , not complete or empty, with adjacency matrix A , the following are equivalent:*

- (i) Γ is strongly regular with parameters (n, k, λ, μ) for certain integers k, λ, μ .
- (ii) $A^2 = (\lambda - \mu)A + (k - \mu)I + \mu J$ for certain real numbers k, λ, μ .

(iii) $AJ = JA$ and A has precisely three distinct eigenvalues.

Thus, connected regular graphs with three distinct eigenvalues are precisely strongly regular graphs. Moreover, the eigenvalues determine the parameters, and vice versa.

Theorem 6.1.2. *Let Γ be a strongly regular graph with adjacency matrix A and parameters (n, k, λ, μ) . Let k, r and s ($k > r > s$) be the distinct eigenvalues of A with multiplicities 1, f and g respectively. Then*

$$(i) \quad k(k-1-\lambda) = \mu(n-k-1),$$

$$(ii) \quad rs = \mu - k, \quad r + s = \lambda - \mu, \quad \text{and}$$

$$(iii) \quad f, g = \frac{1}{2}(n-1 \mp \frac{(r+s)(n-1)+2k}{r-s}).$$

Lemma 6.1.3. *Let Γ be a connected k -regular graph on n vertices with three distinct eigenvalues. If not all eigenvalues are integral, then n is odd and $k = \frac{n-1}{2}$.*

Proof. The minimal polynomial of Γ has integer coefficients, and we know that $\lambda_1 = k$ is an integer. Thus, r and s should be in the form $\frac{a \pm \sqrt{b}}{2}$, for some integers a and b . Since r and s are conjugate algebraic integers, their multiplicities in the characteristic polynomial of Γ should be equal to each other. We have $1 + f + g = 1 + 2f = n$. Thus $f = \frac{n-1}{2}$. We know that the sum of the eigenvalues is zero. Thus, $k + a\frac{n-1}{2} = 0$. This can happen only if $k = \frac{n-1}{2}$ and $a = -1$. \square

The following conjecture due to Pablo Spiga, has find some attention.

Conjecture 6.1.4. *There exists no (non-complete and non-empty) strongly regular Cayley graph Γ , where $\Gamma = \text{Cay}(G, S)$, G is a non-abelian simple group and $\text{Aut}(\Gamma)$ is primitive on the vertices.*

By a theorem of Liebeck-Praeger-Saxl (Theorem 1.6 of the [41]), if such a Cayley graph exist, then S should be a union of conjugacy classes. We prove that such a graph is integral, and S should be in the boolean algebra of the subgroups.

Theorem 6.1.5. *Suppose $\Gamma = \text{Cay}(G, S)$, where G is a non-abelian simple group and $\text{Aut}(\Gamma)$ is primitive on the vertices. If Γ is a strongly regular graph, then Γ is an integral graph and S should be in the boolean algebra of subgroups.*

Proof. By Feit-Thompson's odd order theorem, every finite group of odd order is solvable. Thus, if G is a non-abelian simple group, it should be of even order. Lemma 6.1.3 implies that $\Gamma = \text{Cay}(G, S)$ is an integral graph. Thus, S is χ -integral subset of G and Theorem 3.2.7 along with the fact that S is a union of conjugacy classes proves that $S \in \mathbb{B}(G)$. \square

6.2 Simple eigenvalues in Cayley graphs

In this section we study simple eigenvalues in Cayley graphs. An automorphism of a graph Γ is a permutation π of $V(\Gamma)$ such that $A(\Gamma) = [a_{uv}] = [a_{\pi(u)\pi(v)}]$.

Theorem 6.2.1. *Suppose Γ is a connected graph.*

- i) *If all eigenvalues are simple, then $\text{Aut}(\Gamma)$ is an elementary abelian 2-group.*
- ii) *If Γ is vertex-transitive and all its eigenvalues are simple, then Γ has at most two vertices.*

If G is a non-abelian group, then from Theorem 3.1.3 it is clear that each non-linear character will produce multiple eigenvalues. Therefore, all simple eigenvalues of $\text{Cay}(G, S)$ are among numbers $\lambda(S)$, where λ is an irreducible linear character of G . Each linear character of G is a character of G/G' . We can therefore consider only the Cayley multigraphs over abelian groups.

Theorem 6.2.2. *Let G be a finite group and S a symmetric subset of G . All simple eigenvalues of $\text{Cay}(G, S)$ are integers, and the number of simple eigenvalues of $\text{Cay}(G, S)$ is at most $n_2(G) + 1$, where $n_2(G)$ is the number of subgroup of index 2 in G .*

Proof. Suppose λ is a simple eigenvalue of $\text{Cay}(G, S)$, and $\mathbf{x} = (x(g))_{g \in G}$ is the associated eigenvector with $x(1) = 1$. Let us assume that $\lambda \neq |S|$. Consequently, \mathbf{x} is not j . If h is an element in G , then r_h is in $\text{Aut}(\text{Cay}(G, S))$. Let P_h denote the permutation matrix corresponding to the automorphism r_h . We have $P_h A = A P_h$, where A is the adjacency matrix of the $\text{Cay}(G, S)$. This implies that $P_h \mathbf{x}$ is an eigenvector of λ as well. Notice that $P_h \mathbf{x} = (x(gh))_{g \in G}$, that is to say, P_h permutes the components of \mathbf{x} according to the permutation r_h . Since λ is a simple eigenvalue, we have $P_h \mathbf{x} = a \mathbf{x}$ for a scalar a . We know that P_h preserves the length of vectors, thus $a = \pm 1$. So far, we have deduced that for every $h \in G$, we have $P_h \mathbf{x} = \pm \mathbf{x}$. Notice that if h is of odd order, then $P_h \mathbf{x} = \mathbf{x}$. Let $N(\lambda)$ be the set of those h in G which satisfy $P_h \mathbf{x} = \mathbf{x}$. Clearly the map $h \mapsto a_h$, where $P_h \mathbf{x} = a_h \mathbf{x}$, is

a homomorphism from G to the subgroup $\{1, -1\}$ of the multiplicative group of complex numbers. $N(\lambda)$ is the kernel of this homomorphism, and thus $N(\lambda)$ is a subgroup of index at most 2 in G . We notice that for the eigenvector $\mathbf{x} = (x(g))_{g \in G}$, we have $x(g) = 1$ if $g \in N(\lambda)$ and -1 otherwise. Therefore, $\lambda = 2|N(\lambda) \cap S| - |S| \in \mathbb{Z}$. We have $N(\lambda) = G$ if and only if $\lambda = |S|$. Thus when $\lambda \neq |S|$, each simple eigenvalue is associated with a unique subgroup of index 2 in G . Thus, the number of simple eigenvalues in $\text{Cay}(G, S)$ is at most $n_2(G) + 1$, where $n_2(G)$ is the number of subgroups of index 2 in G . \square

For any group G , we denote by G^2 the subgroup generated by the squares of elements, that is $G^2 = \langle \{x^2 \mid x \in G\} \rangle$. We say that G is generated by squares if $G = G^2$. Note that G^2 is normal in G . This is clear because, for every $x, a \in G$, $a^{-1}x^2a = (a^{-1}xa)^2$. Since every element of odd order in G satisfies an equation like $a = a^{2k}$, all elements of odd order are in G^2 .

Theorem 6.2.3. *The groups G and G/G^2 have the same number of subgroups of index 2.*

Proof. To see this, we start with the following observation: if H is a subgroup of index 2 in G , then H is normal in G and the factor group G/H has order 2. Therefore, $(xH)^2 = H$ for all $x \in G$. It follows that $G^2 \subseteq H$. Since G^2 is normal in G , then it is normal in H and we can consider the factor group H/G^2 . This is a subgroup of G/G^2 and we have $[G/G^2 : H/G^2] = [G : H] = 2$. We have a map from the set of subgroups of G of index 2 to the set of subgroups of G/G^2 of index 2 by sending H to H/G^2 . It is easy to check that this is a well defined bijection. \square

Notice that G/G^2 is abelian since $(xG^2)^2 = G^2$ for all $x \in G$. Therefore, G/G^2 is an elementary abelian 2-group. Let us assume that $G/G^2 \cong \mathbb{Z}_2^n$.

In addition to being a group, \mathbb{Z}_2^n has a natural structure of a vector space over \mathbb{Z}_2 with vector addition being the usual group addition and scalar multiplication defined in the natural way across components. Moreover, the subspaces and the subgroups of \mathbb{Z}_2^n coincide. Finally, we notice that subgroups of index 2 (and so order 2^{n-1}) correspond to subspaces of dimension $n - 1$. Recall that an $(n - 1)$ -dimensional subspace of an n -dimensional vector space V is called a hyperplane of V . We now count the hyperplanes of finite dimensional vector spaces over \mathbb{Z}_2 .

Theorem 6.2.4. *Every n -dimensional vector space over \mathbb{Z}_2 has 2^{n-1} hyperplanes.*

Proof. Every hyperplane is determined by choosing $n-1$ independent vectors of the space. So, one can count the number of sets with k independent vectors to be $(2^n - 1)(2^n - 2) \dots (2^n - 2^k)$. Since every hyperplane has dimension $n - 1$, it has $(2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - 2^{n-2})$ bases with $n - 1$ vectors. Thus the number of hyperplanes in \mathbb{Z}_2^n is:

$$\frac{(2^n - 1)(2^n - 2) \dots (2^n - 2^{n-2})}{(2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - 2^{n-2})} = 2^n - 1.$$

□

Thus, if G is a group of order $2^n m$, where m is odd, then $\text{Cay}(G, S)$ has at most 2^n simple eigenvalues. Notice that for any subgroup H of index 2 in G we have a unique eigenvalue and eigenvector associated with H . If \mathbf{x} is a vector in $\{1, -1\}^G$ which is $+1$ on coordinates in H and -1 on the rest, then \mathbf{x} is an eigenvector of $\text{Cay}(G, S)$ with the corresponding eigenvalue $2|S \cap H| - |S|$ (which is an integer with the same parity as $|S|$). This eigenvalue is not necessarily simple, because it might be associated with other subgroups of index 2.

Corollary 6.2.5. *If G is a finite group and S a symmetric generating set of G , then $\text{Cay}(G, S)$ has at least $n_2(G) + 1$ integer eigenvalues.*

Lemma 6.2.6. *Suppose G is a finite group and S is a symmetric generating set of G . Then;*

- a) *Every simple eigenvalue of $\text{Cay}(G, S)$ is an integer.*
- b) *If $|G|$ is odd, then G has just one simple eigenvalue, namely $|S|$.*
- c) *If $|G| = 4k + 2$, then G has at most 2 simple eigenvalues. In this case $\lambda_1 = |S|$ is simple, and the other possible simple eigenvalue is of the form $4t - |S|$, where $0 \leq t \leq \lfloor \frac{|S|-1}{2} \rfloor$.*
- d) *If $|G| = 4k$, then G can have at most 2^n simple eigenvalues, where $|G| = 2^n m$ and $2 \nmid m$. In this case all simple eigenvalues are of the form $2t - |S|$, where $0 \leq t \leq |S|$.*

Proof. We just need to prove part c. We first show that any group of order $4k + 2$ has a subgroup of index 2. Suppose G is a group of order $4k + 2$. Right regular representation of G defines a homomorphism $\varphi : G \rightarrow S_G$ such that $\varphi(g) = r_g$. The map sign from S_G to $\{\pm 1\}$ is a homomorphism which assign $+1$ to even permutations and -1 to odd permutations. Therefore, $\varrho = (\text{sign}) \circ \varphi$ is a homomorphism from G to $\{\pm 1\}$. Suppose H is the kernel of ϱ , that is to say H is the set of elements $g \in G$ such that $\text{sign}(r_g) = +1$. Clearly, $[G : H] \leq 2$.

By a Theorem of Cauchy, there is a $g \in G$ of order 2. Since $g \neq 1$, r_g has no fixed points. Because r_g has order 2 in S_G , it should be a product of $2k + 1$ disjoint transpositions. It follows that $\text{sign}(r_g) = -1$ and we cannot have $|H| = |G|$. Now the eigenvalue corresponding to H is in the form $2|S \cap H| - |S|$. Since H is a subgroup and S a symmetric subset of G , we have $(H \cap S)^{-1} = H^{-1} \cap S^{-1} = H \cap S$. We notice that H has no involution, therefore the symmetric subset $H \cap S$ of H has even size. This implies that the other possible simple eigenvalue is in the form $4t - |S|$, where $0 \leq t \leq \lfloor \frac{|S|-1}{2} \rfloor$. \square

Lemma 6.2.7. *If $H \leq G$ and ρ is a representation of G , then*

$$\rho(H) = \begin{cases} |H|I & \text{if } H \subseteq \text{Ker}\rho \\ 0 & \text{if } H \not\subseteq \text{Ker}\rho \end{cases}.$$

Proof. Suppose $H \leq G$, and $h \in H$. We have:

$$\rho(H) = \sum_{g \in H} \rho(g) = \sum_{g \in H} \rho(gh) = \rho(h) \left(\sum_{g \in H} \rho(g) \right) = \rho(h)\rho(H).$$

If there is an h in H such that $\rho(h) \neq I$, then $\rho(H) = 0$ otherwise $\rho(H) = |H|I$. \square

Since in an abelian group irreducible representations are characters in $\text{Irr}(G)$, we have the following result as an immediate consequence of the previous lemma.

Corollary 6.2.8. *If G is an abelian group, $H \leq G$ and $\chi \in \text{Irr}(G)$, then*

$$\chi(H) = \begin{cases} |H| & \text{if } H \subseteq \text{Ker}\chi \\ 0 & \text{if } H \not\subseteq \text{Ker}\chi \end{cases}.$$

Let $s(\Gamma)$ denote the number of simple eigenvalues of a connected graph Γ . If G is a finite group, suppose $s(G) = \max\{s(\text{Cay}(G, S)) \mid S = S^{-1}, \langle S \rangle = G\}$, and $s(k) = \max\{s(G) \mid |G| = k\}$.

Theorem 6.2.9. *If $k \geq 3$, then $k^{0.386} \leq s(k) \leq k^{0.66}$.*

Proof. Let $G = \mathbb{Z}_2^m \times \mathbb{Z}_3^{m-1}$. Each character of G is in the form $\lambda \times \mu$ where λ is an irreducible character of \mathbb{Z}_2^m and μ an irreducible character of \mathbb{Z}_3^{m-1} . Suppose $\mathbb{Z}_2^m = \langle x_1, \dots, x_m \rangle$ and $\mathbb{Z}_3^{m-1} = \langle y_1, \dots, y_{m-1} \rangle$. We define $S = \{(x_i, y) \mid 2 \leq i \leq m, y \in \langle y_1, \dots, y_{i-1} \rangle\} \cup \{(x_1, 1)\}$. We have shown below that $\text{Cay}(G, S)$ has maximum number of simple eigenvalues. Notice that under an irreducible representation χ of G , $\chi(S) = \sum_{s \in S} \chi(s)$ is an element of the form

$$\sum_{j=0}^{m-1} a_j 3^j,$$

where each a_j is in $\{-1, 1, 0\}$.

Notice all such sums are distinct, and we only have one representation that gives sum $b_j 3^j$ with all $b_j = \pm 1$, so we have 2^m simple eigenvalues. This provides a lower bound of $|G|^{\log(2)/\log(6)} = |G|^{.386}$ on the number of simple eigenvalues. This establishes the lower bound.

Let G be a finite group of order k , and S a symmetric generating subset of G . We have, $\sum_{\rho \in \text{IRR}(G)} \lambda_\rho^2 = |S||G| \leq |G|^2/2$. We also know that since all simple eigenvalues are integers, we have:

$$\sum_{\rho \in \text{IRR}(G)} \lambda_\rho^2 \geq \sum_{\lambda_i \text{ is simple}} \lambda_i^2 \geq t^3/6.$$

Where t is the number of simple eigenvalues. Thus $t \leq |G|^{2/3} = k^{0.66}$. \square

There are many other interesting results about simple eigenvalues in Cayley graphs. Some more results have been provided in [8].

6.3 Open problems and conjectures

In this section, we mention some open problems and outline some new conjectures.

Open Problem 6.3.1. Is there a similar description as in theorem 2.4.4 of the spectrum of some other classes of non-abelian groups?

Open Problem 6.3.2. What is the necessary and sufficient conditions for,

- $\mathbb{B}(\mathcal{G}) = \mathcal{I}_\rho$?
- $\mathbb{B}(\mathcal{N}) = \mathcal{I}_\rho$?

Open Problem 6.3.3. What are the admissible sets in \mathbb{Z}_n ?

Open Problem 6.3.4. Determine all integral Cayley graphs with 4 distinct eigenvalues.

Notice that there are many constructions for graphs with 4 distinct integral eigenvalues. However, characterization of Cayley graphs with 4 distinct integral eigenvalues is still open.

We recall that for a graph Γ , $s(\Gamma)$ denotes the number of simple eigenvalues of Γ . If G is a finite group, $s(G) = \max\{s(\text{Cay}(G, S)) \mid S = S^{-1}, \langle S \rangle = G\}$, and $s(k) = \max\{s(G) \mid |G| = k\}$.

Conjecture 6.3.5. ([8]) *If k is a positive integer, then $s(k) = O(k^{0.5})$.*

We proved in the second section of this chapter that if $k \geq 3$, then $k^{0.386} \leq s(k) \leq k^{0.67}$. Although we have no example of groups where $s(G)$ would be close to $|G|^{0.5}$, we remark that there are known constructions of non-Cayley graphs whose the number of simple eigenvalues is close to this bound (see [50]).

Conjecture 6.3.6. *Suppose G is a finite group and S a symmetric generating set of G . If $\text{Cay}(G, S)$ is integral, then $|G| \leq (|S| + 1)!$.*

For abelian groups this conjecture is a consequence of Theorem 5.1.3. Characterization of connected cubic and 4-regular integral Cayley graphs, proves the conjecture for $|S| \leq 4$. It is interesting to see that the upper bound offered by conjecture 6.3.6 is sharp when $|S| = 3$ or 4. We proved in chapter 4 that for G and S as in the conjecture 6.3.6, $|G|$ divides $2(2|S| - 1)!$. If one use the Stirling's formula to approximate $(|S| + 1)!$ (and the fact that for $x \geq 1$, $\log(1 + x) \leq x - \frac{x^2}{2}$), then we can see that conjecture is valid if $|S| \geq (\log |G|)^{\frac{1}{4}}$. We notice that for non-bipartite integral $\text{Cay}(G, S)$ the conjecture turns to $|G| \leq \frac{(|S|+1)!}{2}$.

Appendix A

Representation theory in GAP

In this appendix, we provide all the necessary representation theory information regarding non-abelian groups of orders 12, 18 and 24. In the following, $E(n)$ will stand for a primitive n -th root of unity. In the GAP the identity of the group is denoted by “<identity> of ...”. The conjugacy class of element g in G is denoted by g^G .

```
GAP, Version 4.6.4 of 04-May-2013 (free software, GPL)
  | GAP | http://www.gap-system.org
Architecture: i686-pc-cygwin-gcc-default32
Libs used: gmp, readline
Loading the library and packages ...
Components: trans 1.0, prim 2.1, small* 1.0, id* 1.0
Packages:  AClib 1.2, Alnuth 3.0.0, AtlasRep 1.5.0, AutPGrp 1.5, Browse 1.8.2,
           CRISP 1.3.6, Cryst 4.1.11,
           CrystCat 1.1.6, CTblLib 1.2.2, FactInt 1.5.3, FGA 1.2.0, GAPDoc 1.5.1,
           IO 4.2, IRREDSOL 1.2.1,
           LAGUNA 3.6.3, Polenta 1.3.1, Polycyclic 2.11, RadiRoot 2.6, ResClasses
           3.3.0, Sophus 1.23, SpinSym 1.5,
           TomLib 1.2.2
Try '?help' for help. See also '?copyright' and '?authors'
gap> LoadPackage( "repsn" );;
```

```
Repsn for Constructing Representations of Finite Groups
      Version 3.0.2
```


Written by
Vahid Dabbaghian

A.1 Representation theory of non-abelian groups of order 12

```

gap> l := AllSmallGroups(12);;
gap> Ds := List(l,StructureDescription);;
gap> A:=Filtered(l, x->IsAbelian(x)=false);;
gap>
gap> Cl := List( A, ConjugacyClasses);;
gap> RCl:=List(Cl, y->List(y, x->Representative(x)));;
gap> OC1 := List( RCl, y-> List(y, x->Order(x)));;
gap> irr := List( A, Irr);;
gap> iRR:=List(irr, x->List(x, y->IrreducibleAffordingRepresentation(y)));;
gap> D:=[1..Length(A)];;
gap> for i in [1..Length(A)] do
> D[i]:=["the", i, "-th group in the list is", A[i],"A generating set of the
      group:", GeneratorsOfGroup(A[i]), "Center of the group:", List(Center(A[i])),
      "Conjugacy classes:", Cl[i], "Representatives of the classes are:", RCl[i],
      "Order of representatives:", OC1[i], irr[i], "Irreducible Matrix
      Representations:", iRR[i]];
> od;
gap> D;

```

Here is the list of all non-abelian group of order 12 along with their conjugacy classes and irreducible characters and matrix representations:

```

[ [ "the", 1, "-th group in the list is", C3 : C4,

  "A generating set of the group:", [ f1, f2, f3 ],

  "Center of the group:", [ <identity> of ..., f2 ],

  "Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f1*f2^G, f2*f3^G
    ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f1*f2,
    f2*f3 ],

  "Order of representatives:", [ 1, 4, 2, 3, 4, 6 ],

  "Character Table:"
  [ Character( CharacterTable( C3 : C4 ), [ 1, 1, 1, 1, 1, 1 ] ),
    Character( CharacterTable( C3 : C4 ), [ 1, -1, 1, 1, -1, 1 ] ),
    Character( CharacterTable( C3 : C4 ), [ 1, -E(4), -1, 1, E(4), -1 ] ),
    Character( CharacterTable( C3 : C4 ), [ 1, E(4), -1, 1, -E(4), -1 ] ),
    Character( CharacterTable( C3 : C4 ), [ 2, 0, -2, -1, 0, 1 ] ),
    Character( CharacterTable( C3 : C4 ), [ 2, 0, 2, -1, 0, -1 ] ) ],

  "Irreducible Matrix Representations:",
  [ [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ], [ f1, f2, f3 ] ->
    [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ], [
    [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [ [
    E(3)^2, 0 ], [ 0, E(3) ] ] ] ],

  [ "the", 2, "-th group in the list is", A4,

```

```

"A generating set of the group:", [ f1, f2, f3 ],

"Center of the group:", [ <identity> of ... ],

"Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f1^2^G ],

"Representatives of the classes are:", [ <identity> of ..., f1, f2, f1^2 ],

"Order of representatives:", [ 1, 3, 2, 3 ],

"Character Table:"
  [ Character( CharacterTable( A4 ), [ 1, 1, 1, 1 ] ),
    Character( CharacterTable( A4 ), [ 1, E(3)^2, 1, E(3) ] ),
    Character( CharacterTable( A4 ), [ 1, E(3), 1, E(3)^2 ] ),
    Character( CharacterTable( A4 ), [ 3, 0, -1, 0 ] ) ],

"Irreducible Matrix Representations:",
  [ [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
    [ f1, f2, f3 ] -> [ [ [ E(3)^2 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
    [ f1, f2, f3 ] -> [ [ [ E(3) ] ], [ [ 1 ] ], [ [ 1 ] ] ],
    [ f1, f2, f3 ] -> [ [ [ 0, 1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ], [ [ -1, 0,
      0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ], [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0,
      0, 1 ] ] ] ],

[ "the", 3, "-th group in the list is", D12,

"A generating set of the group:", [ f1, f2, f3 ],

"Center of the group:", [ <identity> of ..., f2 ],

"Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f1*f2^G,
  f2*f3^G ],

```



```

gap> A:=Filtered(1, x->IsAbelian(x)=false);;
gap>
gap> Cl := List( A, ConjugacyClasses);;
gap> RCl:=List(Cl, y->List(y, x->Representative(x)));;
gap> OCl := List( RCl, y-> List(y, x->Order(x)));;
gap> irr := List( A, Irr);;
gap> iRR:=List(irr, x->List(x, y->IrreducibleAffordingRepresentation(y)));;
gap> D:=[1..Length(A)];;
gap> for i in [1..Length(A)] do
> D[i]:=["the", i, "-th group in the list is", A[i], "A generating set of the
      group:", GeneratorsOfGroup(A[i]), "Center of the group:", List(Center(A[i])),
      "Conjugacy classes:", Cl[i], "Representatives of the classes are:", RCl[i],
      "Order of representatives:", OCl[i], irr[i], "Irreducible Matrix
      Representations:", iRR[i]];
> od;
gap>
gap> D;

```

Here is the list of all non-abelian group of order 18 along with their conjugacy classes and irreducible characters and matrix representations:

```

[ [ "the", 1, "-th group in the list is", D18,

  "A generating set of the group:", [ f1, f2, f3 ],

  "Center of the group:", [ <identity> of ... ],

  "Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f2^2^G, f2*f3^G
    ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f2^2,
    f2*f3 ],

  "Order of representatives:", [ 1, 2, 9, 3, 9, 9 ],

```

"Character Table:"

```
[ Character( CharacterTable( D18 ), [ 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( D18 ), [ 1, -1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( D18 ), [ 2, 0, -1, 2, -1, -1 ] ),
  Character( CharacterTable( D18 ), [ 2, 0, E(9)^2+E(9)^7, -1,
    E(9)^4+E(9)^5, -E(9)^2-E(9)^4-E(9)^5-E(9)^7 ] ),
  Character( CharacterTable( D18 ), [ 2, 0, E(9)^4+E(9)^5, -1,
    -E(9)^2-E(9)^4-E(9)^5-E(9)^7, E(9)^2+E(9)^7 ] ),
  Character( CharacterTable( D18 ), [ 2, 0, -E(9)^2-E(9)^4-E(9)^5-E(9)^7,
    -1, E(9)^2+E(9)^7, E(9)^4+E(9)^5 ] ) ],
```

"Irreducible Matrix Representations:",

```
[ [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ], [ f1, f2, f3 ]
  -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ]
    ], [ [ 1, 0 ], [ 0, 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(9)^7, 0 ], [ 0, E(9)^2
    ] ], [ [ E(3), 0 ], [ 0, E(3)^2 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(9)^5, 0 ], [ 0, E(9)^4
    ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -E(9)^2-E(9)^5, 0 ], [ 0,
    -E(9)^4-E(9)^7 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],
```

```
[ "the", 2, "-th group in the list is", C3 x S3,
```

"A generating set of the group:", [f1, f2, f3],

"Center of the group:", [<identity> of ..., f2, f2^2],

"Conjugacy classes:", [<identity> of ...^G, f1^G, f2^G, f3^G, f1*f2^G,
f2²^G, f2*f3^G, f1*f2²^G, f2²*f3^G],

"Representatives of the classes are:", [<identity> of ..., f1, f2, f3,
f1*f2, f2², f2*f3, f1*f2², f2²*f3],

"Order of representatives:", [1, 2, 3, 3, 6, 3, 3, 6, 3],

"Character Table:"

```
[ Character( CharacterTable( C3 x S3 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( C3 x S3 ), [ 1, -1, 1, 1, -1, 1, 1, -1, 1 ] ),
  Character( CharacterTable( C3 x S3 ), [ 1, -1, E(3)^2, 1, -E(3)^2, E(3),
    E(3)^2, -E(3), E(3) ] ),
  Character( CharacterTable( C3 x S3 ), [ 1, -1, E(3), 1, -E(3), E(3)^2,
    E(3), -E(3)^2, E(3)^2 ] ),
  Character( CharacterTable( C3 x S3 ), [ 1, 1, E(3)^2, 1, E(3)^2, E(3),
    E(3)^2, E(3), E(3) ] ),
  Character( CharacterTable( C3 x S3 ), [ 1, 1, E(3), 1, E(3), E(3)^2,
    E(3), E(3)^2, E(3)^2 ] ),
  Character( CharacterTable( C3 x S3 ), [ 2, 0, 2, -1, 0, 2, -1, 0, -1 ] ),
  Character( CharacterTable( C3 x S3 ), [ 2, 0, 2*E(3), -1, 0, 2*E(3)^2,
    -E(3), 0, -E(3)^2 ] ),
  Character( CharacterTable( C3 x S3 ), [ 2, 0, 2*E(3)^2, -1, 0, 2*E(3),
    -E(3)^2, 0, -E(3) ] ) ],
```

"Irreducible Matrix Representations:",

```
[ [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ], [ f1, f2, f3 ] ->
  [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [ [
    E(3)^2, 0 ], [ 0, E(3) ] ] ],
```

```

[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3), 0 ], [ 0, E(3) ] ],
  [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3)^2, 0 ], [ 0, E(3)^2
  ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],

```

```

[ "the", 3, "-th group in the list is", (C3 x C3) : C2,

```

```

"A generating set of the group:", [ f1, f2, f3 ],

```

```

"Center of the group:", [ <identity> of ... ],

```

```

"Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f2*f3^G,
  f2^2*f3^G ],

```

```

"Representatives of the classes are:", [ <identity> of ..., f1, f2, f3,
  f2*f3, f2^2*f3 ],

```

```

"Order of representatives:", [ 1, 2, 3, 3, 3, 3 ],

```

```

" Character Table:"

```

```

[ Character( CharacterTable( (C3 x C3) : C2 ), [ 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( (C3 x C3) : C2 ), [ 1, -1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( (C3 x C3) : C2 ), [ 2, 0, 2, -1, -1, -1 ] ),
  Character( CharacterTable( (C3 x C3) : C2 ), [ 2, 0, -1, 2, -1, -1 ] ),
  Character( CharacterTable( (C3 x C3) : C2 ), [ 2, 0, -1, -1, -1, 2 ] ),
  Character( CharacterTable( (C3 x C3) : C2 ), [ 2, 0, -1, -1, 2, -1 ] ) ],

```

```

"Irreducible Matrix Representations:",

```

```

[ [ f1, f2, f3 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ], [ f1, f2, f3 ] ->
  [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [ [
  E(3)^2, 0 ], [ 0, E(3) ] ] ],

```



```

[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ]
], [ [ 1, 0 ], [ 0, 1 ] ] ],
[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ]
], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3), 0 ], [ 0, E(3)^2 ]
], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ] ] ]

```

```

gap>
gap>
gap>

```

A.3 Representation theory of non-abelian groups of order 24

```

gap> l := AllSmallGroups(24);;
Ds := List(l,StructureDescription);;
A:=Filtered(l, x->IsAbelian(x)=false);;

Cl := List( A, ConjugacyClasses);;
RC1:=List(Cl, y->List(y, x->Representative(x)));;
OC1 := List( RC1, y-> List(y, x->Order(x)));;
irr := List( A, Irr);;
iRR:=List(irr, x->List(x, y->IrreducibleAffordingRepresentation(y)));;gap> Ds :=
List(l,StructureDescription);;
gap> A:=Filtered(l, x->IsAbelian(x)=false);;
gap>
gap> Cl := List( A, ConjugacyClasses);;
gap> RC1:=List(Cl, y->List(y, x->Representative(x)));;
gap> OC1 := List( RC1, y-> List(y, x->Order(x)));;
gap> irr := List( A, Irr);;
gap> iRR:=List(irr, x->List(x, y->IrreducibleAffordingRepresentation(y)));;
#I Need to extend a representation of degree 2. This may take a while.

```

```

#I Need to extend a representation of degree 2. This may take a while.
#I Need to extend a representation of degree 2. This may take a while.
gap> D:=[1..12];;
gap> for i in [1..12] do
> D[i]:=["the", i, "-th group in the list is", A[i], "A generating set of the
      group:", GeneratorsOfGroup(A[i]), "Center of the group:", List(Center(A[i])),
      "Conjugacy classes:", Cl[i], "Representatives of the classes are:", RCl[i],
      "Order of representatives:", OCl[i], irr[i], "Irreducible Matrix
      Representations:", iRR[i]];
> od;
gap> D;

```

Here is the list of all non-abelian group of order 24 along with their conjugacy classes and irreducible characters and matrix representations:

```

[ [ "the", 1, "-th group in the list is", C3 : C8,

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ..., f3, f2, f2*f3 ],

  "Conjugacy classes:",
  [ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
    f2*f4^G, f3*f4^G, f1*f2*f3^G, f2*f3*f4^G ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f4,
    f1*f2, f1*f3, f2*f3, f2*f4, f3*f4, f1*f2*f3, f2*f3*f4 ],

  "Order of representatives:", [ 1, 8, 4, 2, 3, 8, 8, 4, 12, 6, 8, 12 ],

```

```

[ Character( CharacterTable( C3 : C8 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1 ] ),
Character( CharacterTable( C3 : C8 ), [ 1, -1, 1, 1, 1, -1, -1, 1, 1, 1, 1,
  -1, 1 ] ),
Character( CharacterTable( C3 : C8 ), [ 1, -E(4), -1, 1, 1, E(4), -E(4),
  -1, -1, 1, E(4), -1 ] ),
Character( CharacterTable( C3 : C8 ), [ 1, E(4), -1, 1, 1, -E(4), E(4),
  -1, -1, 1, -E(4), -1 ] ),
Character( CharacterTable( C3 : C8 ), [ 1, -E(8), E(4), -1, 1, -E(8)^3,
  E(8), -E(4), E(4), -1, E(8)^3, -E(4) ] ),
Character( CharacterTable( C3 : C8 ), [ 1, -E(8)^3, -E(4), -1, 1, -E(8),
  E(8)^3, E(4), -E(4), -1, E(8), E(4) ] ),
Character( CharacterTable( C3 : C8 ), [ 1, E(8)^3, -E(4), -1, 1, E(8),
  -E(8)^3, E(4), -E(4), -1, -E(8), E(4) ] ),
Character( CharacterTable( C3 : C8 ), [ 1, E(8), E(4), -1, 1, E(8)^3,
  -E(8), -E(4), E(4), -1, -E(8)^3, -E(4) ] ),
Character( CharacterTable( C3 : C8 ), [ 2, 0, -2, 2, -1, 0, 0, -2, 1, -1,
  0, 1 ] ),
Character( CharacterTable( C3 : C8 ), [ 2, 0, 2, 2, -1, 0, 0, 2, -1, -1,
  0, -1 ] ),
Character( CharacterTable( C3 : C8 ), [ 2, 0, -2*E(4), -2, -1, 0, 0,
  2*E(4), E(4), 1, 0, -E(4) ] ),
Character( CharacterTable( C3 : C8 ), [ 2, 0, 2*E(4), -2, -1, 0, 0,
  -2*E(4), -E(4), 1, 0, E(4) ] ) ],

```

"Irreducible Matrix Representations:",

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -E(8) ] ], [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
] ],
[ f1, f2, f3, f4 ] -> [ [ [ -E(8)^3 ] ], [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
] ],

```

```

[ f1, f2, f3, f4 ] -> [ [ [ E(8)^3 ] ], [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1
  ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ E(8) ] ], [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ]
  ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ]
  ], [ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
  [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -E(4), 0 ] ], [ [ -E(4), 0 ], [ 0,
  -E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ E(4), 0 ] ], [ [ E(4), 0 ], [ 0,
  E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ]
  ],

```

```
[ "the", 2, "-th group in the list is", SL(2,3),
```

```
  "A generating set of the group:", [ f1, f2, f3, f4 ],
```

```
  "Center of the group:", [ <identity> of ..., f4 ],
```

```
  "Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f4^G, f1^2^G,
  f1*f4^G, f1^2*f2^G ],
```

```
  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f4, f1^2,
  f1*f4, f1^2*f2 ],
```

```
  "Order of representatives:", [ 1, 3, 4, 2, 3, 6, 6 ],
```

```
  "Character Table:"
```

```
[ Character( CharacterTable( SL(2,3) ), [ 1, 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( SL(2,3) ), [ 1, E(3)^2, 1, 1, E(3), E(3)^2,
  E(3) ] ),
```

```

Character( CharacterTable( SL(2,3) ), [ 1, E(3), 1, 1, E(3)^2, E(3),
      E(3)^2 ] ),
Character( CharacterTable( SL(2,3) ), [ 2, -1, 0, -2, -1, 1, 1 ] ),
Character( CharacterTable( SL(2,3) ), [ 2, -E(3), 0, -2, -E(3)^2, E(3),
      E(3)^2 ] ),
Character( CharacterTable( SL(2,3) ), [ 2, -E(3)^2, 0, -2, -E(3), E(3)^2,
      E(3) ] ),
Character( CharacterTable( SL(2,3) ), [ 3, 0, -1, 3, 0, 0, 0 ] ) ],

```

"Irreducible Matrix Representations:"

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ E(3)^2 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ E(3) ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f2, f3, f4, f1*f2*f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [
      0, E(4) ] ],
      [ [ -1, 0 ], [ 0, -1 ] ], [ [
      1/2+1/2*E(4), 1/2+1/2*E(4) ], [
      -1/2+1/2*E(4), 1/2-1/2*E(4) ] ]
],
[ f2, f3, f4, f1^2*f3*f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [
      0, E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ],
      [ [ -1/2*E(12)^8-1/2*E(12)^11,
      -1/2*E(12)^8+1/2*E(12)^11 ],
      [ 1/2*E(12)^8+1/2*E(12)^11,
      -1/2*E(12)^8+1/2*E(12)^11 ]
] ],
[ f2, f3, f4, f1^2*f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [
      0, E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ],
      [ [ 1/2*E(12)^4-1/2*E(12)^7,
      1/2*E(12)^4+1/2*E(12)^7 ],
      [ -1/2*E(12)^4+1/2*E(12)^7,
      1/2*E(12)^4+1/2*E(12)^7 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ], [ [
      -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],

```

```

[ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ] ],
  [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ]
] ] ],

```

```

[ "the", 3, "-th group in the list is", C3 : Q8,

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ..., f3 ],

  "Conjugacy classes:",
  [ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f2*f4^G, f3*f4^G,
    f2*f3*f4^G ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f4,
    f1*f2, f2*f4, f3*f4, f2*f3*f4 ],

  "Order of representatives:", [ 1, 4, 4, 2, 3, 4, 12, 6, 12 ],

  "Character Table:"
  [ Character( CharacterTable( C3 : Q8 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 1, -1, -1, 1, 1, 1, -1, 1, -1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 1, -1, 1, 1, 1, -1, 1, 1, 1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 1, 1, -1, 1, 1, -1, -1, 1, -1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 2, 0, 0, -2, 2, 0, 0, -2, 0 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 2, 0, -2, 2, -1, 0, 1, -1, 1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 2, 0, 2, 2, -1, 0, -1, -1, -1 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 2, 0, 0, -2, -1, 0,
      -E(12)^7+E(12)^11, 1, E(12)^7-E(12)^11 ] ),
    Character( CharacterTable( C3 : Q8 ), [ 2, 0, 0, -2, -1, 0,
      E(12)^7-E(12)^11, 1, -E(12)^7+E(12)^11 ] ) ],

  "Irreducible Matrix Representations:",

```

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [ 0,
    E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ 1, 0 ], [ 0, 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
    [ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
    [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ E(4), 0 ], [ 0,
    -E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [ 0,
    E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ]
] ],

```

```
[ "the", 4, "-th group in the list is", C4 x S3,
```

```
"A generating set of the group:", [ f1, f2, f3, f4 ],
```

```
"Center of the group:", [ <identity> of ..., f3, f2, f2*f3 ],
```

```
"Conjugacy classes:",
```

```
[ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
    f2*f4^G, f3*f4^G, f1*f2*f3^G, f2*f3*f4^G ],
```

```
"Representatives of the classes are:",
```

```
[ <identity> of ..., f1, f2, f3, f4, f1*f2, f1*f3, f2*f3, f2*f4, f3*f4,
    f1*f2*f3, f2*f3*f4 ],
```

```
"Order of representatives:", [ 1, 2, 4, 2, 3, 4, 2, 4, 12, 6, 4, 12 ],
```

```
"Character Table:"
```

```
[ Character( CharacterTable( C4 x S3 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
    1 ] ),
```

```

Character( CharacterTable( C4 x S3 ), [ 1, -1, -1, 1, 1, 1, -1, -1, -1,
    1, 1, -1 ] ),
Character( CharacterTable( C4 x S3 ), [ 1, -1, 1, 1, 1, -1, -1, 1, 1, 1,
    -1, 1 ] ),
Character( CharacterTable( C4 x S3 ), [ 1, 1, -1, 1, 1, -1, 1, -1, -1, 1,
    -1, -1 ] ),
Character( CharacterTable( C4 x S3 ), [ 1, -1, -E(4), -1, 1, E(4), 1,
    E(4), -E(4), -1, -E(4), E(4) ] ),
Character( CharacterTable( C4 x S3 ), [ 1, -1, E(4), -1, 1, -E(4), 1,
    -E(4), E(4), -1, E(4), -E(4) ] ),
Character( CharacterTable( C4 x S3 ), [ 1, 1, -E(4), -1, 1, -E(4), -1,
    E(4), -E(4), -1, E(4), E(4) ] ),
Character( CharacterTable( C4 x S3 ), [ 1, 1, E(4), -1, 1, E(4), -1,
    -E(4), E(4), -1, -E(4), -E(4) ] ),
Character( CharacterTable( C4 x S3 ), [ 2, 0, -2, 2, -1, 0, 0, -2, 1, -1,
    0, 1 ] ),
Character( CharacterTable( C4 x S3 ), [ 2, 0, 2, 2, -1, 0, 0, 2, -1, -1,
    0, -1 ] ),
Character( CharacterTable( C4 x S3 ), [ 2, 0, -2*E(4), -2, -1, 0, 0,
    2*E(4), E(4), 1, 0, -E(4) ] ),
Character( CharacterTable( C4 x S3 ), [ 2, 0, 2*E(4), -2, -1, 0, 0,
    -2*E(4), -E(4), 1, 0, E(4) ] ) ],

```

"Irreducible Matrix Representations:"

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ E(4) ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
[ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],

```



```

[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
  [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -E(4), 0 ], [ 0,
  -E(4) ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(4), 0 ], [ 0, E(4)
  ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ] ],

```

```
[ "the", 5, "-th group in the list is", D24,
```

```
"A generating set of the group:", [ f1, f2, f3, f4 ],
```

```
"Center of the group:", [ <identity> of ..., f3 ],
```

```
"Conjugacy classes:",
```

```
[ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f2*f4^G, f3*f4^G,
  f2*f3*f4^G ],
```

```
"Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f4,
  f1*f2, f2*f4, f3*f4, f2*f3*f4 ],
```

```
"Order of representatives:", [ 1, 2, 4, 2, 3, 2, 12, 6, 12 ],
```

```
"Character Table:"
```

```
[ Character( CharacterTable( D24 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1 ] ),
  Character( CharacterTable( D24 ), [ 1, -1, -1, 1, 1, 1, -1, 1, -1 ] ),
  Character( CharacterTable( D24 ), [ 1, -1, 1, 1, 1, -1, 1, 1, 1 ] ),
  Character( CharacterTable( D24 ), [ 1, 1, -1, 1, 1, -1, -1, 1, -1 ] ),
  Character( CharacterTable( D24 ), [ 2, 0, 0, -2, 2, 0, 0, -2, 0 ] ),
  Character( CharacterTable( D24 ), [ 2, 0, -2, 2, -1, 0, 1, -1, 1 ] ),
  Character( CharacterTable( D24 ), [ 2, 0, 2, 2, -1, 0, -1, -1, -1 ] ),
  Character( CharacterTable( D24 ), [ 2, 0, 0, -2, -1, 0,
    -E(12)^7+E(12)^11, 1, E(12)^7-E(12)^11 ] ),
  Character( CharacterTable( D24 ), [ 2, 0, 0, -2, -1, 0, E(12)^7-E(12)^11,
    1, -E(12)^7+E(12)^11 ] ) ],
```

```

"Irreducible Matrix Representations:"
  [ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -E(4), 0 ], [ 0, E(4)
    ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ 1, 0 ], [ 0, 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
    [ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
    [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(4), 0 ], [ 0, -E(4)
    ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -E(4), 0 ], [ 0, E(4)
    ] ], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],

[ "the", 6, "-th group in the list is", C2 x (C3 : C4),

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ..., f3, f2, f2*f3 ],

  "Conjugacy classes:",
  [ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
    f2*f4^G, f3*f4^G, f1*f2*f3^G, f2*f3*f4^G ],

  "Representatives of the classes are:",
  [ <identity> of ..., f1, f2, f3, f4, f1*f2, f1*f3, f2*f3, f2*f4, f3*f4,
    f1*f2*f3, f2*f3*f4 ],

  "Order of representatives:", [ 1, 4, 2, 2, 3, 4, 4, 2, 6, 6, 4, 6 ],

  "Character Table:"
  [ Character( CharacterTable( C2 x (C3 : C4) ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1,
    1, 1, 1 ] ) ],

```

```

Character( CharacterTable( C2 x (C3 : C4) ), [ 1, -1, -1, 1, 1, 1, -1,
-1, -1, 1, 1, -1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, -1, 1, 1, 1, -1, -1, 1,
1, 1, -1, 1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, 1, -1, 1, 1, -1, 1, -1,
-1, 1, -1, -1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, -E(4), -1, -1, 1, E(4),
E(4), 1, -1, -1, -E(4), 1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, E(4), -1, -1, 1, -E(4),
-E(4), 1, -1, -1, E(4), 1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, -E(4), 1, -1, 1, -E(4),
E(4), -1, 1, -1, E(4), -1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 1, E(4), 1, -1, 1, E(4),
-E(4), -1, 1, -1, -E(4), -1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 2, 0, -2, -2, -1, 0, 0, 2,
1, 1, 0, -1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 2, 0, -2, 2, -1, 0, 0, -2,
1, -1, 0, 1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 2, 0, 2, -2, -1, 0, 0, -2,
-1, 1, 0, 1 ] ),
Character( CharacterTable( C2 x (C3 : C4) ), [ 2, 0, 2, 2, -1, 0, 0, 2,
-1, -1, 0, -1 ] ) ],

```

"Irreducible Matrix Representations:",

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -E(4) ] ], [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ E(4) ] ], [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -E(4) ] ], [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ E(4) ] ], [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ]
], [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],

```

```

[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
  [ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ],
  [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
  [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],

```

```

[ "the", 7, "-th group in the list is", (C6 x C2) : C2,

```

```

  "A generating set of the group:", [ f1, f2, f3, f4 ],

```

```

  "Center of the group:", [ <identity> of ..., f3 ],

```

```

  "Conjugacy classes:",

```

```

  [ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f2*f4^G, f3*f4^G,
    f2*f3*f4^G ],

```

```

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f4,
    f1*f2, f2*f4, f3*f4, f2*f3*f4 ],

```

```

  "Order of representatives:", [ 1, 2, 2, 2, 3, 4, 6, 6, 6 ],

```

```

  "Character Table:"

```

```

  [ Character( CharacterTable( (C6 x C2) : C2 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1
    ] ),
    Character( CharacterTable( (C6 x C2) : C2 ), [ 1, -1, -1, 1, 1, 1, -1, 1,
    -1 ] ),
    Character( CharacterTable( (C6 x C2) : C2 ), [ 1, -1, 1, 1, 1, -1, 1, 1,
    1 ] ),
    Character( CharacterTable( (C6 x C2) : C2 ), [ 1, 1, -1, 1, 1, -1, -1, 1,
    -1 ] ),
    Character( CharacterTable( (C6 x C2) : C2 ), [ 2, 0, -2, 2, -1, 0, 1, -1,
    1 ] ),
    Character( CharacterTable( (C6 x C2) : C2 ), [ 2, 0, 2, 2, -1, 0, -1, -1,
    -1 ] ),

```

```

Character( CharacterTable( (C6 x C2) : C2 ), [ 2, 0, 0, -2, 2, 0, 0, -2,
0 ] ),
Character( CharacterTable( (C6 x C2) : C2 ), [ 2, 0, 0, -2, -1, 0,
-E(3)+E(3)^2, 1, E(3)-E(3)^2 ] ),
Character( CharacterTable( (C6 x C2) : C2 ), [ 2, 0, 0, -2, -1, 0,
E(3)-E(3)^2, 1, -E(3)+E(3)^2 ] ) ],

```

"Irreducible Matrix Representations:"

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
[ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
[ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, 1 ] ],
[ [ -1, 0 ], [ 0, -1 ] ], [ [ 1, 0 ], [ 0, 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, -1 ] ],
[ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, 1 ] ],
[ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ],

```

```
[ "the", 8, "-th group in the list is", C3 x D8,
```

```
"A generating set of the group:", [ f1, f2, f3, f4 ],
```

```
"Center of the group:", [ <identity> of ..., f4, f3, f3*f4, f3^2, f3^2*f4 ],
```

```
"Conjugacy classes:",
```

```
[ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
f3^2^G, f3*f4^G, f1*f2*f3^G, f1*f3^2^G,
f2*f3^2^G, f3^2*f4^G, f1*f2*f3^2^G ],
```

```

"Representatives of the classes are:",
  [ <identity> of ..., f1, f2, f3, f4, f1*f2, f1*f3, f2*f3, f3^2, f3*f4,
    f1*f2*f3, f1*f3^2, f2*f3^2, f3^2*f4, f1*f2*f3^2 ],

"Order of representatives:", [ 1, 2, 2, 3, 2, 4, 6, 6, 3, 6, 12, 6, 6, 6, 12 ],

"CharacterTable:"
  [ Character( CharacterTable( C3 x D8 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
    1, 1, 1, 1 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, -1, 1, 1, 1, -1, -1, 1, 1,
    1, -1, -1, 1, 1 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, 1,
    -1, -1, 1, 1, -1 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1,
    -1, 1, -1, 1, -1 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, -1, E(3)^2, 1, 1, -E(3)^2,
    -E(3)^2, E(3), E(3)^2, E(3)^2, -E(3), -E(3), E(3), E(3) ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, -1, E(3), 1, 1, -E(3),
    -E(3), E(3)^2, E(3), E(3), -E(3)^2, -E(3)^2, E(3)^2, E(3)^2 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, 1, E(3)^2, 1, -1, -E(3)^2,
    E(3)^2, E(3), E(3)^2, -E(3)^2, -E(3), E(3), E(3), -E(3) ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, -1, 1, E(3), 1, -1, -E(3),
    E(3), E(3)^2, E(3), -E(3), -E(3)^2, E(3)^2, E(3)^2, -E(3)^2 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, 1, -1, E(3)^2, 1, -1, E(3)^2,
    -E(3)^2, E(3), E(3)^2, -E(3)^2, E(3), -E(3), E(3), -E(3) ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, 1, -1, E(3), 1, -1, E(3),
    -E(3), E(3)^2, E(3), -E(3), E(3)^2, -E(3)^2, E(3)^2, -E(3)^2 ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, 1, 1, E(3)^2, 1, 1, E(3)^2,
    E(3)^2, E(3), E(3)^2, E(3)^2, E(3), E(3), E(3), E(3) ] ),
    Character( CharacterTable( C3 x D8 ), [ 1, 1, 1, E(3), 1, 1, E(3), E(3),
    E(3)^2, E(3), E(3), E(3)^2, E(3)^2, E(3)^2, E(3)^2 ] ),
    Character( CharacterTable( C3 x D8 ), [ 2, 0, 0, 2, -2, 0, 0, 0, 2, -2,
    0, 0, 0, -2, 0 ] ),
    Character( CharacterTable( C3 x D8 ), [ 2, 0, 0, 2*E(3)^2, -2, 0, 0, 0,
    2*E(3), -2*E(3)^2, 0, 0, 0, -2*E(3), 0 ] ),

```

```
Character( CharacterTable( C3 x D8 ), [ 2, 0, 0, 2*E(3), -2, 0, 0, 0,
    2*E(3)^2, -2*E(3), 0, 0, 0, -2*E(3)^2, 0 ] ) ],
```

```
"Irreducible Matrix Representations:",
```

```
[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
    ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
    ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
    ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, 1 ] ],
    [ [ 1, 0 ], [ 0, 1 ] ],
      [ [ -1, 0 ], [ 0, -1 ] ] ], [ f1, f2, f3, f4
    ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0
      ], [ 0, 1 ] ] ],
      [ [ E(3)^2, 0 ], [ 0, E(3)^2 ] ], [ [ -1, 0
        ], [ 0, -1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, 1 ] ],
    [ [ E(3), 0 ], [ 0, E(3) ] ], [ [ -1, 0 ], [ 0, -1 ] ] ] ],
```

```
[ "the", 9, "-th group in the list is", C3 x Q8,
```

```
"A generating set of the group:", [ f1, f2, f3, f4 ],
```

```

"Center of the group:", [ <identity> of ..., f4, f3, f3*f4, f3^2, f3^2*f4 ],

"Conjugacy classes:",
[ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
  f3^2^G, f3*f4^G, f1*f2*f3^G,
  f1*f3^2^G, f2*f3^2^G, f3^2*f4^G, f1*f2*f3^2^G ],

"Representatives of the classes are:",
[ <identity> of ..., f1, f2, f3, f4, f1*f2, f1*f3, f2*f3, f3^2, f3*f4,
  f1*f2*f3, f1*f3^2, f2*f3^2, f3^2*f4, f1*f2*f3^2 ],

"Order of representatives:", [ 1, 4, 4, 3, 2, 4, 12, 12, 3, 6, 12, 12, 12, 6,
  12 ],

"Character Table:"
[ Character( CharacterTable( C3 x Q8 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1, 1 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, -1, 1, 1, 1, -1, -1, 1, 1,
  1, -1, -1, 1, 1 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, 1, 1, 1, -1, -1, 1, 1, 1,
  -1, -1, 1, 1, -1 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, 1, -1, 1, 1, -1, 1, -1, 1, 1,
  -1, 1, -1, 1, -1 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, -1, E(3)^2, 1, 1, -E(3)^2,
  -E(3)^2, E(3), E(3)^2, E(3)^2, -E(3), -E(3), E(3), E(3) ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, -1, E(3), 1, 1, -E(3),
  -E(3), E(3)^2, E(3), E(3), -E(3)^2, -E(3)^2, E(3)^2, E(3)^2 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, 1, E(3)^2, 1, -1, -E(3)^2,
  E(3)^2, E(3), E(3)^2, -E(3)^2, -E(3), E(3), E(3), -E(3) ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, -1, 1, E(3), 1, -1, -E(3),
  E(3), E(3)^2, E(3), -E(3), -E(3)^2, E(3)^2, E(3)^2, -E(3)^2 ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, 1, -1, E(3)^2, 1, -1, E(3)^2,
  -E(3)^2, E(3), E(3)^2, -E(3)^2, E(3), -E(3), E(3), -E(3) ] ),
  Character( CharacterTable( C3 x Q8 ), [ 1, 1, -1, E(3), 1, -1, E(3),
  -E(3), E(3)^2, E(3), -E(3), E(3)^2, -E(3)^2, E(3)^2, -E(3)^2 ] ),

```



```

Character( CharacterTable( C3 x Q8 ), [ 1, 1, 1, E(3)^2, 1, 1, E(3)^2,
      E(3)^2, E(3), E(3)^2, E(3)^2, E(3), E(3), E(3), E(3) ] ),
Character( CharacterTable( C3 x Q8 ), [ 1, 1, 1, E(3), 1, 1, E(3), E(3),
      E(3)^2, E(3), E(3), E(3)^2, E(3)^2, E(3)^2, E(3)^2 ] ),
Character( CharacterTable( C3 x Q8 ), [ 2, 0, 0, 2, -2, 0, 0, 0, 2, -2,
      0, 0, 0, -2, 0 ] ),
Character( CharacterTable( C3 x Q8 ), [ 2, 0, 0, 2*E(3)^2, -2, 0, 0, 0,
      2*E(3), -2*E(3)^2, 0, 0, 0, -2*E(3), 0 ] ),
Character( CharacterTable( C3 x Q8 ), [ 2, 0, 0, 2*E(3), -2, 0, 0, 0,
      2*E(3)^2, -2*E(3), 0, 0, 0, -2*E(3)^2, 0 ] ) ],

```

"Irreducible Matrix Representations:",

```

[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [ 0,
      E(4) ] ], [ [ 1, 0 ], [ 0, 1 ] ], [ [ -1, 0 ], [ 0, -1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [ 0,
      E(4) ] ], [ [ E(3)^2, 0 ], [ 0, E(3)^2 ] ], [ [ -1, 0 ], [ 0, -1 ] ]
],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ -1, 0 ] ], [ [ -E(4), 0 ], [ 0,
      E(4) ] ], [ [ E(3), 0 ], [ 0, E(3) ] ], [ [ -1, 0 ], [ 0, -1 ] ] ] ],

```

```

[ "the", 10, "-th group in the list is", S4,

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ... ],

  "Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f1*f3^G ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3, f1*f3
    ],

  "Order of representatives:", [ 1, 2, 3, 2, 4 ],

  "Character Table:"
    [ Character( CharacterTable( S4 ), [ 1, 1, 1, 1, 1 ] ),
      Character( CharacterTable( S4 ), [ 1, -1, 1, 1, -1 ] ),
      Character( CharacterTable( S4 ), [ 2, 0, -1, 2, 0 ] ),
      Character( CharacterTable( S4 ), [ 3, -1, 0, -1, 1 ] ),
      Character( CharacterTable( S4 ), [ 3, 1, 0, -1, -1 ] ) ],

  "Irreducible Matrix Representations:",
    [ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
      [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
      [ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ E(3)^2, 0 ], [ 0,
        E(3) ] ], [ [ 1, 0 ], [ 0, 1 ] ], [ [ 1, 0 ], [ 0, 1 ] ] ],
      [ f1, f2, f3, f4 ] -> [ [ [ -1, 0, 0 ], [ 0, 0, -1 ], [ 0, -1, 0 ] ], [ [
        0, 1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ],

```

```

[ [ [-1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [-1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ]
  ] ], [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0,
    0, 1 ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 1, 0, 0 ], [ 0, 0, 1 ], [ 0, 1, 0 ] ], [ [ 0,
  1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ],
  [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
  [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ]
  ] ] ],

[ "the", 11, "-th group in the list is", C2 x A4,

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ..., f1 ],

  "Conjugacy classes:", [ <identity> of ...^G, f1^G, f2^G, f3^G, f1*f2^G,
    f1*f3^G, f2^2^G, f1*f2^2^G ],

  "Representatives of the classes are:", [ <identity> of ..., f1, f2, f3,
    f1*f2, f1*f3, f2^2, f1*f2^2 ],

  "Order of representatives:", [ 1, 2, 3, 2, 6, 2, 3, 6 ],

  "Character Table:"
[   Character( CharacterTable( C2 x A4 ), [ 1, 1, 1, 1, 1, 1, 1, 1 ] ),
     Character( CharacterTable( C2 x A4 ), [ 1, -1, 1, 1, -1, -1, 1, -1 ] ),
     Character( CharacterTable( C2 x A4 ), [ 1, -1, E(3)^2, 1, -E(3)^2, -1,
       E(3), -E(3) ] ),
     Character( CharacterTable( C2 x A4 ), [ 1, -1, E(3), 1, -E(3), -1,
       E(3)^2, -E(3)^2 ] ),
     Character( CharacterTable( C2 x A4 ), [ 1, 1, E(3)^2, 1, E(3)^2, 1, E(3),
       E(3) ] ),
     Character( CharacterTable( C2 x A4 ), [ 1, 1, E(3), 1, E(3), 1, E(3)^2,
       E(3)^2 ] ),

```

```

Character( CharacterTable( C2 x A4 ), [ 3, -3, 0, -1, 0, 1, 0, 0 ] ),
  Character( CharacterTable( C2 x A4 ),
    [ 3, 3, 0, -1, 0, -1, 0, 0 ] ) ),

"Irreducible Matrix Representations:",
[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ], [ [ 1 ] ]
    ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ E(3) ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ E(3)^2 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ E(3) ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, -1 ] ], [ [
    0, 1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ],
    [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
    [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ]
      ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, 1 ] ], [ [ 0,
    1, 0 ], [ 0, 0, 1 ], [ 1, 0, 0 ] ],
    [ [ -1, 0, 0 ], [ 0, 1, 0 ], [ 0, 0, -1 ] ],
    [ [ -1, 0, 0 ], [ 0, -1, 0 ], [ 0, 0, 1 ]
      ] ] ],

[ "the", 12, "-th group in the list is", C2 x C2 x S3,

  "A generating set of the group:", [ f1, f2, f3, f4 ],

  "Center of the group:", [ <identity> of ..., f3, f2, f2*f3 ],

  "Conjugacy classes:",
  [ <identity> of ...^G, f1^G, f2^G, f3^G, f4^G, f1*f2^G, f1*f3^G, f2*f3^G,
    f2*f4^G, f3*f4^G, f1*f2*f3^G, f2*f3*f4^G ],

  "Representatives of the classes are:"
  [ <identity> of ..., f1, f2, f3, f4, f1*f2, f1*f3, f2*f3, f2*f4, f3*f4,
    f1*f2*f3, f2*f3*f4 ],

```

"Order of representatives:", [1, 2, 2, 2, 3, 2, 2, 2, 6, 6, 2, 6],

"Character Table:"

```
[ Character( CharacterTable( C2 x C2 x S3 ), [ 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
  1, 1, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, -1, -1, -1, 1, 1, 1, 1,
  -1, -1, -1, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, -1, -1, 1, 1, 1, -1, -1,
  -1, 1, 1, -1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, -1, 1, -1, 1, -1, 1, -1,
  1, -1, 1, -1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, -1, 1, 1, 1, -1, -1, 1,
  1, 1, -1, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, 1, -1, -1, 1, -1, -1, 1,
  -1, -1, 1, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, 1, -1, 1, 1, -1, 1, -1,
  -1, 1, -1, -1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 1, 1, 1, -1, 1, 1, -1, -1,
  1, -1, -1, -1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 2, 0, -2, -2, -1, 0, 0, 2,
  1, 1, 0, -1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 2, 0, -2, 2, -1, 0, 0, -2,
  1, -1, 0, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 2, 0, 2, -2, -1, 0, 0, -2,
  -1, 1, 0, 1 ] ),
  Character( CharacterTable( C2 x C2 x S3 ), [ 2, 0, 2, 2, -1, 0, 0, 2, -1,
  -1, 0, -1 ] ) ],
```

"Irreducible Matrix Representations:"

```
[ [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ], [ [ 1 ] ] ],
  [ f1, f2, f3, f4 ] -> [ [ [ 1 ] ], [ [ 1 ] ], [ [ -1 ] ], [ [ 1 ] ] ],
```

```

[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
  [ [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ -1, 0 ], [ 0, -1 ] ],
  [ [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
  [ -1, 0 ], [ 0, -1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ],
[ f1, f2, f3, f4 ] -> [ [ [ 0, 1 ], [ 1, 0 ] ], [ [ 1, 0 ], [ 0, 1 ] ], [
  [ 1, 0 ], [ 0, 1 ] ], [ [ E(3)^2, 0 ], [ 0, E(3) ] ] ] ] ]

```

gap>

Appendix B

Cayley graphs programming

B.1 Spectrum computation with GAP

In this section, we provide a program which compute the spectrum of Cayley graphs of finite group with respect to a symmetric generating set.

```
GAP, Version 4.6.4 of 04-May-2013 (free software, GPL)
| GAP |   http://www.gap-system.org
  Architecture: i686-pc-cygwin-gcc-default32
Libs used: gmp, readline
Loading the library and packages ...
Components: trans 1.0, prim 2.1, small* 1.0, id* 1.0
Packages:  AClib 1.2, Alnuth 3.0.0, AtlasRep 1.5.0, AutPGrp 1.5, Browse 1.8.2,
           CRISP 1.3.6, Cryst 4.1.11,
           CrystCat 1.1.6, CTblLib 1.2.2, FactInt 1.5.3, FGA 1.2.0, GAPDoc 1.5.1,
           IO 4.2, IRREDSOL 1.2.1,
           LAGUNA 3.6.3, Polenta 1.3.1, Polycyclic 2.11, RadiRoot 2.6, ResClasses
           3.3.0, Sophus 1.23, SpinSym 1.5,
           TomLib 1.2.2
Try '?help' for help. See also '?copyright' and '?authors'
gap>
gap>
gap>
```

Following program will compute all the eigenvalue of the Cayley graph, $\text{Cay}(G, S)$, over $|G|$ -th cyclotomic field. Here G is a finite group and S a symmetric generating set.

```

gap>
gap>
gap>
gap> setproduct:=function(S,n)
T:=List(Cartesian(T,> S),i->i[1]*i[2]);
local T,m;
> end;
T:=S; m:=1;
> if n=1 then T:=S; fi;
> while n>m do
> T:=List(Cartesian(T,S),i->i[1]*i[2]);
> m:=m+1;
> od;
> return T;
> end;
local d,X,l;
X:=Irr(G)[i];
function( S, n ) ... end
gap>
gap> l:= List([1..d],j->sumceigenn(Gl,setprodauct(S,j)s,i));
sfinder:=function(G,g)
> local c;
> c:=ConjugacyClasses(G);
> return First([1..Length(c)],i->g in c[i]);
> end;
function( G, g ) ... end
gap>
gap> sumeigen:=function(G,S,t)
> local l,irr;
> irr:=Irr(G);
> l:=List(setproduct(S,t),i->classfinder(G,i));
> return List(irr,X->[Sum(l,i->X[i]), "deg=", X[1]]);
> end;
function( G, S, t ) ... end

```



```

gap>
gap> sumeigenn:=function(G,S,i)
> local l,X;
> X:=Irr(G)[i];
> l:=List(S,i->classfinder(G,i));
> return Sum(l,i->X[i]);
> end;
function( G, S, i ) ... end
gap>
gap> sumeigennn:=function(G,S,i)
> local d,X,l;
> X:=Irr(G)[i];
> d:=X[1];
> l:= List([1..d],j->sumeigenn(G,setproduct(S,j),i));
> return l;
> end;
function( G, S, i ) ... end
gap>
gap>
gap> newtonformulae:=function(L)
> local n,a,A,B,i;
> n:=Size(L); a:=-L[1]; A:=[a];
> for i in [2..n] do
> a:=- (1/i)*(Sum(List([1..i-1],j->L[j]*A[i-j]))+L[i]);
> Add(A,a);
> od;
> return A;
> end;
function( L ) ... end
gap>
gap>
gap> root:=function(G, L)
> local m,n,x,f,r;
> x:=Indeterminate(Rationals,"x");
> n:=Size(L);
> m:=Order(G);
> r:=Field(E(m));

```

```

> f:=Sum(List([1..n],j->L[j]*x^(n-j)))+x^n;
> return RootsOfPolynomial(r, f);
> end;
function( G, L ) ... end
gap>
gap> eigenX:=function(G,S,i)
> local d,X,l;
> X:=Irr(G)[i];
> d:=X[1];
>
> l:=root(G, newtonformulae(sumeigen(G,S,i)));
> return [l, d];
> end;
function( G, S, i ) ... end
gap>
gap> eigenCayley:=function(G,S)
> return List([1..Size(ConjugacyClasses(G))],i->eigenX(G,S,i));
> end;
function( G, S ) ... end
gap>
gap> listexpand:=function(L)
> local a,i,j;
> a:=[];
> for i in [1..Size(L[1])] do
> for j in [1..L[2]] do
> Add(a,L[1][i]);
> od;
> od;
> return a;
> end;
function( L ) ... end
gap>
gap> EigenCayley:=function(G,S)
> local e1,E1,a,B,i;
> E1:=[];
> e1:=eigenCayley(G,S);
> a:=List(e1,i->listexpand(i));

```

```

> for i in [1..Size(a)] do
> Append(E1,a[i]);
> od;
> B:=Set(E1);
> return List(B,i-> [i, Size( Filtered(E1,j->j=i)) ] );
> end;
function( G, S ) ... end
gap>
gap>
gap> G:=DihedralGroup(12);
<pc group of size 12 with 3 generators>
gap> A:=GeneratorsOfGroup(G);
[ f1, f2, f3 ]
gap> List(A, x->Order(x));
[ 2, 6, 3 ]
gap> B:=[A[1],A[2], A[3], Inverse(A[2]), Inverse(A[3])];
[ f1, f2, f3, f2*f3^2, f3^2 ]
gap> EigenCayley(G,B);
[ [-3, 2 ], [ -1, 5 ], [ 1, 3 ], [ 3, 1 ], [ 5, 1 ] ]
gap> G:=DihedralGroup(20);
EigenCayley(G,B);<pc group of size 20 with 3 generators>
gap> A:=GeneratorsOfGroup(G);
[ f1, f2, f3 ]
gap> List(A, x->Order(x));
[ 2, 10, 5 ]
gap> B:=[A[1],A[2], A[3], Inverse(A[2]), Inverse(A[3])];
[ f1, f2, f3, f2*f3^4, f3^4 ]
gap> EigenCayley(G,B);
[ [-2, 4 ], [ -1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 3, 1 ], [ 5, 1 ], [
-2*E(5)-2*E(5)^4, 2 ], [ -2*E(5)^2-2*E(5)^3, 2 ],
[ 2*E(5)^2+2*E(5)^3, 2 ], [ 2*E(5)+2*E(5)^4, 2 ] ]
gap>

```

B.2 Cayley graph construction with GRAPE

Following program will construct the Cayley graph, $\text{Cay}(G, S)$, where G is a finite group and S a symmetric generating set. We can compute the automorphism group of the graph as well.

```

gap>
gap>
gap>
gap> # We Test the isomorphism of graphs with Grape package in GAP
gap> # There are many more interesting functions to compute other graph parameters
gap>
gap>
gap> RequirePackage("grape");
-----
Loading GRAPE 4.6.1 (GGraph Algorithms using PErmutation groups)
by Leonard H. Soicher (http://www.maths.qmul.ac.uk/~leonard/).
Homepage: http://www.maths.qmul.ac.uk/~leonard/grape/
-----
true
gap> G:=DihedralGroup(20);
<pc group of size 20 with 3 generators>
gap> A:=GeneratorsOfGroup(G);
[ f1, f2, f3 ]
gap> List(A, x->Order(x));
[ 2, 10, 5 ]
gap> B:=[A[1],A[2], A[3], Inverse(A[2]), Inverse(A[3])];
[ f1, f2, f3, f2*f3^4, f3^4 ]
gap> gamma:=CayleyGraph(G,B);;
gap> Diameter(gamma);
4
gap> Girth(gamma);
3
gap> IsBipartite( gamma );
false
gap> IsDistanceRegular( gamma );
false
gap> IndependentSet( gamma ) ;
[ 1, 5, 7, 10, 12, 17 ]

```

```

gap> autG:=AutGroupGraph( gamma );;
gap> StructureDescription(autG);
"C2 x C2 x D10"
gap> cl:=List( ConjugacyClasses(G), x->Representative(x));
[ <identity> of ..., f1, f2, f3, f1*f2, f2*f3, f3^2, f2*f3^2 ]
gap> Group([cl[2],cl[5]])=G;
true
gap> C:=[cl[2],cl[5],cl[5]^-1];
[ f1, f1*f2, f1*f2 ]
gap> List(C, x->Order(x));
[ 2, 2, 2 ]
gap> gamma1:=CayleyGraph(G,C);;
gap> IsIsomorphicGraph( gamma1, gamma );
false
gap>

```

B.3 $(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ admits no connected cubic integral Cayley graph

Here we show that group $(\mathbb{Z}_6 \times \mathbb{Z}_2) \rtimes \mathbb{Z}_2$ does not admit a connected cubic integral Cayley graph.

```

gap> l := AllSmallGroups(24);; A:=Filtered(l, x->IsAbelian(x)=false);; B:=List(A,
  StructureDescription);
[ "C3 : C8", "SL(2,3)", "C3 : Q8", "C4 x S3", "D24", "C2 x (C3 : C4)", "(C6 x C2)
  : C2", "C3 x D8", "C3 x Q8", "S4",
  "C2 x A4", "C2 x C2 x S3" ]
gap>
gap>
gap>
gap>
gap> A[7];
(C6 x C2) : C2
gap> List(A[7], Order);

```

```

[ 1, 3, 3, 2, 6, 6, 2, 6, 6, 2, 6, 6, 2, 2, 2, 2, 2, 4, 4, 4, 4, 4, 4 ]
gap> a6:=Filtered(A[7], x->Order(x)=6);
[ f3*f4, f3*f4^2, f2*f4, f2*f4^2, f2*f3*f4, f2*f3*f4^2 ]
gap> a2:=Filtered(A[7], x->Order(x)=2);
[ f3, f2, f2*f3, f1, f1*f4, f1*f4^2, f1*f3, f1*f3*f4, f1*f3*f4^2 ]
gap> d:=[];
[ ]
gap> for x in a6 do
> for y in a2 do
> if Order(Group(x,y))=24 then
> Add(d, [x,x^-1,y]);
> fi;
> od;
> od;
gap> d;
[ [ f2*f4, f2*f4^2, f1 ], [ f2*f4, f2*f4^2, f1*f4 ], [ f2*f4, f2*f4^2, f1*f4^2 ],
  [ f2*f4, f2*f4^2, f1*f3 ],
  [ f2*f4, f2*f4^2, f1*f3*f4 ], [ f2*f4, f2*f4^2, f1*f3*f4^2 ], [ f2*f4^2, f2*f4,
  f1 ], [ f2*f4^2, f2*f4, f1*f4 ],
  [ f2*f4^2, f2*f4, f1*f4^2 ], [ f2*f4^2, f2*f4, f1*f3 ], [ f2*f4^2, f2*f4,
  f1*f3*f4 ],
  [ f2*f4^2, f2*f4, f1*f3*f4^2 ], [ f2*f3*f4, f2*f3*f4^2, f1 ], [ f2*f3*f4,
  f2*f3*f4^2, f1*f4 ],
  [ f2*f3*f4, f2*f3*f4^2, f1*f4^2 ], [ f2*f3*f4, f2*f3*f4^2, f1*f3 ], [ f2*f3*f4,
  f2*f3*f4^2, f1*f3*f4 ],
  [ f2*f3*f4, f2*f3*f4^2, f1*f3*f4^2 ], [ f2*f3*f4^2, f2*f3*f4, f1 ], [
  f2*f3*f4^2, f2*f3*f4, f1*f4 ],
  [ f2*f3*f4^2, f2*f3*f4, f1*f4^2 ], [ f2*f3*f4^2, f2*f3*f4, f1*f3 ], [
  f2*f3*f4^2, f2*f3*f4, f1*f3*f4 ],
  [ f2*f3*f4^2, f2*f3*f4, f1*f3*f4^2 ] ]
gap> s:=[];
[ ]
gap> for x in d do
> Add(s, EigenCayley(A[7],x));
> od;
gap> s;

```



```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ],
```

```
[ [-3, 1 ], [-2, 2 ], [-1, 1 ], [ 0, 4 ], [ 1, 1 ], [ 2, 2 ], [ 3, 1 ], [
  -E(8)+E(8)^3, 4 ], [ E(8)-E(8)^3, 4 ] ] ],
```

gap>

Bibliography

- [1] A. Abdollahi and M. Jazaeri: On groups admitting no integral Cayley graphs besides complete multipartite graphs, *Appl. Anal. Discrete Math.* 7 (2013), 119–128.
- [2] A. Abdollahi and E. Vatandoost: Which Cayley graphs are integral? *Electr. J. Combin.*, 16(1) (2009), R122, 1–17.
- [3] A. Abdollahi and E. Vatandoost: Integral quartic Cayley graphs on abelian groups, *Electr. J. Combin.*, 18: P89, 2011.
- [4] O. Ahmadi, N. Alon, I. F. Blake, I. E. Shparlinski: Graphs with integral spectrum, *Linear Alg. Appl.*, 430 (2009), 547–552.
- [5] A. Ahmady: Integral Cayley graphs of small degree, submitted.
- [6] A. Ahmady: Representation and character integral sets, submitted.
- [7] A. Ahmady and J. P. Bell: Integral Cayley graphs over dihedral groups, in preparation.
- [8] A. Ahmady and J. P. Bell: Simple eigenvalues in Cayley graphs, in preparation.
- [9] A. Ahmady, J. P. Bell and B. Mohar: Integral Cayley Graphs and Groups, submitted.
- [10] A. Ahmady, M. DeVos, R. Krakovski and B. Mohar: Integral Cayley multigraphs over Abelian and Hamiltonian groups, *Electr. J. Combin.*, to appear.
- [11] F. Annexstein, M. Baumslag, and A. L. Rosenberg: Group action graphs and parallel architectures, *SIAM J. Comput.*, 19 (1990), 544–569.
- [12] R. C. Alperin and B. L. Peterson: Integral sets and Cayley graphs of finite groups, *Electr. J. Combin.*, 19 (2012), no. 1, Paper 44, 12 pp.

- [13] L. Babai: Spectra of Cayley graphs, *Journal of Combinatorial Theory Ser. B*, 27 (1979), 180–189.
- [14] K. Balińska, D. Cvetković, M. Lepović, S. Simić: There are exactly 150 connected integral graphs up to 10 vertices, *Univ. Beograd. Publ. Elektrotehn. Fak., Ser. Mat.*, 10 (1999), 95–105.
- [15] K. Balińska, M. Kupczyk, S.K. Simić, K.T. Zwierzyński: On generating all integral graphs on 11 vertices, *The Technical University of Poznan, Computer Science Center Report No. 469*, (2000).
- [16] K. Balińska, D. Cvetković, Z. Rodosavljevic, S. Simić, D. Stevanović: A survey on integral graphs, *Univ. Beograd, Publ. Elektrotehn. Fak. Ser. Mat.* 13 (2003), 42–65.
- [17] M. Basić, M. Petković, D. Stevanović: Perfect state transfer in integral circulant graphs. *Appl. Math. Lett.* 22 (2009), no. 7, 1117–1121.
- [18] W. G. Bridges and R. A. Mena: Rational G-matrices with rational eigenvalues. *J. Combin. Theory, Ser. A* 32 (1982), 264–280.
- [19] F. C. Bussemaker, D. Cvetković: There are exactly 13 connected, cubic, integral graphs. *Univ. Beograd, Publ. Elektrotehn. Fak., Ser. Mat. Fiz., Nos. 544–576* (1976), 43–48.
- [20] G. Cooperman and L. Finkelstein: New methods for using Cayley graphs in interconnection networks, *Discrete Appl. Math.* 37–38 (1992), 95–118.
- [21] G. Cooperman , L. Finkelstein , N. Sarawagi: Applications of Cayley graphs, *App. Alg., Lecture Notes in Comput. Sci.* 508, Springer-Verlag, Berlin (1991), 367–378.
- [22] D. Cvetković, I. Gutman, N. Trinajstić: Conjugated molecules having integral graph spectra. *Chem Phys. Letters*, 29 (1974), 65–68.
- [23] D. Cvetković, P. Rowlinson, S. Simić: *An Introduction to the Theory of Graph Spectra.* London Mathematical Society, Student Texts 75, 2010.
- [24] D. Cvetković, S. Simić, D. Stevanović: 4-regular integral graphs. *Univ. Beograd, Publ. Elektrotehn. Fak., Ser. Mat.*, 9 (1998), 89–102.
- [25] P. Diaconis and M. Shahshahani: Generating a random permutation with random transpositions. *Z. Wahrsch. Verw. Gebiete* 57 (1981), 159–179.

- [26] W. Fulton and J. Harris: Representation Theory. A first course, Springer-Verlag, 1991.
- [27] Y. Gomi, T. Maeda, K. Shinoda: Gauss sums on finite groups. *Tokyo J. Math.* 35 (2012), no. 1, 165–179.
- [28] C. Godsil and G. Royle: Algebraic Graph Theory. Graduate Texts in Mathematics. Vol. 207. Springer, 2001.
- [29] C. Godsil: State transfer on graphs, *Discrete Math.* 312 (2012), no. 1, 129–147.
- [30] M. Hall: The Theory of Groups, Macmillan, New York, 1959.
- [31] A. J. Hoffman: On the polynomial of a graph, *Amer. Math. Monthly* 70 (1963) 30–36.
- [32] F. Harary and A. J. Schwenk: Which graphs have integral spectra? in “Graphs and Combinatorics (Proc. Capital Conf., George Washington Univ., Washington, D.C., 1973)”. *Lecture Notes in Mathematics* 406. Springer, Berlin (1974), 45–51.
- [33] K. Hoffman and R. A. Kunze: Linear Algebra, Prentice-Hall; 2nd Ed., p. 407, 1971.
- [34] T. W. Hungerford: Algebra, Springer; Graduate Texts in Mathematics, Vol. 73, p. 504, 1980.
- [35] A. Ilić, M. Basić: New results on the energy of integral circulant graphs. *Appl. Math. Comput.* 218 (2011), no. 7, 3470–3482.
- [36] G. James and M. Liebeck: Representations and Characters of Groups. Second edition. Cambridge University Press, 2001.
- [37] D. Kletzing: Structure and Representations of Q-Groups, Springer Lecture Notes in Mathematics, Vol. 1084, p. 290, 1984.
- [38] W. Klotz and T. Sander: Integral Cayley graphs over abelian groups, *Electron. J. Combin.* 17 (2010), no. 1, Research Paper 81, 13 pp.
- [39] K. H. Leung, B. Schmidt: The field descent method. *Des. Codes Cryptogr.* 36 (2005), no. 2, 171–188.
- [40] K. H. Leung, B. Schmidt: New restrictions on possible orders of circulant Hadamard matrices. *Des. Codes Cryptogr.* 64 (2012), no. 1-2, 143–151.

- [41] M. W. Liebeck, C. E. Praeger, J. Saxl: Regular subgroups of primitive permutation groups. *Mem. Amer. Math. Soc.* 203 (2010), No. 952.
- [42] G. A. Miller and H. C. Moreno: Non-abelian groups in which every subgroup is abelian, *Trans. Amer. Math. Soc.* 4 (1903), 398–404.
- [43] M. Minchenko and I. M. Wanless: Spectral moments of regular graphs in terms of subgraph counts. Submitted.
- [44] M. Minchenko and I. M. Wanless: Quartic integral Cayley graphs. In preparation.
- [45] D. S. Mitrinović and J. Sándor, *Handbook of Number Theory*. Dordrecht, Netherlands: Kluwer, 1995.
- [46] R. W. K. Odoni: Weil numbers and CM fields. II. *J. Number Theory* 38 (1991), no. 3, 366–377.
- [47] D. J. S. Robinson: *A Course in the Theory of Groups*, Springer; Graduate Texts in Mathematics, Vol. 80, 2nd ed., XVIII, p. 499, 1996.
- [48] D. Rockmore, P. Kostelec, W. Hordijk, and P. Stadler: Fast fourier transforms for fitness landscapes. *Applied and Computational Harmonic Analysis*, 12(1) (2002), 57–76.
- [49] M. Roitman: An infinite family of integral graphs, *Discrete Math.* 52 , No.2 (1984), 313–315.
- [50] H. Sachs, M. Stiebitz: Automorphism group and spectrum of a graph. *Studies in pure mathematics*, 587–604, Birkhauser, Basel, 1983.
- [51] A. J. Schwenk: Exactly thirteen connected cubic graphs have integral spectra. *Proceedings of the International Graph Theory Conference at Kalamazoo*, (Y. Alavi and D. Lick, eds.) Springer-Verlag. May 1976.
- [52] W. So: Integral circulant graphs. *Discrete Math.* 306 (2005), 153–158.
- [53] D. Stevanović: Nonexistence of some 4-Regular integral graphs, *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.*, 10, (1999).
- [54] D. Stevanović: 4-Regular integral graphs avoiding ± 3 in the spectrum, *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.*, (2003), 99–110.

- [55] D. Stevanović, N. M. M. de Abreu, M. A. A. de Freitas, and R. Del-Vecchio: Walks and regular integral graphs. *Linear Algebra Appl.*, 423(1) (2007), 119–135.
- [56] D. Stevanović: Applications of graph spectra in quantum physics, in: D. Cvetkovic, I. Gutman, *Selected Topics on Applications of Graph Spectra*, Mathematical Institute SANU, Belgrade, 2011, pp. 85–111.
- [57] R.J. Turyn: Character sums and difference sets, *Pacific J. Math.* 15 (1965), 319–346.
- [58] L. Wang and H. Sun: Infinitely many pairs of cospectral integral regular graphs, *Appl. Math. J. Chinese Univ.*, No. 26(3) (2011), 280–286.