Self-Complementary Vertex-Transitive Graphs

Guang Rao

This thesis is presented for the degree of
Doctor of Philosophy
of The University of Western Australia
School of Mathematics & Statistics.
September 8, 2014

Abstract

A graph Γ is *self-complementary* if its complement is isomorphic to the graph itself. An isomorphism that maps Γ to its complement $\overline{\Gamma}$ is called a *complementing isomorphism*. The majority of this dissertation is intended to present my research results on the study of self-complementary vertex-transitive graphs. I will provide an introductory mini-course for the backgrounds, and then discuss four problems: constructions of self-complementary vertex-transitive graphs, self-complementary vertex-transitive graphs of order a product of two primes, self-complementary metacirculants, and self-complementary vertex-transitive graphs of prime-cube order. The main analysis on these problems relies on the two pivotal results due to Guralnick et al. [22] and Li, Praeger [31], which characterise the full automorphism group of a self-complementary vertex-transitive graph in the primitive and the imprimitive cases respectively.

For constructions of self-complementary vertex-transitive graphs, there are generally three known construction methods: construction by partitioning the complementing isomorphism orbits; construction using the coset graph; the lexicographic product. In this dissertation I shall develop various alternative construction methods. As a result, I find a family of self-complementary Cayley graphs of non-nilpotent groups, a new construction for self-complementary metacirculants of p-groups.

A *complementing isomorphism* of a self-complementary graph is an isomorphism between the graph and its complement. For the self-complementary vertex-transitive graphs whose automorphism groups are of affine type, we have obtained a characterisation of all their complementing isomorphisms. Furthermore, we provide a construction of self-complementary metacirculants which are Cayley graphs and have insoluble automorphism groups. This is the first known example with this property in the literature.

For the self-complementary vertex-transitive graphs of order a product of two primes, we give a complete classification of these graphs: they are either a lexicographic product of two self-complementary vertex-transitive graphs of prime order, or a normal Cayley graph of an abelian group.

A graph is called a *metacirculant* if its full automorphism group contains a transitive metacyclic subgroup. We shall explore self-complementary metacirculants and show that the full automorphism group of these graphs is either soluble or contains the only insoluble composition factor A_5. This extends a result due to Li and Praeger [32] which says that the full automorphism group of a self-complementary circulant is soluble.

Finally, we will investigate self-complementary vertex-transitive graphs of prime-cube order. We successfully show that for each type of the groups of prime-cube order, there exist self-complementary Cayley graphs of the corresponding groups. Moreover, we also gain a characterisation of all the self-complementary vertex-transitive graphs of prime-cube order: they are normal Cayley graphs, or a lexicographic product of two smaller self-complementary vertex-transitive graphs, or their automorphism group is soluble.

Acknowledgements

The University of Western Australia, is the university where I spent my entire five-year postgraduate study, including my completed master degree, and thenceforth my PhD. This period was bittersweet, which I think would never be repeated again in my life. I still can remember the first day that I came to Perth, Australia, kicking start my fresh ever oversea study, I was so excited but dumb at almost everything. In contrast, now I have been honed to fully adapt the study and lifestyle here.

Studying in mathematics is usually a tough work, especially for those who study mathematics in high level. Luckily, there are many nice people in my math school. In particular, my math school has a very strong and active research group — Centre for the Mathematics of Symmetry and Computation. Here, I met many world-wide highly recognised mathematicians, and of course my master supervisors and my PhD supervisors as well.

I was very grateful that my principal PhD supervisor, Winthrop Professor Cai Heng Li, who is known as a famous expert in my research area, and who eventually took major care of my PhD study, agreed to be my supervisor. It was my fortune and honor to have this precious chance. I very admire his great knowledge in the research area and his insightful viewpoint of the problems. He could always give me useful and illuminating comments on my work, and helped solve numerous problems, not only those in research, but also the difficulties I encountered in my life. My gratitude should also extend to his spouse, Doctor Jian Ping Wu, who is also working as a researcher in the same department, for her kindness, helpful tips in life, and her consistent passion on organising many many enjoyable activities.

Professor Gordon Royle, as my second PhD supervisor, has also assisted me in aspects of areas. Remember the time that I was preparing the slides for a presentation for my research proposal, I was very lost about how I could give a good presentation. He made many constructive suggestions to me and leaded me to a clear thought. As a result, I did quite well in my talk and had my proposal approved by Graduate Research School. He always has an agile mind and can show me a different way to approach the problems.

Doctor Shu Jiao Song, as my additional PhD supervisor, took over Cai Heng Li's supervision work while Cai Heng was oversea. She did a fantastic job in supervising

me. For that period, we always had long discussions and met each other frequently over the weeks. We solved a lot of critical problems together and made heaps of substantial progress in the research. I very appreciate her time spent with me and her patience in supervising me.

Moreover, I should definitely need to say thank you to my parents for their countless support. Being in Australia for my postgraduate study, I had to stay apart from my family. I know they suffered a lot for this longish time, especially for the lonely feeling that one had to bear.

Besides, I am thankful to all the friends, whom I got to know in Perth while I was doing my study and whom I knew in China, for their company and encouragements. I treasure the joy we shared, the place we travelled together, and the fun we had. This helped me kill the time and refresh myself when I got stuck in research. Especially I want to cheer to those who discussed math problems with me. That was truly a great fun!

Contents

List of Figures

Chapter 1

Introduction

Talking about a graph in graph theory we usually mean a set of nodes together with some links between these nodes. The model of graphs can be used to represent miscellaneous types of relations and processes in physical, biological, social and information system [1].

One approach in the study of graphs lies in combinatorics, from which point of view the term "self-complementary" arises. A graph is *self-complementary* if the graph and its complement can be rearranged to have the same look. Self-complementary graphs have been introduced for longer than half a century [50] and have been studied extensively, see Section 1.2 for a further elucidation.

On the other hand, algebraic graph theorists concentrate on applying algebraic tools and methods to characterise properties of a graph. One of the main streams of this is to use group theory to describe the symmetry of a graph. Usually, by equipping a graph with some algebraic conditions, one could discover many beautiful properties of the graph. There are various terms for describing a graph with high symmetry in group-theoretic language, such as vertex-transitive, edge-transitive, symmetric, distance-transitive etc. In particular, *vertex-transitive* is possibly the simplest and the most commonly heard one in algebraic graph theory. Intuitively, a vertex-transitive graph is a graph all of whose vertices are not distinguishable from one another. A huge amount of research has been carried out for this type of graphs, see [19] for a detailed introduction. In this dissertation we discuss a specific object in the field — self-complementary vertex-transitive graphs.

1.1 The Objective and Main Results

To determine the self-complementary graphs of a given order is to ask how one can bisect the edge set of a complete graph of this order in a way such that the graph with the first part of the edges looks exactly the same as the graph with the second part. It is obvious that this problem itself is interesting. However, solving this problem is extremely hard. In fact, it is known [12] that the problem of checking a given graph is self-complementary or not are polynomial-time equivalent to the general graph isomorphism problem — one of the only two unresolved problems

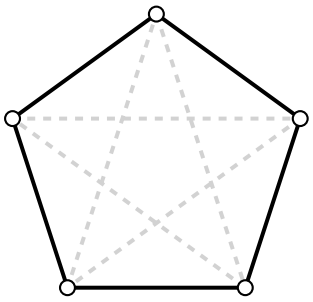


Figure 1.1: The smallest self-complementary vertex-transitive graph

(the other being integer factorisation) listed by Garey and Johnson [17] that are unknown to be NP-complete nor tractable.

In the meantime, vertex-transitivity provides a very nice property for graphs. Technically, a graph is *vertex-transitive* if its automorphism group is transitive on its vertex set. By imposing the vertex-transitivity property on a graph, one may interpret the automorphism group of the graph as a transitive permutation group. Consequently, we can investigate the graphs by taking normal quotients of the vertex set and hence study the quasiprimitive actions. For transitive permutation groups, fruitful results have been obtained (for example, the famous O'Nan–Scott theorem [37]).

Over the recent decades, the study of self-complementary vertex-transitive graphs has been significantly progressed (see [22, 30, 31]). In particular, a generalised notion called homogeneous factorisations of a complete graph (see Section 1.2) was introduced. This renders the complexity of the study of self-complementary vertex-transitive graphs much reduced. The chief goal of this dissertation is to characterise the structures of special families of self-complementary vertex-transitive graphs and hence find new construction methods for self-complementary vertex-transitive graphs. The main results of this dissertation are encapsulated below.

1.1.1 Self-complementary graphs of non-nilpotent groups

So far, most known self-complementary vertex-transitive graphs are constructed via method given in Section 3.1, which is in particular based on Cayley graphs. Moreover, to the best of our knowledge, all known examples of self-complementary Cayley graphs are Cayley graphs of nilpotent groups.

In Section 3.3 we will present a new construction of self-complementary vertex-transitive graphs, which provides a family of self-complementary Cayley graphs of non-nilpotent groups.

1.1.2 A construction of self-complementary metacirculants

We call a graph Γ a *metacirculant* if its full automorphism group $\mathsf{Aut}\Gamma$ contains a metacyclic transitive subgroup. In particular, if $\mathsf{Aut}\Gamma$ contains a transitive cyclic subgroup, then Γ is a *circulant*. According to the results in [25, 38], there are self-complementary circulants that cannot be constructed by the construction method

provided in Section 3.1. Thus, it is necessary to seek other methods to construct these graphs.

In Chapter 4 we will introduce a method to construct a class of self-complementary Cayley graphs of non-abelian metacyclic p-groups.

1.1.3 Self-complementary vertex-primitive graphs

The graphs that are vertex primitive is a very important case among the investigations in self-complementary vertex-transitive graphs. By a theorem stated in [22] by Guralnick et al., the full automorphism group of a self-complementary vertex-primitive graph is either affine, or of product action type. As the product action type is somewhat well understood, the study of the affine case turns out to be critical.

Given a self-complementary vertex-transitive graph Γ, a *complementing isomorphism* of Γ is a graph isomorphism that interchanges Γ and its complement $\overline{\Gamma}$. For the self-complementary vertex-primitive graphs that has an affine full automorphism group, we have gained a characterisation of their complementing isomorphisms in Chapter 5, and hence we are able to construct these graphs.

In order to consolidate our result, we are able to provide a construction in Section 5.3 for self-complementary metacirculants which are Cayley graphs and have insoluble automorphism groups. To the best of our knowledge, this the first example of self-complementary graphs with this property. Consequently, it yields the existence of a self-complementary metacirculant of which the automorphism group is insoluble (see Lemma 5.3.4). Moreover, we further generalise this construction in Section 7.2 such that there are self-complementary metacirculants whose automorphism groups contain arbitrarily many insoluble factor A_5.

1.1.4 The pq-case

By the pq-case we mean the study of self-complementary vertex-transitive graphs of order pq, where p, q are primes. The early study of this case was not easy, for instance, Koolen [26] in 1997 derived the non-existence of the self-complementary vertex-transitive graphs of order $3p$. In 1979, it was first conjectured by Zelinka [55] that the existence of a self-complementary vertex-transitive graph of order a product of two distinct primes p, q implies both p, q are congruent to 1 module 4. This was confirmed by Li [27] later. However, the knowledge of the structure of such kind of graphs was very limited, until a complete classification [33] was obtained in my PhD project. In Chapter 6 we shall provide a decent approach to the classification.

In details, we showed that a self-complementary vertex-transitive graph of order a product of two primes is one of the following:

(i) a lexicographic product of two self-complementary vertex-transitive graphs, of which each is a circulant of prime order; or

(ii) a normal Cayley graph of an abelian group.

A consequence of this result tells that a self-complementary vertex-transitive graph of order a product of two distinct primes is necessarily a circulant.

1.1.5 Self-complementary metacirculants

Self-complementary circulants have been widely studied since the first family of such graphs was constructed by Sachs [50] in 1962. In particular, the automorphism group of self-complementary circulants have been proved to be soluble [32].

In contrast, not much attention has been drawn to self-complementary metacirculants. In Chapter 7 we characterise the automorphism group of a self-complementary metacirculant and show that the automorphism group of a self-complementary metacirculant is either soluble or contains A_5 as its only insoluble composition factor.

A metacirculant Γ is said to be a *Sylow-circulant* if $\mathsf{Aut}\Gamma$ has a transitive metacyclic subgroup R of which all Sylow subgroups are cyclic. In this case, the group R has a normal Hall subgroup N such that the orders N and R/N are coprime. Based on the information we have about self-complementary metacirculants, a self-complementary Sylow-circulant must have a soluble automorphism group. In particular, if a self-complementary metacirculant is of a square-free order, then its automorphism group is soluble.

1.1.6 The p^3-case

In Chapter 8 we will explore the p^3-case, that is, the self-complementary vertex-transitive graphs of prime-cube order. Since we have studied the pq-case and self-complementary metacirculants, the study of self-complementary vertex-transitive graphs of prime-cube order is a natural extension.

It has been determined that the vertex-transitive graphs of prime-cube order are all Cayley graphs (see [41]). Thus, we will in fact study self-complementary Cayley graphs of order p^3. There are in total five non-isomorphic groups of order p^3 (refer to [3, Section 8]):

$$\mathbb{Z}_p^3,\ \mathbb{Z}_p \times \mathbb{Z}_{p^2},\ \mathbb{Z}_{p^3},\ \mathbb{Z}_p^2{:}\mathbb{Z}_p,\ \mathbb{Z}_{p^2}{:}\mathbb{Z}_p.$$

In Section 8.2 and Section 8.3 we will show that for each type of these groups, there always exist self-complementary Cayley graphs of the corresponding group.

Furthermore, we also give a characterisation of self-complementary vertex-transitive graphs of prime-cube order. They are normal Cayley graphs, or a lexicographic product of two smaller self-complementary vertex-transitive graphs, or the full automorphism group is soluble (see Theorem 8.1.2).

1.2 Background

The idea of self-complementary seems purely of combinatorial flavor while the concept of vertex-transitive is much more algebraic. Hence, the definition of self-complementary vertex-transitive graphs sounds like describing a graph in both combinatorial and algebraic language. In algebraic graph theory, such way of mingling a combinatorial object with some algebra is always desired. But the meaning of studying self-complementary vertex-transitive graphs is far more beyond this.

In fact, the properties of self-complementary vertex-transitive graphs filter most of the graphs. For an illustration, according to Beezer's survey [6], there are totally 50 502 031 367 952 non-isomorphic graphs on 13 vertices, of which 5 600 are self-complementary, and 14 are vertex-transitive, but only two are both self-complementary and vertex-transitive. However, these graphs have important applications in many different areas. One of the typical applications is to be used for bounding diagonal Ramsey numbers [10, 11, 23]. For instance, Luo et al. [23] achieved 3 new lower bounds for diagonal Ramsey numbers by considering some properties of self-complementary graphs. The *diagonal Ramsey number* $R(n, n)$ is the least integer such that for any graph of that order, or greater, neither the graph itself nor its complement contains a complete subgraph of size n. Ideally, one may expect the edges of the graph distribute equivalently. Thus, the additional property of vertex-transitivity comes naturally. Furthermore, self-complementary vertex-transitive graphs also play a key role in the research of message transmission [40]. In information theory, the Shannon capacity is used to measure the highest rate of the reliable information transmission over a certain communication channel. However, "the computational complexity of the Shannon capacity is unknown, and even the value of the Shannon capacity for certain small graphs such as $\mathbf{C}_7$ (a cycle graph of seven vertices) remains unknown [2]."Nonetheless, the Shannon capacity of a self-complementary vertex-transitive graph of order n has been found to be $\sqrt{n}$ [40].

The study of self-complementary vertex-transitive graphs has a long history. Readers may refer to a wonderful survey in 2006 due to Beezer [6]. I will give a few details here.

The initial study of self-complementary vertex-transitive graphs dates back to 1962, more than half a century ago. Sachs [50], as one of the early endeavorers in studying self-complementary graphs, he established many general properties of self-complementary graphs. In particular, he studied the order of self-complementary circulants and gave a corresponding construction method. Since then, these graphs have attracted plenty of interest.

Early study of self-complementary vertex-transitive graphs has its main focus on numerical problems, such as enumerations, the orders of the graphs (see [15, 27, 28, 47, 50, 55]). Among these problems, the study of the orders of self-complementary vertex-transitive graphs lasted for more than two decades. In 1979, Zelinka [55] showed that if there exists a self-complementary vertex-transitive graph, then its order is congruent to 1 modulo 4, and he also proposed the correctness of the converse. In 1996, Fronček, Rosa and Širáň [15] solved the problem on the circulant case. (See [4] for an alternative proof using simple algebraic method.) They further suggested an existence condition when the order of a self-complementary vertex-transitive graph is a product of two distinct primes. This question was solved one year later by Li [27]. In 1998, Li [28] also wrote a survey concerning the general order problem on self-complementary vertex-transitive graphs. The general problem was finally resolved in 1999 by Muzychuck [43] who showed that a self-complementary vertex-transitive graph of order n exists if and only if p^m is congruent to 1 modulo

4 for each p^m, the highest power of a prime p which divides n. The paper is surprisingly short — only 3-page long! His proof introduced a concept of *Sylow subgraphs*, which is similar to the concept of Sylow p-subgroups in finite group theory.

Rather than the order problem, a lot of effort had also been made in self-complementary circulants. A *circulant* is a graph whose full automorphism group admits a transitive cyclic subgroup. Circulants are necessarily vertex-transitive. The first construction method of self-complementary circulants was given by Sachs [50] in 1962. After that, Zelinka [55], Mathon [42], Rao [46], and Suprunenko [51] did further study on self-complementary circulants.

Given a graph, an *arc* is an ordered pair of adjacent vertices in the graph. A graph is *symmetric* if its automorphism group is transitive on all the arcs of the graph. It is easy to see that a connected symmetric graph is vertex-transitive. Some nice results in self-complementary symmetric graphs were obtained between early 1990s and early 2000s. In 1992, Zhang [56] gave a characterisation on automorphism groups of all self-complementary symmetric graphs. After about ten years, Peisert [44] gave a full classification of self-complementary symmetric graphs, which says that self-complementary symmetric graphs consist of Paley graphs, one infinite family of graphs and one exceptional graph. In comparison with the definition of "symmetric", a weaker version is "*edge-transitive*", which means the full automorphism group of the graph is transitive on the edge set of the graph. By presenting a classification of edge-transitive circulants, Zhang [57] also successfully showed that all self-complementary symmetric circulants are Paley graphs.

Cayley graphs (defined later), are an important family of vertex-transitive graphs. Most of the constructions of self-complementary Cayley graphs involve in using group automorphisms of the underlying group of the Cayley graph (see [46, 50, 51, 55]). Hence, a few researchers turned to look for the *non self-complementary Cayley isomorphism graphs* (see [25, 38]), that is, the self-complementary Cayley graphs that are not constructed from the above-mentioned method. Moreover, it is worth mentioning that before the 21st century, all known self-complementary vertex-transitive graphs were Cayley graphs. A family of non-Cayley graphs was finally discovered in 2001 by Li and Praeger [29], which shows that there exist self-complementary vertex-transitive graphs which are not Cayley graphs.

In the 21st century, the study of self-complementary vertex-transitive graphs has been raised to a new high level (see [18, 22, 30, 31, 32, 45]). In 2002, Li and Praeger [30, 31] first realised the notion of a self-complementary vertex-transitive graph can be generalised to the concept of TODs (transitive orbital decompositions), or homogeneous factorisations of complete graphs. Given a complete graph of order n, a *homogeneous factorisation* of this graph is a decomposition of the graph into k mutually isomorphic subgraphs with the same vertex set, such that there exists a permutation group $G < \mathrm{S}_n$ on these vertices, which leaves the decomposition invariant, permutes all the k subgraphs transitively, and induces a transitive automorphism group on each of the subgraphs. Self-complementary vertex-transitive graphs exactly correspond to the homogeneous factorisations when $k = 2$. In 2004, with a further collaboration with Guralnick and Saxl they studied the vertex-primitive case

[22]. Later, the idea of homogeneous factorisations was also extended to arbitrary graphs and digraphs [18]. The research of homogeneous factorisations has opened the door for more detailed study in self-complementary vertex-transitive graphs. As a consequence, a few more investigations [32, 33, 34, 45] in specific topics have been carried out.

1.3 Structure of the Dissertation

This section is dedicated for an explanation of the structure of this dissertation.

In Chapter 2, we will introduce the basic concepts of groups and graphs, and then collect some necessary preliminary results for the proof of our main results.

In Chapter 3, we will first present a classical method to construct self-complementary vertex-transitive graphs. The construction method is based on the fixed-point-free automorphisms of groups. This leads us to study the associated problems regarding to the fixed-point-free automorphisms. Furthermore, we construct an infinity family of self-complementary Cayley graphs of non-nilpotent groups, which is inspired by the classical construction method.

As an extension of Chapter 3, we introduce more construction methods in Chapter 4 for self-complementary vertex-transitive graphs. In particular, we find a new construction method to construct a family of self-complementary Cayley graphs of non-abelian metacyclic groups.

In Chapter 5, we will consider the primitive case, that is, the self-complementary vertex-transitive graphs which are vertex primitive. We will focus on the affine case and give a characterisation of the corresponding complementing isomorphisms. Consequently, we are able to construct all the corresponding graphs using these complementing isomorphisms. In addition, we provide an example of self-complementary metacirculants which are Cayley graphs and have insoluble automorphism groups.

In Chapter 6 we study the pq-case, that is, the self-complementary vertex-transitive graphs of order pq where p, q are primes and not necessarily equal. By discussing the primitive case and the imprimitive case, we obtain a complete classification for all the self-complementary vertex-transitive graphs of order pq. Moreover, we also have a complete list of the point stabilisers when the graph is vertex primitive.

Chapter 7 is devoted to the investigation on self-complementary metacirculants. We first generalise the example that we developed in Chapter 5. Consequently, we show that there are self-complementary metacirculants whose automorphism groups contain a section $\mathrm{A}_5 \times \cdots \mathrm{A}_5$, where the copies of A_5 can be arbitrarily many. After that we discuss the primitive and the imprimitive case for self-complementary metacirculants, and show that the full automorphism group of a self-complementary metacirculant is either soluble or contains A_5 as its only insoluble composition factor.

Finally, in Chapter 8 we will explore the self-complementary vertex-transitive graphs of prime-cube order. We first show that for each of the five types of groups of order p^3 with p being a prime, there are self-complementary Cayley graphs of the corresponding groups. Further, we characterise all the self-complementary vertex-

transitive graphs of prime-cube order in Theorem 8.1.2, which says that a self-complementary vertex-transitive graph Γ of prime-cube order is one of the following:

(i) a normal Cayley graph of prime-cube order;

(ii) a lexicographic product of two smaller self-complementary vertex-transitive graphs;

(iii) the full automorphism group $\mathsf{Aut}\Gamma$ is soluble, and the vertex set has block systems of size p and p^2.

Chapter 2

Groups and Graphs

In the field of algebraic graph theory, groups and graphs are the most elementary objects; and they have a lot of interplays between each other. Therefore, it is necessary to spare this chapter for a short course on groups and graphs, and keep it for a further reference. For group theory, the author shall adopt most of the notations and results from [3, 13, 48, 52]; for graph theory, the main source of terminology is from [8, 19].

Part I – Groups

2.1 Concepts of Groups

A *group* is a set G together with a binary operation

$$\cdot : G \times G \to G$$

satisfying the conditions below:

(i) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for each $x, y, z \in G$. (Associativity)

(ii) There exists an element $1 \in G$, called the *identity* element of G, such that $x \cdot 1 = 1 \cdot x = x$ for each $x \in G$. (Existence of an identity element)

(iii) For each $x \in G$ there exists $x^{-1} \in G$, called the *inverse* of x, such that $x \cdot x^{-1} = x^{-1} \cdot x = e$. (Existence of an inverse for each $x \in G$)

We will write xy in place of $x \cdot y$ from now on. If $G = \{1\}$, then we simply write $G = 1$. The *order* of a group G is the number of elements of G, denoted by $|G|$. A group G is *finite* if $|G|$ is finite. Throughout this dissertation all groups are assumed to be finite.

We will also assume that readers are familiar with the basic terminology of groups. Let G, K be groups and let H be a subgroup of G. Let $x, y \in G$ and let S be a subset of G. In the following we list some of those most commonly-used notations:

- $o(x)$: the order of x.
- S^x: the set consists of the elements $x^{-1}sx$ for all $s \in S$.
- $\langle S \rangle$: the group generated by the elements of S.
- xH (or Hx): the left (or right) coset with the representative x.
- $[G : H]$: the set of all the right cosets of H in G.
- $|G : H|$: the index of H in G.
- $H < G$ (or $H \leq G$): H is a proper subgroup of G (or H is a subgroup of G).
- $H \lhd G$ (or $H \trianglelefteq G$): H is a proper normal subgroup of G (or H is a normal subgroup of G).
- The *commutator* of x and y is $[x, y] := x^{-1}y^{-1}xy$.
- H char G: H is characteristic in G.
- $G \times K$: the direct product of G and K.
- $\mathbf{Z}(G)$: the centre of G.
- The *normal closure* of S in G is $S^G := \langle g^{-1}Sg | g \in G \rangle$.
- Suppose that there is a group homomorphism $\rho : G \to K$. The *kernel* of ρ is $\mathsf{Ker}\,\rho := \{g \in G | \rho(g) = 1\}$ and the *image* of ρ is $\mathsf{Im}\,\rho := \{\rho(g) | g \in G\}$.
- $\mathsf{Aut}(G)$: the full automorphism group of G.
- $G \cong K$: G is isomorphic to K.
- $G \lesssim K$: G is isomorphic to a subgroup of K.
- $G^{\#}$: the set of all the non-identity elements of G.

A group G is *abelian* if $xy = yx$ for all $x, y \in G$. A subclass of abelian groups are *cyclic groups* — the groups that are generated by a single element. The cyclic group of order n is denoted by $\mathbb{Z}_n$.

Let G be a group and let N be a normal subgroup of G. The set $[G : N]$ together with the operation $(Nx)(Ny) := Nxy$ forms the *quotient group* of G by N, denoted by G/N. Assume that $G/N \cong M$ for some group M. We sometimes write $G = N.M$, and say that G is an *extension of N by M*. Especially, if $N \cong \mathbb{Z}_n, M \cong \mathbb{Z}_m$ for some $n, m \in \mathbb{N}$, then we say G is *metacyclic*.

Lemma 2.1.1. *A subgroup or quotient group of a metacyclic group is also metacyclic.*

Proof. Let $G = N.M$ be a metacyclic group with $N \cong \mathbb{Z}_n, M \cong \mathbb{Z}_m$. Let $H < G$ and let $K \lhd G$.

Consider the subgroup H. Notice that $N \cap H \lhd H$, which is cyclic. Moreover,

$$H/(N \cap H) \cong HN/N \leq G/N \cong M,$$

so H is metacyclic.

Consider the quotient group G/K. Since $K \cap N$ is normal in N, we have

$$KN/K \cong N/(K \cap N) \text{ is cyclic.}$$

Note that both K, N are normal in G, so is KN, and

$$(G/K)/(KN/K) \cong G/KN \cong (G/N)/(KN/N) \cong M/(KN/N).$$

A quotient group of a cyclic group M is surely cyclic, then it follows G/K is metacyclic. □

Given a group G, the group $G' := \langle [x, y] \mid x, y \in G \rangle$ is called the *derived group* of G. Since the set of commutators is invariant under the group automorphisms of G, it follows that G' is a characteristic subgroup of G; moreover, G' is the largest normal subgroup of G such that G/G' is abelian ([3, Proposition 1.6]). Let $G^{(0)} := G$, $G^{(1)} := G'$. We define $G^{(k)}$ to be the derived group of $G^{(k-1)}$ for all $k \in \mathbb{N}$. It is evident that $G^{(k)}$ is a characteristic subgroup of G for each k.

Lemma 2.1.2. [48, 1.5.6 (iii)] *Let H, K be subgroups of a group G. If K is characteristic in H, and H is normal in G, then K is normal in G.*

Let G be a group and let $H, K \leq G$. We define a *double coset* of H and K in G to be the set $HxK = \{hxk | h \in H, k \in K\}$ for some $x \in G$. Pick two distinct double cosets HxK and HyK such that $(HxK) \cap (HyK) \neq \emptyset$. Then there exist $h_1, h_2 \in H$ and $k_1, k_2 \in K$ with $h_1 x k_1 = h_2 y k_2$, which follows that $x \in HyK$ and $y \in HxK$, and so $HxK = HyK$. Thus, any two double cosets are either disjoint or equal.

2.2 Permutation Groups

Throughout this section Ω denotes a non-empty finite set.

Each bijection of Ω onto itself is called a *permutation* of Ω. One can easily check that the set of all the permutations of Ω forms a group under the mapping composition. This set is usually denoted by $\mathrm{Sym}(\Omega)$. In the case that $\Omega = \{1, \ldots, n\}$, the group $\mathrm{Sym}(\Omega)$ is also denoted by S_n, and is called the *symmetric group of degree n*. Any subgroup of $\mathrm{Sym}(\Omega)$ is said to be a *permutation group* on Ω.

An important subgroup of S_n is the *alternating group* A_n — the derived subgroup of S_n.

Theorem 2.2.1. ([48, Theorem 3.2.1 and 3.2.3])

(i) A_n *is simple if and only if* $n \neq 1, 2$ *or* 4.

(ii) *If* $n \neq 4$, *then* A_n *is the only normal subgroup of* S_n.

It is easy to see that A_n is not abelian if $n \geq 4$, hence a consequence of the above theorem is that A_n is insoluble for every $n \geq 5$.

Let G be a group. For each $\alpha \in \Omega, x \in G$, define a function $(\alpha, x) \mapsto \alpha^x$ from $\Omega \times G$ into Ω. Then this function defines an *action* of G on Ω (or G *acts* on Ω) if the function satisfies:

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$; and

(ii) $(\alpha^x)^y = \alpha^{xy}$ for all $\alpha \in \Omega$ and all $x, y \in G$.

In fact, each element x in G induces a permutation of Ω by the map $\bar{x} : \alpha \mapsto \alpha^x$ for all $\alpha \in \Omega$. Therefore, there is a natural group homomorphism $\rho : G \to \mathrm{Sym}(\Omega)$ given by $\rho(x) := \bar{x}$. We call ρ a *(permutation) representation* of G on Ω, call the size of Ω the *degree* of the G-action, and call the kernel of the representation ρ the *kernel* of the action. In the case when $\mathsf{Ker}\,\rho = 1$ the action of G is said to be *faithful*.

Provided an action of G on Ω, an element α of Ω is mapped to different elements by various elements of G. The set of all these elements are called the *orbit* of α under G, denoted by $\alpha^G := \{\alpha^x | x \in G\}$. If G only has one orbit on Ω then G is *transitive* on Ω; otherwise it is said to be *intransitive*. Let $\alpha \in \Omega$. The *stabiliser* in G of the element α is the set of all the elements of G that fix α under the action, denoted by

$$G_\alpha := \{g \in G | \alpha^g = \alpha\}.$$

The action of G is said to be *semiregular* if $G_\alpha = 1$ for all $\alpha \in \Omega$. In other words, if G is semiregular on Ω, then any non-identity element of G moves at least one element of Ω.

A notable connection between orbits and point stabilisers is as follows:

Theorem 2.2.2 (The Orbit-Stabiliser Property)**.** ([13, Theorem 1.4 (iii)]) *Let* G *be a group acting on* Ω. *Then*

$$|\alpha^G||G_\alpha| = |G|$$

for all $\alpha \in \Omega$.

In the above theorem, if G is both transitive and semiregular, that is,

$$\alpha^G = \Omega, \quad G_\alpha = 1$$

for some $\alpha \in \Omega$, then we say G is a *regular* group on Ω.

Lemma 2.2.3. *Let* G *be an abelian group acting transitively on a set* Ω. *Then* G *is regular on* Ω.

Proof. Let $\alpha \in \Omega$, and let $g \in G_\alpha$ such that $\alpha^g = \alpha$. Since G is abelian, for any $h \in G$ we have

$$\alpha^h = (\alpha^g)^h = (\alpha^h)^g.$$

Moreover, G is transitive, so g stabilises all the elements of Ω, and $g = 1$. This yields that $G_\alpha = 1$, and the result follows from Theorem 2.2.2. □

The theorem below collects the basic facts on transitive groups.

Theorem 2.2.4. [13, Corollary 1.4A, Exercises 1.4.1] *Let G be transitive on Ω. The the following hold:*

(i) *The point stabilisers in G form a single conjugacy class of subgroups of G. In particular, $G_{\alpha^g} = g^{-1}G_\alpha g$ for all $\alpha \in \Omega, g \in G$.*

(ii) *G is regular on Ω if and only if $|G| = |\Omega|$.*

(iii) *For each $\alpha \in \Omega, H \leq G$, the following are equivalent:*

  (a) *$G = G_\alpha H$;*

  (b) *$G = HG_\alpha$;*

  (c) *H is transitive on Ω.*

  In particular, the only transitive subgroup of G that contains G_α is G itself.

Permutation groups enjoy very broad application. We illustrate some classical examples below.

Example 2.2.5. Let G be a group and let $H \leq G$. Define the *normaliser* of H in G by

$$\mathbf{N}_G(H) := \{g \in G | g^{-1}hg \in H \text{ for all } h \in H\}$$

and define the *centraliser* of H in G by

$$\mathbf{C}_G(H) := \{g \in G | gh = hg \text{ for all } h \in H\}.$$

For each $g \in \mathbf{N}_G(H)$, it is clear that the function (called *conjugation*) $\tau(g) : h \mapsto g^{-1}hg$ is an automorphism of H. And it is easy to check that the representation $\tau : \mathbf{N}_G(H) \to \mathsf{Aut}(H)$ has the kernel $\mathbf{C}_G(H)$, thus

$$\mathbf{N}_G(H)/\mathbf{C}_G(H) \lesssim \mathsf{Aut}(H).$$

Example 2.2.6. Let G be a group and let $H \leq G$ be a subgroup of index n. Let $\Omega := [G : H]$. Define a function ρ by $\rho(g) : Hx \mapsto Hxg$ for all $g \in G$. Then $\rho : G \to \mathrm{Sym}(\Omega)$ is a transitive permutation representation of G on Ω with the kernel

$$\mathsf{Core}_G(H) := \bigcap_{g \in G} g^{-1}Hg.$$

In the above example, the function ρ is usually called *right multiplication*, and similarly a *left multiplication* can be defined. The group $\mathsf{Core}_G(H)$ is called the *core* of H in G, which is the maximal normal subgroup of G that is contained in H. In the case the core is trivial, that is, $\mathsf{Core}_G(H) = 1$, we say that H is a *core-free* subgroup of G. From the viewpoint of the action it is easy to show that

$$G/\mathsf{Core}_G(H) \lesssim \mathrm{S}_n.$$

Let Δ, Σ be finite non-empty sets. Let H, K be groups acting on Δ and Σ respectively. The groups H and K are said to be *permutation isomorphic* if there is a bijection $\lambda : \Delta \to \Sigma$ and a group isomorphism $\rho : H \to K$ such that

$$\lambda(\alpha^h) = \lambda(\alpha)^{\rho(h)} \quad \text{for all } \alpha \in \Omega \text{ and all } h \in H.$$

Recall Theorem 2.2.4 (ii) that a transitive group G is regular on a set Ω if and only if the group and the set have equal size. Furthermore, we can fix an element $\alpha \in \Omega$ and label the element α^g as g for all $g \in G$. Such way of labelling is feasible due to the fact that G is semiregular; and all elements of Ω are labelled as G is transitive. By this labelling one can easily find that the G-action on Ω is permutation isomorphic to the right multiplication on G itself, and hence regular actions can be sometimes viewed as permutations of group elements.

Let G be a group acting on Ω. For each $k \geq 1$, let $\Omega^{(k)}$ be the set of all the k-tuples $(\alpha_1, \ldots, \alpha_k)$ where $\alpha_i \in \Omega$ and all α_i are distinct. Then G has a natural action on $\Omega^{(k)}$ by defining

$$(\alpha_1, \ldots, \alpha_k)^g := (\alpha_1^g, \ldots, \alpha_k^g).$$

If G is transitive on $\Omega^{(k)}$, then we say G is *k-transitive* on Ω. Dual to this concept, we also say that G is *half-transitive* on Ω if all the G-orbits in Ω have equal size. Moreover, if G is transitive on Ω, we call the orbits of G on $\Omega^{(2)}$ the *orbitals* of G on Ω. It is clear that the set $\Delta_0 := \{(\alpha, \alpha) | \alpha \in \Omega\}$ is a G-orbital, which is called the *trivial* or *diagonal* orbital. For each G-orbital Δ there is also an orbital $\Delta^* := \{(\beta, \alpha) | (\alpha, \beta) \in \Delta\}$. The orbitals Δ with $\Delta = \Delta^*$ are called *self-paired*; the diagonal orbital is an example of a self-paired orbital.

The following is known to be Burnside's theorem, which will be frequently used in the latter chapters.

Theorem 2.2.7. [13, Theorem 3.5B] *Let G be a transitive subgroup of S_p where p is a prime. Then G is either 2-transitive or $G \leq \mathrm{AGL}(1, p)$.*

2.3 Blocks and Primitivity

Given a group action G on a set Ω. We can actually consider the group action on each G-orbit independently. Thus, the transitive groups are of our major interest. In particular, the concept of blocks is very helpful in understanding a transitive group action. In this section we let G be a group acting transitively on Ω.

Let Δ be a subset of Ω. We define the *orbit* of Δ under G to be

$$\Delta^G := \{\alpha^g | \alpha \in \Delta, g \in G\}.$$

A non-empty subset B of Ω is called a *block* for G if for each $g \in G$ either $B^g = B$ or $B^g \cap B = \emptyset$. Take a block B from Ω and set $\mathcal{B} := \{B^g | g \in G\}$. Then it is not hard to see that the set $\mathcal{B}$ is invariant under the action of G, and it forms a partition of Ω where each element of $\mathcal{B}$ has the same size. We will call $\mathcal{B}$ the *block system*

containing B under the action of G. There are certainly *trivial blocks* such as the singletons $\{\alpha\}$ ($\alpha \in \Omega$) and Ω the set itself. We shall call all other blocks rather than these *nontrivial*. Unless specified, by a block we always mean a nontrivial block hereinafter.

Indeed, the notation for a point stabiliser can be extended as follows: let Δ be a non-empty subset of Ω (not necessarily a block for G). Then the *pointwise stabiliser* of Δ in G is denoted by

$$G_{(\Delta)} := \{g \in G | \alpha^g = \alpha \text{ for all } \alpha \in \Delta\}$$

and the *setwise stabiliser* of Δ in G is denoted by

$$G_{\Delta} := \{g \in G | \Delta^g = \Delta\}.$$

It is straightforward to check that both $G_{(B)}$ and G_B are groups and $G_{(B)} \trianglelefteq G_B$.

Let us fix a block system $\mathcal{B}$ of Ω. Define the group homomorphism $\rho : G \to \mathrm{Sym}(\mathcal{B})$ by

$$\rho(g) : B \mapsto B^g.$$

It is obvious that the kernel of ρ is $G_{(\mathcal{B})}$. We denote the the image of ρ by $G^{\mathcal{B}}$ and call it the *induced action* of G on $\mathcal{B}$. Then $G^{\mathcal{B}} \cong G/G_{(\mathcal{B})}$.

The group G is said to be *primitive* if there is no blocks in Ω; otherwise we say G is *imprimitive*. The following provides a nice property for normal subgroups of G.

Theorem 2.3.1. ([13, Theorem 1.6A]) *Let G be a group acting transitively on a set Ω. Let N be a normal subgroup of G. Then*

(i) *the orbits of N form a block system for G;*

(ii) *if B_1 and B_2 are two N-orbits then N^{B_1} and N^{B_2} are permutation isomorphic;*

(iii) *if G is primitive on Ω then either N is transitive or N lies in the kernel of the action.*

In fact, in Theorem 2.3.1, since G is transitive, for any two N-orbits B_1, B_2, there exists a $g \in G$ such that $B_1^g = B_2$, hence $|B_1| = |B_2|$ and N is half-transitive on Ω. Moreover, due to this special property of N, we use the notation Ω_N to denote the block system of Ω obtained by collecting all the N-orbits, and call Ω_N the *normal partition* of Ω by N.

In analysis of primitive groups, the normaliser and the centraliser are considered quite frequently. The following are some of their basic properties.

Theorem 2.3.2. [13, Theorem 4.2A] *Let α be an element in Ω. Let G be a transitive subgroup of* $\mathrm{Sym}(\Omega)$*, and let C be the centraliser of G in* $\mathrm{Sym}(\Omega)$*. Then:*

(i) *C is semiregular, and $C \cong \mathbf{N}_G(G_\alpha)/G_\alpha$;*

(ii) *C is transitive if and only if G is regular;*

(iii) *if C is transitive, then it is conjugate to G in* $\mathrm{Sym}(\Omega)$ *and hence C is regular;*

(iv) *$C = 1$ if and only if G_α is self-normalising in G (that is, $\mathbf{N}_G(G_\alpha) = G_\alpha$);*

(v) *if G is abelian, then $C = G$;*

(vi) *if G is primitive and non-abelian, then $C = 1$.*

A nontrivial normal subgroup M of a group G is called *minimal* if it does not properly contain any other subgroup which is normal in G. The *socle* of G is the group generated by all the minimal normal subgroups of G, denoted by $\mathsf{soc}(G)$. It is evident that $\mathsf{soc}(G)$ is normal in G, moreover, $\mathsf{soc}(G)$ is characteristic in G as the set of all the minimal normal subgroups is fixed by any automorphism of G. The minimal normal subgroups as well as the socles play a critical role in characterising primitive permutation groups. The following are some fundamental properties:

Theorem 2.3.3. [13, Theorem 4.3A] *Let G be a group. Let M be a minimal normal subgroup of G and let N be a normal subgroup of G.*

(i) *Either $M \trianglelefteq N$ or $\langle M, N\rangle = M \times N$.*

(ii) *There exist minimal normal subgroups $M_1, \ldots, M_r$ such that*

$$\mathsf{soc}(G) = M_1 \times \ldots \times M_r.$$

(iii) *The group $M = T_1 \times \ldots \times T_s$ where T_i are simple and mutually conjugate under G.*

(iv) *If the subgroup M_i in* (ii) *are all non-abelian, then $M_1, \ldots, M_r$ are the only minimal normal subgroups of G. Similarly, if the T_i in* (iii) *are all non-abelian, then they are the only minimal normal subgroup of M.*

A *quasiprimitive* group is a permutation group all of whose nontrivial normal subgroups are transitive. It is obvious that primitive groups are quasiprimitive by Theorem 2.3.1, however the converse is not necessarily true. The following result was originally presented for the primitive case, but indeed also applies to quasiprimitive groups.

Theorem 2.3.4. [13, Theorem 4.3B] *Let G be a group acting quasiprimitively on Ω, and let M be a minimal normal subgroup of G. Then exactly one of the following holds:*

(i) *M is a regular elementary abelian group of order p^d for some prime p and some integer d, and $\mathsf{soc}(G) = M = \mathbf{C}_G(M)$;*

(ii) *M is regular and non-abelian, $\mathbf{C}_G(M)$ is a minimal normal subgroup of G which is permutation isomorphic to M, and $\mathsf{soc}(G) = M \times \mathbf{C}_G(M)$;*

(iii) *M is non-abelian, $\mathbf{C}_G(M) = 1$ and $\mathsf{soc}(G) = M$.*

A consequence of this theorem is the following.

Corollary 2.3.5. [13, Corollary 4.3B] *Let G be a primitive group. Then $\mathsf{soc}(G)$ is a direct product of isomorphic simple groups. Let N denote the normaliser of $\mathsf{soc}(G)$ in the symmetric group. Then $\mathsf{soc}(G)$ is a minimal normal subgroup of N. Moreover, if $\mathsf{soc}(G)$ is not regular, then it is the only minimal normal subgroup of N.*

For 2-transitivity we have:

Theorem 2.3.6. [13, Theorem 4.1B] *A 2-transitive group has a unique minimal normal subgroup M. Moreover, M is either a regular elementary abelian p-group for some prime p, or a nonregular non-abelian simple group.*

The following O'Nan-Scott Theorem is well known.

Theorem 2.3.7. [13, Theorem 4.1A] *Let G be a primitive group of degree n. Then*

(i) *$\mathsf{soc}(G)$ is a regular elementary abelian p-group for some prime p, and G is isomorphic to a subgroup of the affine group $\mathrm{AGL}(m, p)$; or*

(ii) *$\mathsf{soc}(G)$ is isomorphic to a direct product T^m where T is a non-abelian simple group, and one of the following holds:*

  (a) *$m = 1$ and G is isomorphic to a subgroup of $\mathsf{Aut}(T)$;*

  (b) *$m \geq 2$ and G is a group of "diagonal type" with $n = |T|^{m-1}$;*

  (c) *$m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to T^d. And G is isomorphic to a subgroup of the wreath product $U \wr \mathrm{S}_{m/d}$ with the "product action", and $n = \ell^{m/d}$ where ℓ is the degree of U;*

  (d) *$m \geq 6$ and $\mathsf{soc}(G)$ is regular, $n = |T|^m$.*

2.4 Soluble Groups

Given a group G, if $G^{(k)} = 1$ for some $k \in \mathbb{N}$, then G is *soluble*; and if $G^{(k)} \neq 1$ for all $k \in \mathbb{N}$, then G is *insoluble*. Soluble groups have nice properties between its related groups.

Lemma 2.4.1. [3, Proposition 11.3] *Let G be a group. Let H be a subgroup of G and let N be a normal subgroup of G.*

(i) *If G is soluble, then H is also soluble;*

(ii) *if G is soluble, then G/N is also soluble;*

(iii) *if both $N, G/N$ are soluble, then G is also soluble;*

(iv) *if both G, H are soluble, then $G \times H$ is also soluble.*

We are in a good position to define a *composition series* of a group G, that is a series of subgroups:

$$1 = G_0 < G_1 < \ldots < G_n = G$$

where $G_i \lhd G_{i+1}$ and G_{i+1}/G_i (called a *composition factor*) is simple for all i. Thus, by Lemma 2.4.1 a soluble group can be interpreted as a group all of whose composition factors have prime orders ([3, Proposition 11.4]).

The notion of permutation groups is also used to prove Sylow's Theorem. Let G be a group and let p be a prime divisor of $|G|$. The group G is a *p-group* if $|G|$ is a power of p, and $H \leq G$ is a *p-subgroup* of G if $|H|$ is a power of p. Given a number n, the *p-part* of n is denoted by n_p, which is the highest p-power that divides n. For those subgroups whose order is exactly $|G|_p$, we call them *Sylow p-subgroups* of G.

Theorem 2.4.2. ([3, Sylow's Theorem]) *Let G be a group and let p be a prime divisor of $|G|$. Then*

(i) *G has at least one Sylow p-subgroup.*

(ii) *All Sylow p-subgroups of G are conjugate.*

(iii) *Any p-subgroup of G is contained in a Sylow p-subgroup of G.*

(iv) *The number of Sylow p-subgroups of G is congruent to 1 modulo p.*

Sometimes Sylow subgroups do the trick for permutation groups. The following is an example:

Lemma 2.4.3. *Let $p, m, k \in \mathbb{N}$ with p being a prime. Let G be a transitive permutation group on a set Ω with $|\Omega| = p^k m$. Then each Sylow p-subgroup of G has the orbit of size at least p^k. In particular, if $m = 1$, then any Sylow p-subgroup of G is transitive on Ω.*

Proof. Let P be a Sylow p-subgroup of G and let $\alpha \in \Omega$. By Theorem 2.2.2,

$$|\Omega||G_\alpha| = |G|. \tag{2.1}$$

Taking the p-part of (2.1) we have

$$p^k \cdot |G_\alpha|_p = |G|_p = |P|. \tag{2.2}$$

In the meantime, the application of Theorem 2.2.2 on P gives

$$|\alpha^P||P_\alpha| = |P|. \tag{2.3}$$

Note that $G_\alpha \geq P_\alpha$, hence the result follows by a comparison between (2.2) and (2.3). □

An extension to the concepts of p-groups and Sylow p-subgroups is π-groups and Hall π-subgroups. (Note that there is also a concept of *Sylow π-subgroup*, but we do not need this concept in this thesis.) Let π be a non-empty set of primes. A *π-number* is a positive integer such that all its prime divisors belong to π. Let G be a group. The *π-elements* of G are the elements whose order is a π-number. Let H be a subgroup of G. If all the elements in H is a π-element, then H is called a *π-subgroup* of G. In contrast, we denote π' the set of all the primes that do not belong to π. Hence we have the concepts of *π'-numbers*, *π'-elements* and *π'-groups*. Moreover, if the subgroup H has the property that $|G : H|$ is a π'-number, then H is a *Hall π-subgroup* of G, and vice versa.

The normal π-subgroups of a group G play a special role. A *π-core* of G is the group

$$\mathbf{O}_\pi(G) := \langle H | H \text{ is a normal } \pi\text{-subgroup of } G \rangle.$$

It is clear that $\mathbf{O}_\pi(G)$ is the maximal normal π-subgroup of G, and hence $\mathbf{O}_\pi(G)$ is characteristic. Moreover, $\mathbf{O}_\pi\left(G/\mathbf{O}_\pi(G)\right) = 1$. For this reason, we usually consider the *upper $\pi\pi'$-series*, that is a series of G obtained by repeatedly applying $\mathbf{O}_\pi$ and $\mathbf{O}_{\pi'}$:

$$1 = P_0 \lhd N_0 \lhd P_1 \lhd N_1 \lhd \ldots \lhd P_m \lhd N_m = G$$

where $N_i/P_i = \mathbf{O}_\pi(G/P_i)$ and $P_{i+1}/N_i = \mathbf{O}_{\pi'}(G/N_i)$ for all i. It is sometimes convenient to denote the first few terms $N_0, P_0, N_1, \ldots$ by

$$\mathbf{O}_\pi(G), \mathbf{O}_{\pi\pi'}(G), \mathbf{O}_{\pi\pi'\pi}, \ldots$$

An important property of Hall π-subgroups is the following:

Theorem 2.4.4. ([48, Theorem 9.1.7]) *Let G be a soluble group and let π be a non-empty set of primes. Then every π-subgroup is contained in a Hall π-subgroup of G. Moreover, all π-subgroups are conjugate.*

2.5 Products of Groups

In this section we let H, K be groups.

Recall that the *direct product* of H and K is the set $G := \{(h, k) | h \in H, k \in K\}$ together with the operation

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1 h_2, k_1 k_2).$$

Let $Z \leq \mathbf{Z}(H)$ be maximal in the sense that there exists an isomorphism ϕ such that $\phi(Z) \leq \mathbf{Z}(K)$. Let $\mathbf{Z}(H, K) := \{(h, \phi(h)) | h \in Z\}$. The *central product* of H and K is the group

$$G := (H \times K)/\mathbf{Z}(H, K),$$

which is usually denoted by $H \circ K$.

A slight generalisation of the direct product is the semidirect product. Suppose K acts on H in the way that for each $k \in K$ the map $\bar{k} : h \mapsto h^k$ is an automorphism of H. Set $G := \{(h, k)|h \in H, k \in K\}$ and define the product on G by

$$(h_1, k_1) \cdot (h_2, k_2) := (h_1 h_2^{k_1^{-1}}, k_1 k_2).$$

It is easy to verify that G forms a group under the product operation, and we shall call G the *semidirect product* of H by K, written by $H{:}K$. Observe that $H \lhd G$ and $H \cap K = 1$. Indeed, given any groups H, K satisfying these conditions we can always construct the semidirect product of H by K. For the case that $K = \mathsf{Aut}(H)$, the group

$$H{:}K = H{:}\mathsf{Aut}(H)$$

is called the *holomorph* of H and denoted by $\mathsf{Hol}(H)$. Another often-seen example of the semidirect product could be the *dihedral groups* $\mathrm{D}_{2n} = \mathbb{Z}_n{:}\mathbb{Z}_2$.

The normaliser of a regular group G in the symmetric group equals the holomorph of G.

Lemma 2.5.1. [13, Exercises 2.5.5 and 2.5.6] *Let Ω be a finite set. Let $X = \mathrm{Sym}(\Omega)$ and let $G < X$ be regular on Ω. Then*

$$\mathbf{N}_X(G) = G{:}\mathsf{Aut}(G) = \mathsf{Hol}(G).$$

The wreath product plays an important role in characterising imprimitive permutation groups. Let $H^n := \{(h_1, \ldots, h_n)|h_i \in H\}$ be the Cartesian product of n copies of H, and let $K \leq \mathrm{S}_n$ act on H^n by permuting the n subscripts. That is $\rho : K \to \mathsf{Aut}(H^n)$, which is defined by

$$\rho(k^{-1}) : (h_1, \ldots, h_n) \mapsto (h_{1^k}, \ldots, h_{n^k}).$$

Then the *wreath product* of H by K is the semidirect product $H^n{:}K$, which is usually denoted by $H \wr K$.The group H^n is called the *base group* of the wreath product.

A *complement* to a normal subgroup N of a group G is a subgroup H of G such that $G = N{:}H$.

Theorem 2.5.2. ([3, Schur-Zassenhaus Theorem]) *Any normal Hall subgroup of a group has a complement.*

2.6 Linear Groups

By associating a permutation group with vector spaces, linear groups provide a gateway to view permutation groups geometrically. Moreover, linear groups have a strong connection with group representation theory, which we will discuss in the next section. In this section we will review the basic properties of various types of linear groups.

Notation. Throughout this section we let $\mathbb{F}_q$ denote the field of order q where $q = p^\ell$ for some prime p and some integer ℓ. Let $n \in \mathbb{N}$ and let V be a vector space

of dimension n over $\mathbb{F}_q$. The zero vector of V is written by $\mathbf{0}_V$, or $\mathbf{0}$ if there is no confusion. The set of all the nonzero elements in $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^*$, and similarly the set of all the nonzero vectors in V is denoted by $V^\#$.

We will assume readers are familiar with the definitions of linear groups such as the general linear groups, the special linear groups, the affine linear groups etc. For the sake of clarity, we take an example: the *general linear group* is the group consisting of all the invertible linear transformations of V, which we denote by $\mathrm{GL}(n,q)$, or $\mathrm{GL}(n,V)$ if we want to specify the vector space V.

Lemma 2.6.1. *Let $\rho : A \mapsto \det A$ be a group homomorphism from $\mathrm{GL}(n,q)$ onto the multiplicative group $\mathbb{F}_q^*$. Then $\mathsf{Ker}\,\rho = \mathrm{SL}(n,q)$ and*

$$\mathrm{SL}(n,q) \lhd \mathrm{GL}(n,q).$$

Moreover, the quotient group $\mathrm{GL}(n,q)/\mathrm{SL}(n,q)$ is isomorphic to $\mathbb{Z}_{q-1}$, the multiplicative group of the ground field.

Note that each element of $\mathrm{GL}(n,V)$ can be regarded as an $n \times n$ matrix. Thus, the group action of $\mathrm{GL}(n,V)$ on V is given by $v^g := vg$ for each $g \in \mathrm{GL}(n,V), v \in V$. For simplicity, if there is no confusion, the centre of $\mathrm{GL}(n,q)$ is denoted by $\mathbf{Z} := \mathbf{Z}(\mathrm{GL}(n,q))$. It is readily seen that

$$\mathbf{Z} = \{\lambda I | \lambda \in \mathbb{F}_q^*\} \cong \mathbb{Z}_{q-1},$$

and the elements of $\mathbf{Z}$ are the only elements that fix all the 1-dimensional subspaces of V.

The maximum order of a p-element in $\mathrm{GL}(d,p)$ is constrained by d.

Lemma 2.6.2. *If $d \geq 2$, then the largest order p^e of p-elements of $\mathrm{GL}(d,p)$ satisfies $p^e \geq d > p^{e-1}$.*

Proof. Let U be the set of the elements of $\mathrm{GL}(d,p)$ with the following form

$$\begin{pmatrix} 1 & a_{12} & a_{13} & \cdots & a_{1d} \\ 0 & 1 & a_{23} & & a_{2d} \\ \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & a_{d-1,d} \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then U forms a Sylow p-subgroup of $\mathrm{GL}(d,p)$. Let $u \in U$ be such that $o(u) = p^e$ is the largest order of elements of U, where e is an integer. Let $u = A + I$. Notice that for any $u \in U$, we have $u^{p^e} = I$ if and only if $(A+I)^{p^e} = I$, if and only if (using the binomial theorem) $A^{p^e} = 0$. By careful choice of u, we can ensure that $A^b \neq 0$ for $b < d$, so that $A^{p^e} = 0$ implies $p^e \geq d$ and $p^{e-1} < d$. □

Let $\mathrm{SL}(n,q)$ be acting on the set Ω of 1-dimensional subspaces of V, so that the kernel of this action is $\mathrm{SL}(n,q) \cap \mathbf{Z}$. Then we obtain the action of $\mathrm{PSL}(n,q)$ on Ω. A similar description may also define the action of $\mathrm{PGL}(n,q)$ on Ω. It can be shown [53] that $\mathrm{PSL}(2,2) \cong \mathrm{S}_3$ and $\mathrm{PSL}(2,3) \cong \mathrm{A}_4$, which are both soluble. In fact, when $n \geq 2$, these are the only exceptional cases that $\mathrm{PSL}(n,q)$ is soluble.

Theorem 2.6.3. [53] *If $n \geq 2$, then $\mathrm{PSL}(n,q)$ is simple, except when $n = 2$ and $q = 2$ or 3.*

Recall that $\mathrm{AGL}(n,q)$ is the full automorphism group of the vector space V. Moreover, $\mathrm{GL}(n,q)$ and $\mathrm{AGL}(n,q)$ have an interesting relation.

Lemma 2.6.4. *For each $n \in \mathbb{N}$, we have $\mathrm{AGL}(n,q) \lesssim \mathrm{GL}(n+1,q)$.*

Proof. Let

$$G := \left\{ \begin{pmatrix} 1 & 0 \\ \alpha & A \end{pmatrix} \middle| \alpha \text{ is an } n\text{-dimensional column vector, } A \in \mathrm{GL}(n,q) \right\}$$
$$H := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \middle| A \in \mathrm{GL}(n,q) \right\}$$
$$N := \left\{ \begin{pmatrix} 1 & 0 \\ \beta & I \end{pmatrix} \middle| \beta \text{ is an } n\text{-dimensional column vector} \right\}.$$

It is easy to verify that G, N, H are groups, and particularly $G \leq \mathrm{GL}(n+1,q)$, $H \cong \mathrm{GL}(n,q)$, and $N \cong T_V$ the additive group of the n-dimensional vector space V over the field $\mathbb{F}_q$. Notice that

$$\begin{pmatrix} 1 & 0 \\ \alpha & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} 1 & 0 \\ A^{-1}\alpha & I \end{pmatrix},$$

so $G = \langle N, H \rangle$. Moreover, H normalises N and $N \cap H = 1$, we have

$$G = N{:}H \cong T_V{:}\mathrm{GL}(n,q) \cong \mathrm{AGL}(n,q).$$

□

A consequence of Lemma 2.6.4 gives us a chain, which we will use later:

$$\mathrm{AGL}(1,q) \lesssim \mathrm{GL}(2,q) \lesssim \mathrm{AGL}(2,q) \lesssim \ldots \lesssim \mathrm{AGL}(n,q) \lesssim \mathrm{GL}(n+1,q).$$

If $n = rs$ for some $r, s \in \mathbb{N}$, then the vector space V can be decomposed as the tensor product of an r-dimensional vector space U and an s-dimensional vector space W. Consequently, this enables us to define an action of $\mathrm{GL}(r, q^s)$ on V, and hence $\mathrm{GL}(r, q^s)$ can be embedded into $\mathrm{GL}(rs, q)$.

Lemma 2.6.5. *Let $r, s \in \mathbb{N}$. Then $\mathrm{GL}(r, q^s)$ is isomorphic to a subgroup of $\mathrm{GL}(rs, q)$. Moreover, $\mathrm{GL}(r, q^s)$ acts transitively on the set of basis vectors of the vector space $\mathbb{F}_{q^s}^r$, and particularly, it is transitive on the set of 1-dimensional subspaces of the vector space $\mathbb{F}_q^{rs}$.*

In regards to Lemma 2.6.5, the group $\mathrm{GL}(1, q^n) \cong \mathbb{Z}_{q^n-1}$ can be viewed as a subgroup of $\mathrm{GL}(n, q)$, which is transitive on $V^{\#}$, all the nonzero vectors of the vector space V. The group $\mathrm{GL}(1, q^n)$ is usually referred as a *Singer subgroup* of $\mathrm{GL}(n, q)$; and the generators of this group and their conjugates are the so-called *Singer cycles*.

2.7 Groups and Representations

The machinery of group representation theory can be used to extract key information of a given group. In this section we present a short introduction.

Let $n \in \mathbb{N}$ and let V be a vector space of dimension n over a field $\mathbb{F}$. Let G be a group.

A homomorphism

$$\rho : G \to \mathrm{GL}(n, \mathbb{F})$$

is called a *representation* of G over $\mathbb{F}$ of *degree* n. Since ρ is a homomorphism, we have

$$\rho(gh) = \rho(g)\rho(h) \quad \text{for all } g, h \in G.$$

The *kernel* of the representation (homomorphism)

$$\mathsf{Ker}\,\rho = \{g \in G | \rho(g) = I\}$$

is a normal subgroup of G. In the case that $\mathsf{Ker}\,\rho = 1$ we say the representation ρ is *faithful*; otherwise we say it is not faithful.

The representation ρ of G naturally induces a G-action on the vector space V. More precisely, for each $v \in V$, we have

$$vg := v\rho(g).$$

This defines a multiplication between the elements of V and the elements of G. Let us view V as an additive group T_V, then this additive group together with the group G form a group, the extension of T_V by G, denoted by $X = T_V.G$. Since $\rho(G)$ is a subgroup of $\mathrm{GL}(n, \mathbb{F})$, we have X is a subgroup of $\mathrm{AGL}(n, \mathbb{F})$.

Let us define the *group algebra* $\mathbb{F}G := \left\{ \sum_{g \in G} \alpha_g g | \alpha_g \in \mathbb{F} \right\}$. It is straightforward to check that for all $u, v \in V$ and $g, h \in G$ the following are satisfied:

(1) $vg \in V$,

(2) $v(gh) = (vg)h$,

(3) $(\lambda v)g = \lambda(vg) = v(\lambda g)$,

(4) $v1 = v$,

(5) $(u + v)g = ug + vg$,

(6) $\mathbf{0}g = \mathbf{0}$.

Then the vector space V is an $\mathbb{F}G$-*module*. And a subspace W of V is an $\mathbb{F}G$-*submodule* if it is invariant under the action of G, that is, for all $w \in W$ and $g \in G$ we have

$$wg \in W.$$

Correspondingly, the *trivial* submodules of V are $\{0\}$ and V. The *simple* (or *irreducible*) modules are the modules that does not contain any nontrivial submodules. If V is an irreducible $\mathbb{F}G$-module with respect to the representation ρ, then we say ρ is an *irreducible* representation of G; otherwise we say ρ *reducible*. In regards to permutation group concepts, if V is an $\mathbb{F}G$-module, then the group $X = T_V.G$ is transitive on V; and moreover, if V is an irreducible $\mathbb{F}G$-module, then the group X is primitive on V, and we simply say G is irreducible on V.

Let $\rho : G \to \mathrm{GL}(1, \mathbb{F}) \cong \mathbb{F}^*$ be a representation of G. Then we say ρ is a *linear* representation of G. It is immediate that ρ is irreducible; and if ρ is faithful then G is cyclic.

In group representation theory, one of the very important results was obtained in 1898 by Heinrich Maschke [3], the most junior of the three initial mathematics faculty of the University of Chicago.

Theorem 2.7.1. [3, Maschke's Theorem] *Let G be a group and let $\mathbb{F}_q$ be a field such that $(|G|, q) = 1$. Let V be an $\mathbb{F}_qG$-module. If V has an $\mathbb{F}_qG$-submodule W, then there exists an $\mathbb{F}_qG$-submodule U of V such that $V = U \oplus W$.*

An $\mathbb{F}G$-module is said to be *semisimple* (or *completely reducible*) if it is a direct sum of simple modules. A simple implication by Maschke's Theorem is the following:

Corollary 2.7.2. *Let G be a group and let $\mathbb{F}_q$ be a field such that $(|G|, q) = 1$. Then every nontrivial $\mathbb{F}_qG$-module is semisimple.*

Part II – Graphs

2.8 Concepts of Graphs

Let V be a vertex set, that is, a collection of *vertices*. A *graph* $\Gamma = (V, E)$ can be obtained by associating the vertex set V with a set E of *edges* that connect some (possibly none or all) pairs of distinct vertices. Let $u, v \in V$ be distinct vertices of the graph Γ. If the pair (u, v) as well as the pair (v, u) are elements of the edge set E, then Γ has an *undirected edge* between u and v, and this edge is denoted by the unordered pair $\{u, v\}$. If all the edges of Γ are undirected, then Γ is said to be an *undirected graph*. The size of V is denoted by $|V|$, called the *order* of Γ. In the case that $|V|$ is a finite number, Γ is said to be a *finite graph*.

The undirected graphs are sometimes also referred to be *simple graphs*. In contrast, there are *digraphs*, or *directed graphs*, each of which consists of a vertex set V and an arc set A, where an *arc* (or a *directed edge*) is an ordered pair of distinct vertices. Throughout this dissertation, unless otherwise mentioned, all graphs are assumed to be both undirected and finite.

Given an edge $\{u, v\}$ in a graph Γ, we sometimes write $u \sim v$, and say u and v are *adjacent*, and v is a *neighbour* of u and vice versa. If every vertex in Γ is adjacent to all the other vertices in Γ, then Γ is a *complete* graph, and it is denoted by $\mathbf{K}_n$ if the order of Γ is n. For each vertex v in the graph Γ, the set of all its neighbours are denoted by $N(v)$ or $N_\Gamma(v)$ if we need to specify the graph; and the size of $N(v)$ is said to be the *valency* of v in Γ. If all the vertices of Γ have valency 0, then Γ is said to be an *empty* graph. A graph in which every vertex has valency k is said to be *regular* of valency k or *k-regular*.

Let $\Gamma = (V, E)$ be a graph. A graph $\Gamma' = (V', E')$ is a *subgraph* of Γ if

$$V' \subseteq V, \quad \text{and } E' \subseteq E,$$

and the subgraph Γ' is *induced* if

$$E' = (V' \times V') \cap E.$$

The *complement* $\overline{\Gamma}$ of Γ is a graph with the same vertex set V as Γ such that any pair of distinct vertices are adjacent in $\overline{\Gamma}$ if and only if they are not adjacent in Γ.

Let $v_0, \ldots, v_r$ be mutually distinct vertices of a graph Γ. A *path* of length r in Γ is a sequence

$$v_0 \sim v_1 \sim \ldots \sim v_r;$$

and if v_r is also adjacent to v_0, then Γ contains a *cycle* $\mathbf{C}_{r+1}$ with the vertices $v_0, \ldots, v_r$. The graph Γ is said to be *connected* if any two of its vertices are connected by a path, otherwise Γ is said to be *disconnected*.

A graph Γ is called *bipartite* if its vertex set can be partitioned into two disjoint subsets V_1 and V_2 such that every edge in Γ has one end in V_1 and the other end

in V_2. A variation of the complete graph is the *complete bipartite graph* $\Gamma = (V, E)$, where there exist disjoint subsets V_1, V_2 such that

$$V = V_1 \cup V_2 \quad \text{and} \quad E = (V_1 \times V_2) \cup (V_2 \times V_1);$$

in the case that $|V_1| = m, |V_2| = n$ this graph is denoted by $\mathbf{K}_{m,n}$. It is obvious that the complement of $\mathbf{K}_{m,n}$ is disconnected, and is a union of the complete graphs $\mathbf{K}_m$ and $\mathbf{K}_n$.

Let $\Gamma_1 = (V_1, E_1), \Gamma_2 = (V_2, E_2)$ be graphs. An *isomorphism* φ from Γ_1 to Γ_2 is a bijection from V_1 to V_2 such that $u \sim v$ if and only if $\varphi(u) \sim \varphi(v)$ for any two vertices $u, v \in V_1$. If such a φ exists, then we say Γ_1 is *isomorphic* to Γ_2 and vice versa, denoted by $\Gamma_1 \cong \Gamma_2$ or $\Gamma \overset{\varphi}{\cong} \Gamma_2$ if we want to specify the isomorphism. In the case that $\Gamma_1 = \Gamma_2 = \Gamma$, then φ is actually an *automorphism* of Γ. All the automorphisms of Γ form the *full automorphism group* $\mathsf{Aut}\Gamma$. Any subgroup of $\mathsf{Aut}\Gamma$ is called an *automorphism group* of Γ.

2.9 Vertex-Transitive Graphs

Let $\Gamma = (V, E)$ be a graph. The full automorphism group $\mathsf{Aut}\Gamma$ naturally induces an action on V, and $\mathsf{Aut}\Gamma$ can be viewed as a subgroup of $\mathrm{Sym}(V)$. Thus, from now on, we shall simply say $\mathsf{Aut}\Gamma$ acts on Γ, and so do its subgroups. Moreover, if $\mathsf{Aut}\Gamma$ is transitive on V, then Γ is a *vertex-transitive* graph; in particular, if $\mathsf{Aut}\Gamma$ is primitive on V, then we say Γ is a *vertex-primitive* graph. A vertex-transitive graph Γ has all its vertices being equivalent, and consequently, every vertex of Γ has the same number of neighbours. This follows that vertex-transitive graphs are always regular.

An important family of vertex-transitive graphs is Cayley graphs.

Definition 2.9.1. Let R be a group and let $S \subseteq R^{\#}$ be a *self-inverse* set, that is, the set that is closed under taking inverses. The *Cayley graph*, which is usually denoted by $\mathrm{Cay}(R, S)$, is a graph $\Gamma = (V, E)$ where $V = R$ and two vertices x, y are adjacent if and only if $xy^{-1} \in S$.

The definition of Cayley graphs is proper as we chose the set S to be self-inverse so that $yx^{-1} = (xy^{-1})^{-1}$; and all the Cayley graphs are undirected.

Given a group R and its subset S, we let $\mathsf{Aut}(R, S)$ be the subgroup of $\mathsf{Aut}(R)$ that fixes the set S setwise. The following result is straightforward:

Theorem 2.9.2. [8, Proposition 16.2] *Let R be a group with a subset S such that there is a Cayley graph $\Gamma = \mathrm{Cay}(R, S)$. Let v be the vertex that is represented by the identity of R. Then*

(i) *The graph Γ is vertex-transitive. In particular, R is isomorphic to a subgroup of $\mathsf{Aut}\Gamma$, which acts regularly on the vertex set V.*

(ii) $\mathsf{Aut}(R, S) \lesssim (\mathsf{Aut}\Gamma)_v$.

More importantly, Cayley graphs have special properties among vertex-transitive graphs.

Theorem 2.9.3. [19, Lemma 3.7.1 and 3.7.2] *A graph is a Cayley graph if and only if there is a group acting regularly on its vertex set.*

Lemma 2.9.4. [19, Lemma 3.7.3] *Let $\sigma \in \mathsf{Aut}(R)$. Then σ induces an isomorphism from $\mathrm{Cay}(R, S)$ to $\mathrm{Cay}(R, S^\sigma)$.*

Let $\Gamma = (V, E)$ be a graph such that its full automorphism group $\mathsf{Aut}\Gamma$ admits a cyclic subgroup R acting transitively on V. It follows from Lemma 2.2.3 that R is regular on V, and hence Γ is a Cayley graph on the group R. Such a graph is called a *circulant*. More generally, if $\mathsf{Aut}\Gamma$ contains a metacyclic transitive group, then Γ is said to be a *metacirculant*. However, a metacirculant is not necessarily a Cayley graph; the Petersen graph is the smallest counterexample.

Analogous to vertex-transitivity, we can define a graph Γ to be *edge-transitive* (or *arc-transitive*) if the full automorphism group $\mathsf{Aut}\Gamma$ induces a transitive group on the edge (or arc) set of Γ. It is readily seen that a connected arc-transitive graph is vertex-transitive. Hence, arc-transitive graphs can be viewed as a special class of vertex-transitive graphs.

Let G be a transitive group on a finite set Ω. Recall that an orbital of G on Ω is the set $\Delta := (\alpha, \beta)^G$ for some $\alpha, \beta \in \Omega$. We define the *orbital graph* $\Gamma(\Delta) := (\Omega, \Delta)$. It is evident that $\Gamma(\Delta)$ is a digraph, since (β, α) does not have to be in Δ; moreover, $\Gamma(\Delta)$ is arc-transitive as it is defined. Note that G is transitive, it follows that each element of Ω is adjoined by an arc from $\Gamma(\Delta)$, hence it should be no confusion that we use the notation $(\alpha, \beta)^G$ for $\Gamma(\Delta)$ hereinafter. For convenience, sometimes we also need the concept of an *undirected orbital graph*, that is an undirected graph obtained by forcing all the arcs of an orbital graph to be undirected edges.

There are several ways we can construct a vertex-transitive graph. The following is a group-theoretic approach via the action on cosets.

Definition 2.9.5. Let G be a group. Let H be a subgroup of G, and let $S \subseteq G \setminus H$ be a self-inverse set. The *coset graph* of G with respect to H and S is a graph $\Gamma = (V, E)$ where $V = [G : H]$ the set of all the right cosets of H, and for any $Hx, Hy \in V$, the vertices Hx, Hy are adjacent in Γ if and only if $xy^{-1} \in HSH$. Such a graph is usually denoted by $\mathrm{Cos}(G, H, HSH)$.

By the definition of the coset graph Γ we see that $xy^{-1} \in HSH$ if and only if $yx^{-1} \in HS^{-1}H$. It then follows from the choice of the set S that Γ is undirected. Moreover, the condition $S \subseteq G \setminus H$ guarantees the graph Γ does not contain any loops, so Γ is simple. Also note that the group G acts transitively on the cosets $[G : H]$ by the right multiplication

$$(Hx)^g \mapsto Hxg \quad \text{for all } x \in G,$$

so Γ is vertex-transitive, and by Example 2.2.6, the group H is core-free in G if the G-action is faithful. One may notice that if $H = 1$, then the graph Γ exactly corresponds to the Cayley graph $\mathrm{Cay}(G, S)$. Hence, the coset graph can be

understood to be a generalisation of Cayley graphs. Indeed, according to [49], every vertex-transitive graph can be recognised as a coset graph. Furthermore, if we waive the self-inverse condition on S, we can show [39, Theorems 1 and 2] that Γ is an orbital graph if and only if $HSH = HsH$ for some $s \in S$. This yields that any coset graph $\mathrm{Cos}(G, H, HSH)$ is an edge-disjoint union of certain orbital graphs $\mathrm{Cos}(G, H, Hs_iH)$ where $S' = \{s_1, \ldots, s_m\} \subseteq S$ is minimal such that

$$HS'H = HSH.$$

2.10 Normal Quotients

In characterising a vertex-transitive graph, the method of taking quotient graphs is commonly used. Let $\Gamma = (V, E)$ be a graph with $G \leq \mathsf{Aut}\Gamma$ acting transitively on V. Suppose that G admits a block system $\mathcal{B}$ on V. Then the *quotient graph* $\Gamma_{\mathcal{B}}$ with respect to the G-action is the graph with the vertex set $\mathcal{B}$, and for any $B_1, B_2 \in \mathcal{B}$, they are adjacent if and only if there exist $v_1 \in B_1, v_2 \in B_2$ such that $(v_1, v_2) \in E$. In particular, if N is a normal subgroup of G such that $\mathcal{B} = V_N$, then the quotient graph $\Gamma_{\mathcal{B}}$ is also written as Γ_N.

The benefit of taking quotient graphs of a graph is that many nice properties of the original graph are inherited by the new quotient graph. For instance, the quotient graph of a connected graph is also connected; and the quotient graph of a vertex-transitive graph is again vertex-transitive. In the following we deduce some basic properties of quotient graphs for our further usage.

Note that $G^{\mathcal{B}}$ is the induced permutation group of G on $\mathcal{B}$, and $G^{\mathcal{B}} \cong G/G_{(\mathcal{B})}$. We usually denote $K := G_{(\mathcal{B})}$ so that $G = K.G^{\mathcal{B}}$, where $K \lhd G$. Recall Theorem 2.3.1 states that the orbits of a normal subgroup of a transitive group form a block system. In our case, the group K is even more special such that the corresponding quotient group is a faithful permutation group on the corresponding quotient graph. In the sense of this correspondence we say $\mathcal{B}$ is the *normal quotient* of V with the kernel K. For each $B \in \mathcal{B}$, denote the induced subgraph of Γ on B by $[B]_\Gamma$. Let $B_1, B_2 \in \mathcal{B}$. Theorem 2.3.1 says that K^{B_1} is permutationally isomorphic to K^{B_2}. In fact, by the transitivity of G, one can show that $G_{B_1} \cong G_{B_2}$, and $G_{B_1}^{B_1}$ is permutationally isomorphic to $G_{B_2}^{B_2}$. In particular, all the induced subgraphs $[B]_\Gamma$ are mutually isomorphic and vertex-transitive. We say the block system $\mathcal{B}$ is *minimal* (or *maximal*) if G_B^B (or $G^{\mathcal{B}}$) is primitive on B (or $\mathcal{B}$), where B is a block of $\mathcal{B}$.

Lemma 2.10.1. *Let G be a transitive permutation group on a set Ω. Let N be an intransitive subgroup of G so that $\mathcal{B} = \Omega_N$ is a normal partition. Let Σ be an undirected orbital graph containing an edge $\{\alpha, \beta\}$ where $\alpha \in B$ and $\beta \in B'$ with $B \neq B'$ such that the quotient $\Sigma_{\mathcal{B}}$ is connected. Then each connected component of Σ contains at least one vertex from each block in $\mathcal{B}$.*

Proof. Let C be the vertex set of a connected component of Σ. Label the blocks $\mathcal{B} = \{B_1, B_2, \ldots, B_m\}$ such that $C \cap B_i \neq \emptyset$ for $i = 1, 2, \ldots, k$, where $1 \leq k \leq m$. Suppose that $k < m$. Since $\Gamma_{\mathcal{B}}$ is connected, there exist $\alpha_i \in B_i$ and $\alpha_j \in B_j$, where

$i \leq k$ and $j > k$, such that $\{\alpha_i, \alpha_j\}$ is an edge of Σ. Let $\beta \in C \cap B_i$. Since N is transitive on B_i, there exists $x \in N$ such that $\alpha_i^x = \beta$. Then $\alpha_j^x \in B_j$, and $\{\alpha_i^x, \alpha_j^x\}$ is an edge of Σ, so β is adjacent to the vertex $\alpha_j^x \in B_j$, which is a contradiction. □

It is obvious that K acts on each $[B]_\Gamma$. However, this action is not necessarily faithful, considering $K = K_{(B)}.K^B$. Furthermore, we have the following:

Lemma 2.10.2. *Let $\Gamma = (V, E)$ be a graph with the block system $\mathcal{B} = \{B_1, \ldots, B_t\}$ on V with respect to a transitive subgroup $G \leq \mathsf{Aut}\Gamma$. Let $K := G_{(\mathcal{B})}$. Then*

$$K \leq K^{B_1} \times K^{B_2} \times \ldots \times K^{B_t}.$$

Proof. By the definition of K, it stabilises all the B_i setwise. Thus, for each $g \in K$ we can write $g = g^{B_1} g^{B_2} \ldots g^{B_t}$, where $g^{B_i} \in K^{B_i}$ for all i. Note that for any distinct i, j, the elements g^{B_i} and g^{B_j} are disjoint, in the sense that no vertex in V is permuted by both g^{B_i} and g^{B_j}. Therefore, $g \in K^{B_1} \times \ldots \times K^{B_t}$, and we complete the proof. □

2.11 Self-Complementary Vertex-Transitive Graphs

A graph is said to be *self-complementary* if its complement is isomorphic to the graph itself. In this section, we shall discuss self-complementary vertex-transitive graphs and establish their fundamental properties.

Firstly, any self-complementary graph is connected, followed by the lemma below.

Lemma 2.11.1. *Let $\Gamma = (V, E)$ be a graph. Then either Γ or $\overline{\Gamma}$ is connected.*

Proof. Suppose that Γ is disconnected. Then there exist disjoint subsets V_1, V_2 such that $V = V_1 \cup V_2$, and $v_1 \nsim v_2$ for any $v_1 \in V_1, v_2 \in V_2$. Consider the complement graph $\overline{\Gamma}$. Let $u, v \in V$.

(i) If $u, v \in V_1$, then the path $u \sim w \sim v$ connects them for some $w \in V_2$; similar path also applies to when $u, v \in V_2$.

(ii) If $u \in V_1, v \in V_2$, then the path $u \sim v$ connects them.

This shows that $\overline{\Gamma}$ is connected. □

Observe that any automorphism of a graph Γ preserves the adjacency as well as the non-adjacency, and so it is also an automorphism of $\overline{\Gamma}$. As a result, $\mathsf{Aut}\Gamma = \mathsf{Aut}\overline{\Gamma}$.

Let Γ be a self-complementary graph of order n. Then Γ possesses precisely half number of edges of the complete graph $\mathbf{K}_n$, so $n(n-1)/4$ is an integer, and

$$n \equiv 0 \text{ or } 1 \pmod 4. \tag{2.4}$$

Assume further that Γ is regular. Then a vertex of Γ has equal number of neighbours and non-neighbours, which implies n is an odd number, and

$$n \equiv 1 \pmod 4. \tag{2.5}$$

We know that a vertex-transitive graph is always regular. Hence this gives a necessary condition on the order of self-complementary vertex-transitive graphs. In fact, a necessary and sufficient condition has been obtained by Muzychuck [43].

Theorem 2.11.2. *A self-complementary vertex-transitive graph of order n exists if and only if $n_p \equiv 1 \pmod 4$ for all prime p.*

Let $\Gamma = (V, E)$ be a self-complementary graph. A *complementing isomorphism* of Γ is an isomorphism $\sigma \in \mathrm{Sym}(V)$ that maps Γ to $\overline{\Gamma}$. It is easy to see that σ maps the edges to nonedges, and also maps the nonedges to edges, so σ interchanges Γ and $\overline{\Gamma}$. Thus, any even power of σ is indeed an automorphism of Γ or $\overline{\Gamma}$. Consequently, the order $o(\sigma) = 2^e b$ for some $e \geq 1$ and b an odd number. Let $G := \mathsf{Aut}\Gamma$. Consider the group $X := \langle \mathsf{Aut}\Gamma, \sigma \rangle$. Then $X = G \cup G\sigma$ as $\sigma^2 \in \mathsf{Aut}\Gamma$. In other words, all the complementing isomorphisms of Γ lie in the same coset $G\sigma$ where σ is a coset representative. For simplicity, we always take σ to be of 2-power order hereinafter.

Lemma 2.11.3. *Let σ be a complementing isomorphism of a self-complementary graph Γ. Then σ^2 fixes at most one vertex of Γ. Consequently, $o(\sigma) \neq 2$ and 4 divides $o(\sigma)$.*

Proof. To the contrary, we suppose that σ^2 fixes two vertices u, v. First observe that σ does not fix both u and v, otherwise σ would fix the adjacency relation between u and v, which is not possible. Without loss of generality, let us assume the vertex u is not fixed by σ. However, since σ^2 fixes u, it follows that σ fixes the adjacency relation between u and u^σ, which is again not possible. □

We remark Lemma 2.11.3 that if Γ is a self-complementary digraph, then $o(\sigma) = 2$ is possible for a complementing isomorphism σ of Γ. A simple example is a digraph with two vertices and one arc. Moreover, if Γ is regular, then it follows from (2.5) that Γ has odd number vertices, and by Lemma 2.11.3 we have σ^2 fixes precisely one vertex of Γ. Particularly, any complementing isomorphism of a self-complementary vertex-transitive graph fixes exactly one vertex of the graph.

Let us now restrict Γ to be a self-complementary vertex-transitive graph with a complementing isomorphism σ. Let $G := \mathsf{Aut}\Gamma$ and let $X := \langle G, \sigma \rangle$. Then the group X has been characterised in the primitive and the imprimitive cases. The following two theorems will be frequently quoted in the remainder of the thesis.

Theorem 2.11.4. [22, Theorem 1.3] *Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive digraph with a complementing isomorphism σ. Let $G := \mathsf{Aut}\Gamma$ and let $X := \langle G, \sigma \rangle$. Assume that X is primitive on V. Then one of the following holds:*

(i) *X is an affine group with socle of odd order;*

(ii) *X is almost simple with socle $\mathrm{PSL}(2, q^2)$ with q odd;*

(iii) *X is of product action type with socle* $\mathrm{PSL}(2,q^2)^\ell$*, where q is odd and $\ell \geq 2$.*

Moreover, if Γ is undirected, then X is affine or of product action type.

Theorem 2.11.5. [31, Lemma 4.1] *Let Γ be a self-complementary vertex-transitive graph with a complementing isomorphism σ. Let $G := \mathsf{Aut}\Gamma$ and let $X := \langle G, \sigma \rangle$. Suppose that X is imprimitive on V, and $\mathcal{B}$ is a block system of V under the action of X. Let $B \in \mathcal{B}$. Then*

(i) *the induced subgraph $[B]_\Gamma$ is self-complementary, $G_B^B \leq \mathsf{Aut}[B]_\Gamma$, and σ induces a complementing isomorphism between $[B]_\Gamma$ and $\overline{[B]}_\Gamma$; and*

(ii) *there is a self-complementary graph Σ with the vertex set $\mathcal{B}$ such that $G^{\mathcal{B}} \leq \mathsf{Aut}\Sigma$ and any element in $X^{\mathcal{B}} \setminus G^{\mathcal{B}}$ is a complementing isomorphism of Σ.*

Remark. In Theorem 2.11.5, the quotient graph $\Gamma_{\mathcal{B}}$ may not be self-complementary, see [31, Example 4.3]. Moreover, we notice that G is of index 2 in X, and so either $G^{\mathcal{B}} = X^{\mathcal{B}}$, or $G^{\mathcal{B}}$ is of index 2 in $X^{\mathcal{B}}$. Since σ induces a complementing isomorphism by the theorem, σ does not belong to the kernel $X_{(\mathcal{B})}$, and the following conclusion follows.

Corollary 2.11.6. *The kernel $X_{(\mathcal{B})}$ is contained in G.*

We end this section by a construction method of self-complementary vertex-transitive graphs. Recall from Section 2.9 that the coset graph produces all vertex-transitive graphs. In particular, we can use the coset graph to construct the graphs that are self-complementary.

Lemma 2.11.7. [29, Lemma 2.2] *Let G be a finite group, and let H be a core-free subgroup of G. Then*

(i) *there exists a coset digraph of G with respect to H which is self-complementary if and only if there exists an automorphism $\sigma \in \mathsf{Aut}(G)$ of order a power of 2 such that $H^\sigma = H$, and for each $g \in G \setminus H$ we have $(HgH)^\sigma \neq HgH$;*

(ii) *there exists an undirected coset graph of G with respect to H which is self-complementary if and only if there exists an automorphism $\sigma \in \mathsf{Aut}(G)$ of order a power of 2 such that $H^\sigma = H$, and for each $g \in G \setminus H$ we have $(HgH)^\sigma \notin \{HgH, Hg^{-1}H\}$.*

By Lemma 2.11.7 all the self-complementary vertex-transitive graphs can be constructed via coset graphs, but practically given an arbitrary group G, to find the subgroups H satisfying the conditions in Lemma 2.11.7 is not an easy job. Nonetheless, the coset graphs still have their own special power. For instance, Li and Praeger [29] used the construction of the coset graph to find a class of self-complementary vertex-transitive graphs that are not Cayley graphs.

Note that, as mentioned in Section 2.9, a graph Γ with a vertex-transitive group $G \leq \mathsf{Aut}\Gamma$ can be reconstructed by $\mathrm{Cos}(G, G_v, G_v S G_v)$ for a vertex v in Γ and a self-inverse set $S \subseteq G \setminus G_v$. Moreover, if Γ is self-complementary with a complementing isomorphism σ fixing v, then we can have a larger group $X := \langle G, \sigma \rangle$. Consequently, since the conjugation of σ stabilises G, it can be regarded as an automorphism of G. It is easy to see that G_v is core-free in G, and $G_v^\sigma = G_v$. We could further require $o(\sigma)$ to be a 2-power. This interpretation of Lemma 2.11.7 is sometimes useful for the study of self-complementary vertex-transitive graphs (see Lemma 6.3.2 for example).

Chapter 3

Self-Complementary Graphs and Fixed-Point-Free Automorphisms of Groups

Although the class of self-complementary vertex-transitive graphs has been studied for more than half a century, a bit surprising status is that there are not many examples which are known to be self-complementary vertex-transitive graphs. In fact, except for one family of self-complementary vertex-transitive graphs which are not Cayley graphs constructed in [29], to the best of our knowledge, all known examples of self-complementary Cayley graphs are Cayley graphs of nilpotent groups, and most of them are Cayley graphs of abelian groups.

In this chapter, we introduce a classical method for constructing self-complementary vertex-transitive graphs, that is constructions by group automorphisms. We then discuss its associated properties and problems, and give a new construction of self-complementary Cayley graphs of non-nilpotent groups, which is inspired by the classical method.

Theorem 3.0.8. *Let $R = \mathbb{Z}_p^d{:}\mathbb{Z}_\ell \leq \mathrm{AGL}(1, p^d)$, where $p^d - 1$ is divisible by 8, and ℓ is a primitive divisor of $p^d - 1$. Then there exist Cayley graphs of R which are self-complementary.*

3.1 Self-Complementary Cayley Graphs

Let R be a group and let $S \subseteq R^\#$ be self-inverse. Let $\Gamma = \mathrm{Cay}(R, S)$ be a Cayley graph. Recall from Lemma 2.9.4 that every automorphism $\sigma \in \mathsf{Aut}(R)$ induces an isomorphism from $\mathrm{Cay}(R, S)$ to $\mathrm{Cay}(R, S^\sigma)$. Also note that the complement of $\mathrm{Cay}(R, S)$ is $\mathrm{Cay}(R, R^\# \setminus S)$. Thus, if the set S admits an associated $\sigma \in \mathsf{Aut}(R)$ such that

$$S^\sigma = R^\# \setminus S, \tag{3.1}$$

then

$$\Gamma = \mathrm{Cay}(R, S) \cong \mathrm{Cay}(R, S^\sigma) = \mathrm{Cay}(R, R^\# \setminus S) = \overline{\Gamma},$$

and hence Γ is self-complementary. In this case, Γ is a self-complementary graph, and σ is a complementing isomorphism of Γ. Noting that S is self-inverse, that is $S = S^{-1}$, we further require that σ^2 is fixed-point-free by Lemma 2.11.3, and $g^{-1} \in g^{\langle\sigma^2\rangle}$ for any $g \in R$. This motivates the following definitions.

Definition 3.1.1. Let R be a group, and let $\sigma \in \mathsf{Aut}(R)$. The automorphism σ is said to be *fixed-point-free* if σ does not fix any non-identity elements of R. Let $S \subseteq R^{\#}$ be such that $S^{\sigma} = R^{\#} \setminus S$. Then

(i) S is an *SC-subset* of R (SC stands for self-complementary);

(ii) σ is a *normal complementing isomorphism* between the graphs $\mathrm{Cay}(R, S)$ and $\mathrm{Cay}(R, R^{\#} \setminus S)$.

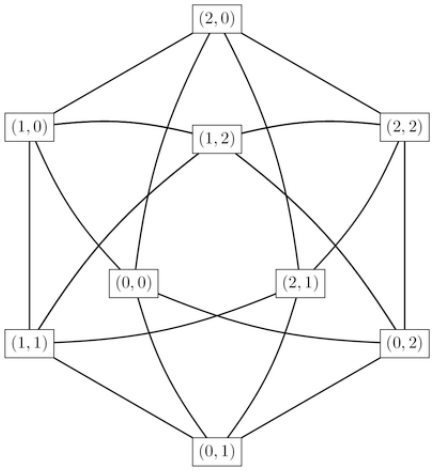


Figure 3.1: A self-complementary Cayley graph of the group $\mathbb{Z}_3^2$

Godsil [20, Lemma 2.1] showed that $\mathbf{N}_{\mathsf{Aut}\Gamma}(R) = R{:}\mathsf{Aut}(R, S)$ for a graph $\Gamma = \mathrm{Cay}(R, S)$. In fact, when Γ is self-complementary with a complementing isomorphism σ, this result is extendable to $X := \langle \mathsf{Aut}\Gamma, \sigma \rangle$.

Lemma 3.1.2. *Let $\Gamma = \mathrm{Cay}(R, S)$ be self-complementary with a normal complementing isomorphism σ. Let $\hat{R}$ be the right multiplication regular group on the vertex set $V = R$. Then*

$$\mathbf{N}_X(\hat{R}) = \hat{R}{:}\langle \mathsf{Aut}(R, S), \sigma \rangle.$$

Proof. By Lemma 2.5.1,

$$\mathbf{N}_X(\hat{R}) = \mathbf{N}_{\mathrm{Sym}(R)}(\hat{R}) \cap X = \left(\hat{R}{:}\mathsf{Aut}(R)\right) \cap X = \hat{R}{:}\langle \mathsf{Aut}(R, S), \sigma \rangle.$$

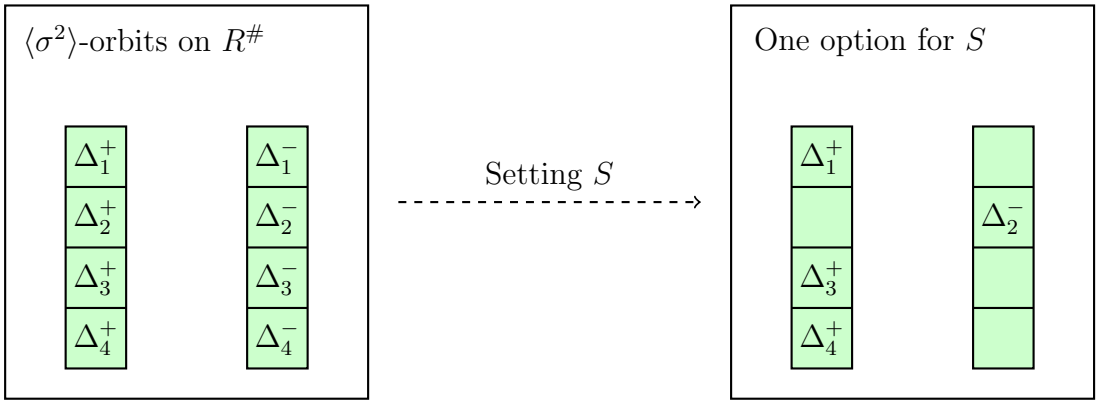
□

Conversely, if a group R has an automorphism σ of order a power of 2 such that σ^2 is fixed-point-free, then the following construction indeed produces self-complementary graphs (see [28]).

Construction 3.1.3. *Let R be a group and let $\sigma \in \mathsf{Aut}(R)$ of order a power of 2 be such that σ^2 is fixed-point-free. Then every orbit of $\langle\sigma\rangle$ on $R^\#$ has length divisible by 4 and is divided into two parts by $\langle\sigma^2\rangle$. We define a subset S and a graph $\Gamma = \mathrm{Cay}(R, S)$ as follows:*

(1) *Let $\Delta_1, \Delta_2, \ldots, \Delta_r$ be the $\langle\sigma\rangle$-orbits on $R^\#$, and label the two orbits of $\langle\sigma^2\rangle$ on Δ_i as Δ_i^+ and Δ_i^- for $i \in \{1, \ldots, r\}$.*

(2) *Set $S = \cup_{i=1}^r \Delta_i^{\varepsilon_i}$, where $\varepsilon_i = +$ or $-$. (We remark that there are 2^r different choices for such a subset S.)*



Lemma 3.1.4. *Let $\Gamma = \mathrm{Cay}(R, S)$ be constructed as in Construction 3.1.3. Then Γ is self-complementary with σ being a normal complementing isomorphism of Γ.*

Cayley graphs have been used to construct various self-complementary vertex-transitive graphs (see Sachs (1962), Zelinka (1979), Suprunenko (1985) and Rao (1985), and more recent work in [14, 46, 56]). However, not all self-complementary vertex-transitive graphs are Cayley graphs (see [29] for example).

3.2 Fixed-Point-Free Automorphisms of Groups

The method of Construction 3.1.3 naturally leads us to the following group theoretic problem.

Problem 3.2.1. Characterise finite groups which have fixed-point-free automorphisms of order a power of 2.

This problem has been studied in the literature. D. Gorenstein and I. N. Herstein [21] showed that if a group has a fixed-point-free automorphism of order 4, then its commutator subgroup is nilpotent. Later, Huhro [24] proved the following general result.

Theorem 3.2.2. (Huhro) *If a finite group R has an automorphism of order 2^n then its nilpotent height $h(R)$ is at most n.*

Moreover, Berkovič [7] showed the following.

Theorem 3.2.3. *A metacyclic group that admits a fixed-point-free automorphism is abelian.*

Next, we study groups with fixed-point-free automorphisms.

Lemma 3.2.4. *If A has a fixed-point-free automorphism σ and B has a fixed-point-free automorphism τ, then (σ, τ) is a fixed-point-free automorphism of $A \times B$.*

Proof. Suppose that (σ, τ) fixes a non-identity element (a, b), where $a \in A$ and $b \in B$. Then $(a, b) = (a, b)^{(\sigma,\tau)} = (a^\sigma, b^\tau)$. Thus $a^\sigma = a$, and $b^\tau = b$. Since (a, b) is not an identity element, $a \neq 1$ or $b \neq 1$, which is a contradiction. □

This simple lemma provides us with a method for constructing self-complementary graphs based on smaller examples, see . An immediate consequence of Lemma 3.2.4 is about nilpotent groups.

Proposition 3.2.5. *A nilpotent group has a fixed-point-free automorphism if and only if each of its Sylow subgroups has a fixed-point-free automorphism.*

Lemma 3.2.6. *If a group has a fixed-point-free automorphism of order a prime-power, then so does each of its Sylow subgroups.*

Proof. Let G be a group which has a fixed-point-free automorphism σ of order p^f with p prime. Then the order $|G|$ is coprime to p. Let P be a Sylow subgroup of G. Then P^σ is a Sylow subgroup, and by Sylow theorem, there exists an element $g \in G$ such that $P^{\sigma g} = (P^\sigma)^g = P$.

Suppose that a non-identity element $x \in P$ is fixed by σg. Then

$$x^\sigma = x^{g^{-1}},$$

and so $x = x^{\sigma^{p^f}} = x^{g^{-p^f}}$. Since the order $o(g)$ is relatively prime to p, we conclude that $x^{g^{-1}} = x$, and so $x^\sigma = x$, which is a contradiction □

This shows that a critical case for solving Problem 3.2.1 is to characterise finite p-groups with p prime which have fixed-point-free automorphisms of order a power of 2.

Let R be an abelian group of order pq with p, q prime. Then $R \cong \mathbb{Z}_p^2$ or $\mathbb{Z}_{pq}$. The next lemma tells us when R has an automorphism σ of order a power of 2 such that σ^2 is fixed-point-free.

Lemma 3.2.7. *Let R be an abelian group of order pq where p, q are odd prime numbers. Then there exists $\sigma \in \mathsf{Aut}(R)$ such that σ^2 is of order a power of 2 and fixed-point-free if and only if $R \cong \mathbb{Z}_p^2$, or R is cyclic with $p, q \equiv 1 \pmod 4$.*

Proof. First, assume that $R = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p^2$. Let $\sigma \in \mathsf{Aut}(R)$ be such that

$$\sigma : \quad a \to b, \quad b \to a^{-1}.$$

Then σ^2 maps each element $x \in R$ to the inverse x^{-1}, hence σ^2 is fixed-point-free, and σ^2 has order 2.

Next, assume that $R = \langle a \rangle = \mathbb{Z}_{p^2}$. Then $\mathsf{Aut}(R) = \mathbb{Z}_{p(p-1)}$, and thus 4 divides the order of $\mathsf{Aut}(R)$ if and only if 4 divides $p-1$. Moreover, if σ is an automorphism of R of order divisible by 4, then σ^2 obviously fixes no non-identity element of R.

Finally, assume that $p \neq q$, and $R = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Then $\mathsf{Aut}(R) = \mathsf{Aut}(\langle a \rangle) \times \mathsf{Aut}(\langle b \rangle) = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$. If $p, q \equiv 1 \pmod 4$, then let $x_1 \in \mathsf{Aut}(\langle a \rangle), y_1 \in \mathsf{Aut}(\langle b \rangle)$ be of order 4. By Lemma 3.2.4 we have $(x_1, y_1) \in \mathsf{Aut}(R)$ is of order 4 and the square $(x_1, y_1)^2$ fixes no non-identity element of R. Conversely, suppose that $p \not\equiv 1 \pmod 4$. Let $\sigma \in \mathsf{Aut}(R)$ be of order a power of 2. Then $\sigma = (x^i, y^j)$ such that x^i is of order 2, and $\sigma^2 = (x^{2i}, y^{2j}) = (1, \tau^{2j})$. Clearly, σ^2 fixes the element a. □

3.3 Self-Complementary Cayley graphs of Non-Nilpotent Groups

In this section, we present an infinite family of self-complementary Cayley graphs of non-nilpotent groups.

Let $F = \mathbb{F}_{p^d}$ be a field of order p^d, where p is a prime and d is a positive integer. Then the additive group F^+ and the multiplicative group $F^\times$ are such that

$$F^+ \cong \mathbb{Z}_p^d, \quad F^\times = \mathbb{Z}_{p^d-1}.$$

The group $F^\times$ naturally acts on F^+ by multiplication, giving rise to the group $\mathrm{AGL}(1, p^d) = F^+{:}F^\times \cong \mathbb{Z}_p^d{:}\mathbb{Z}_{p^d-1}$. The field F has an automorphism ρ of order d, called a *Frobenius automorphism*, such that

$$g^\rho = g^p, \text{ where } g \in F^\times.$$

This action defines groups: $\Gamma\mathrm{L}(1, p^d) = \langle F^\times, \rho \rangle \cong \mathbb{Z}_{p^d-1}{:}\mathbb{Z}_d$, and

$$\mathrm{A}\Gamma\mathrm{L}(1, p^d) = (F^+{:}F^\times){:}\langle \rho \rangle \cong (\mathbb{Z}_p^d{:}\mathbb{Z}_{p^d-1}){:}\mathbb{Z}_d \cong \mathbb{Z}_p^d{:}\Gamma\mathrm{L}(1, p^d).$$

Now we are ready to construct new self-complementary Cayley graphs. Let p be a prime, recall that the *p-part* n_p of an integer n is the highest p-power that divides n.

Construction 3.3.1. Let p be an odd prime, and $d = 2^f m$ where $f \geq 2$ and m is odd. Let ℓ be a primitive prime divisor of $p^d - 1$. Let $g \in F^\times$ be of order ℓ, and let

$$R = F^+{:}\langle g \rangle = \mathbb{Z}_p^d{:}\mathbb{Z}_\ell \leq \mathrm{AGL}(1, p^d).$$

Let $z \in F^\times$ be of order $(p^d - 1)_2$ and $\sigma = \rho^m$, and let

$$\tau = \sigma z.$$

The group R is a Frobenius group with F^+ being the Frobenius kernel and $\langle g\rangle$ being a Frobenius complement. Thus, in particular, R is not nilpotent. The next lemma shows that τ is a fixed-point-free automorphism of R of order $2^f \geq 4$.

Lemma 3.3.2. *The automorphism $\tau \in \mathsf{Aut}(R)$ is of order $(p^d-1)_2 = 2^f(p-1)_2$, and τ^2 fixes no non-identity elements of R.*

Proof. Since the order of the Frobenius automorphism ρ has order $2^f m$, the order of $\sigma = \rho^m$ equals 2^f, and by definition

$$x^\sigma = x^{p^m}, \text{ where } x \in \mathrm{GL}(1, p^d).$$

In particular, $z^\sigma = z^{p^m}$, and so $\tau^2 = \sigma z \sigma z = \sigma^2 z^{p^m+1}$, and

$$\tau^{2^i} = \sigma^{2^i} z^{(p^{2^{i-1}m}+1)\ldots(p^{2m}+1)(p^m+1)}.$$

Let $2^s = (p-1)_2$ be the 2-part of $p-1$. Then $\tau^{2^f} \in \langle z\rangle$ is of order 2^s, and $o(\tau) = o(z) = 2^f(p-1)_2$.

Let z_0 be the involution of $\langle z\rangle$. Then $z_0 \in \langle \tau^{2^f}\rangle$. Now any element of R may be written as ax such that $a \in \mathbb{Z}_p^d$ and $x \in \langle g\rangle \leq F^\times$. If $a \neq 1$ then

$$(ax)^{z_0} = a^{-1}x \neq ax.$$

Thus z_0 fixes no point of $R \setminus \langle g\rangle$. It implies that τ^2 and τ fix no points of $R \setminus \langle g\rangle$. On the other hand, if $a = 1$ and $x \neq 1$, then $o(x) = \ell$, and since $xz = zx$, we have

$$x^{\tau^{2^{f-1}}} = x^{\sigma^{2^{f-1}} z^{(p^{2^{f-1}m}+1)\ldots(p^{2m}+1)(p^m+1)}} = x^{p^{2^{f-1}m}}.$$

If $x^{p^{2^{f-1}m}} = x^{\tau^{2^{f-1}m}} = x$, then $x^{p^{2^{f-1}m}-1} = 1$. Noticing that $2^{f-1}m < 2^f m = d$, this is not possible since x is of order ℓ and ℓ is a primitive prime divisor of p^d-1. Therefore, τ^2 is a fixed-point-free automorphism of the group R; in particular, τ is a fixed-point-free automorphism of R. □

Proof of Theorem 3.0.8. Let $R = \mathbb{Z}_p^d{:}\mathbb{Z}_\ell \leq \mathrm{AGL}(1, p^d)$ where $p^d \equiv 1 \pmod 8$ and ℓ is a primitive divisor of p^d-1. Let τ be an automorphism of R as constructed in Construction 3.3.1. Then by Lemma 3.3.2, τ is of order $2^f(p-1)_2 \geq 8$ and τ^2 is fixed-point-free. Thus, by Construction 3.1.3, there exist $S \subseteq R^\#$ such that $\Gamma = \mathrm{Cay}(R, S)$ is self-complementary with τ being a complementing isomorphism. □

We note that the smallest group satisfying Construction 3.3.1 is $R = \mathbb{Z}_3^4{:}\mathbb{Z}_5$. This gives rise to self-complementary graphs of order $3^4 \cdot 5$. Applying Lemma 3.2.4 along with Construction 3.3.1 we can produce more examples of self-complementary graphs.

Example 3.3.3. Let $R_1 = \mathbb{Z}_3^4{:}\mathbb{Z}_5$ and $R_2 = \mathbb{Z}_5^4{:}\mathbb{Z}_{13}$ be Frobenius groups, and let $\sigma_1 \in \mathsf{Aut}(R_1), \sigma_2 \in \mathsf{Aut}(R_2)$ be as in Construction 3.3.1. Then there is a self-complementary Cayley graph of the group $R_1 \times R_2$ with (σ_1, σ_2) being a complementing isomorphism.

Chapter 4

More Constructions

It is known that there are self-complementary circulants which cannot be constructed by the method given in Construction 3.1.3 (see [25, 38]). In this chapter, we present a new method to construct a family of self-complementary Cayley graphs of non-abelian metacyclic groups.

Theorem 4.0.4. *Let R be a non-abelian split metacyclic p-group, where $p \equiv 1 \pmod 4$ is a prime. Then there exist self-complementary Cayley graphs of R.*

4.1 Self-Complementary Metacirculants

We first present a simple lemma.

Lemma 4.1.1. *Let r be an integer, and let p be a prime such that $2^r \mid p-1$. Then the simultaneous equations*

$$\begin{cases} \lambda^{2^r} \equiv 1 \pmod{p^d} & \cdots\cdots \ (4.1) \\ \lambda^{2^r} \equiv 1 \pmod{p^e} & \cdots\cdots \ (4.2) \end{cases}$$

have a solution.

Proof. Without loss of generality, assume that $d \geq e$, so that equation (4.1) implies equation (4.2). Let $G = \mathbb{Z}_{p^d}$ be an additive group. One can define the natural multiplication on G so that all the multiplicative invertible elements of G form a group $G^* = \langle \mu \rangle \cong \mathbb{Z}_{p^{d-1}(p-1)}$. Consequently,

$$\mu^{p^{d-1}(p-1)} \equiv 1 \pmod{p^d}.$$

Therefore, the number $\mu^{\frac{p-1}{2^r}p^{d-1}}$ gives a solution to equation (4.1) and hence equation (4.2). □

Now we start our construction. Let R be a split metacyclic p-group, where p is a prime congruent to 1 modulo 4, that is, $R = \mathbb{Z}_{p^d}{:}\mathbb{Z}_{p^e}$, where d, e are positive integers. Then R has a pair of generators a, b such that $\langle a \rangle \lhd R$, $o(a) = p^d$, $o(b) = p^e$, and

$$bab^{-1} = a^{1+p^f},$$

where f is a positive integer. Let $c = a^{p^f}$. Then the commutator subgroup

$$R' = \langle c \rangle \cong \mathbb{Z}_{p^{d-f}}.$$

Let σ be an automorphism of $\langle a \rangle$, and τ be an automorphism of $\langle b \rangle$ such that σ, τ have same order 2^r, where $4 \leq 2^r \leq (p-1)_2$.

By Lemma 4.1.1 there exists a positive integer λ which is coprime to p such that

$$a^\sigma = a^\lambda, \quad b^\tau = b^\lambda.$$

By Construction 3.1.3 we can construct an SC-subset $S_1 \subset \langle a \rangle$ with respect to σ. Then $S_1^\sigma = \langle a \rangle^\# \setminus S_1$, and so for any elements $x = a^{i_1}$ and $y = a^{i_2}$,

$$a^{i_2 - i_1} = yx^{-1} \in S_1 \Longleftrightarrow a^{(i_2-i_1)\lambda} = y^\lambda x^{-\lambda} = y^\sigma (x^\sigma)^{-1} \notin S_1.$$

Let $\overline{R} = R/\langle c \rangle = \langle \overline{a}, \overline{b} \rangle \cong \mathbb{Z}_{p^f} \times \mathbb{Z}_{p^e}$. Then the pair (σ, τ) induces an automorphism $\overline{\rho}$ of $\overline{R}$ as follows

$$(\overline{a}^i \overline{b}^j)^{\overline{\rho}} = \overline{a}^{i\lambda} \overline{b}^{j\lambda} = (\overline{a}^i \overline{b}^j)^\lambda, \quad \text{where } 0 \leq i \leq p^f - 1 \text{ and } 0 \leq j \leq p^e - 1.$$

Let $\overline{S}_2 \subset \langle \overline{a}, \overline{b} \rangle$ be an SC-subset with respect to $\overline{\rho}$. Then $\overline{S}_2^{\overline{\rho}} = \langle \overline{a}, \overline{b} \rangle^\# \setminus \overline{S}_2$, and the Cayley graph

$$\Sigma = \mathrm{Cay}(\langle \overline{a}, \overline{b} \rangle, \overline{S}_2)$$

is self-complementary with complementing isomorphism $\overline{\rho}$.

Let $I = \{(i,j) \mid \overline{a}^i \overline{b}^j \in \overline{S}_2, 0 \leq i \leq p^f - 1, 0 \leq j \leq p^e - 1\}$, and let

$$S_2 = \bigcup_{(i,j) \in I} a^i b^j \langle c \rangle,$$
$$\Gamma_2 = \mathrm{Cay}(R, S_2).$$

We notice that, since $a^{p^f} = c$, elements of R can be written as

$$a^i b^j c^k, \quad \text{where } 0 \leq i \leq p^f - 1,\ 0 \leq j \leq p^e - 1, \text{ and } 0 \leq k \leq p^f - 1.$$

By the definition, we have the conclusion in the next lemma.

Lemma 4.1.2. *The Cayley graph $\Gamma_2 = \Sigma[\overline{\mathbf{K}}_{p^f}]$, and for any elements $x = a^{i_1} b^{j_1} c^{k_1}$ and $y = a^{i_2} b^{j_2} c^{k_2}$, where $0 \leq i_1 \neq i_2 \leq p^f - 1$, $0 \leq j_1, j_2 \leq p^e - 1$, and $0 \leq k_1, k_2 \leq p^f - 1$, we have*

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^\lambda \overline{x}^{-\lambda} = \overline{y}^{\overline{\rho}} (\overline{x}^{\overline{\rho}})^{-1} \notin \overline{S}_2.$$

Now we are ready to present our construction of self-complementary Cayley graphs of the metacyclic group R.

Construction 4.1.3. Use the notation defined above, let

$$S = S_1 \cup (S_2 \setminus \langle a \rangle),$$

and $\Gamma = \mathrm{Cay}(R, S)$. Define a permutation ρ of the set R:

$$\rho: \ a^i b^j c^k \mapsto a^{i\lambda} b^{j\lambda} c^{k\lambda}, \quad \text{where } 0 \leq i \leq p^f - 1,\ 0 \leq j \leq p^e - 1, \text{ and } 0 \leq k \leq p^f - 1.$$

We remark that with a proper choice of S_1 and $\overline{S}_2$, the graph Γ produced in this construction is not a lexicographic graph product of smaller graphs.

We note that the map ρ only fixes the identity of R, but ρ is not an automorphism of the group R. The next lemma shows ρ maps Γ to its complement $\overline{\Gamma}$.

Lemma 4.1.4. *The Cayley graph Γ defined in Construction 4.1.3 is self-complementary, and ρ is a complementing isomorphism.*

Proof. Pick two vertices $x = a^{i_1}b^{j_1}c_1$, and $y = a^{i_2}b^{j_2}c_2$, where $0 \le i_1, i_2 \le p^f - 1$, $0 \le j_1, j_2 \le p^e - 1$, and $c_1, c_2 \in \langle c\rangle$. Recall that $\langle c\rangle = R'$, so

$$\begin{aligned} yx^{-1} &= (a^{i_2}b^{j_2}c_2)(a^{i_1}b^{j_1}c_1)^{-1} \\ &= a^{i_2-i_1}b^{j_2-j_1}c'; \end{aligned}$$

$$\begin{aligned} y^\rho(x^\rho)^{-1} &= (a^{i_2\lambda}b^{j_2\lambda}c_2^\lambda)(a^{i_1\lambda}b^{j_1\lambda}c_1^\lambda)^{-1} \\ &= a^{(i_2-i_1)\lambda}b^{(j_2-j_1)\lambda}c''. \end{aligned}$$

First, assume that $j_2 = j_1$. Then we have

$$\begin{aligned} &yx^{-1} = a^{i_2-i_1}c' \in a^{i_2-i_1}\langle c\rangle \\ &y^\rho(x^\rho)^{-1} = a^{(i_2-i_1)\lambda}c'' \in a^{(i_2-i_1)\lambda}\langle c\rangle = y^\sigma(x^\sigma)^{-1}\langle c\rangle. \end{aligned}$$

Both yx^{-1} and $y^\rho(x^\rho)^{-1} \in \langle a\rangle$. By the definition of σ, we have $yx^{-1} \in S_1$ if and only if $y^\rho(x^\rho)^{-1} = y^\sigma(x^\sigma)^{-1} \notin S_1$.

Assume now $j_2 \neq j_1$. Then $\overline{y}\,\overline{x}^{-1} = \overline{a}^{i_2-i_1}\overline{b}^{j_2-j_1}$, and $\overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} = \overline{a}^{(i_2-i_1)\lambda}\overline{b}^{(j_2-j_1)\lambda}$. By the definition of S_2 and $\overline{S}_2$, we have

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} \notin \overline{S}_2 \Longleftrightarrow y^\rho(x^\rho)^{-1} \notin S_2.$$

Therefore, x, y are adjacent in Γ if and only if x^ρ, y^ρ are not adjacent in Γ, and so ρ is a isomorphism between Γ and $\overline{\Gamma}$. In particular, $\Gamma \cong \overline{\Gamma}$, and ρ is a complementing isomorphism. □

We remark that the smallest example of self-complementary graphs that can be constructed by Construction 4.1.3 is Cayley graphs of the group $\mathbb{Z}_{25}{:}\mathbb{Z}_5$.

Proof of Theorem 4.0.4. Let R be a non-abelian split metacyclic group. Let Γ be a Cayley graph of R defined in Construction 4.1.3. Then by Lemma 4.1.4, Γ is a self-complementary metacirculant. □

4.2 The Lexicographic Product

We have seen a generic construction method given in Lemma 3.2.4 based on the direct product of groups. Here we introduce a well-known method based on the lexicographic product (which sometimes also called the *wreath product*). Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ be graphs. The *lexicographic product* of Γ_2 by

Γ_1 is the graph Γ with the vertex set $V = V_1 \times V_2$ such that two vertices (v_1, v_2) and (v_1', v_2') are adjacent if and only if v_1, v_1' are adjacent in Γ_1, or $v_1 = v_1'$ and v_2, v_2' are adjacent in Γ_2. We usually denote Γ by $\Gamma_1[\Gamma_2]$. It is not hard to see that $\mathsf{Aut}\Gamma_2 \wr \mathsf{Aut}\Gamma_1 \leq \mathsf{Aut}\Gamma$. Moreover, one may easily find that both the self-complementary and vertex-transitive properties are inherited by the lexicographic product.

Lemma 4.2.1. [6, Theorems 4.2 and 4.3] *If both graphs Γ_1, Γ_2 are self-complementary (or vertex-transitive), then so is $\Gamma_1[\Gamma_2]$.*

The smallest self-complementary vertex-transitive graph is the 5-cycle $\mathbf{C}_5$. Thus, by Lemma 4.2.1 we can produce the graph $\mathbf{C}_5[\mathbf{C}_5]$, which is a self-complementary vertex-transitive graph of order 25, and whose full automorphism group contains a subgroup $\mathrm{D}_{10} \wr \mathrm{D}_{10}$. Moreover, the converse of Lemma 4.2.1 also holds for self-complementary vertex-transitive graphs.

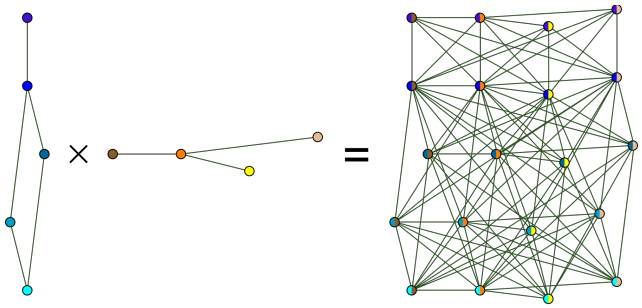


Figure 4.1: The lexicographic product of two graphs[1]

Lemma 4.2.2. *Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph with a complementing isomorphism σ. Suppose that V admits a block system $\mathcal{B}$ under the action of $X := \langle \mathsf{Aut}\Gamma, \sigma \rangle$. Let $B \in \mathcal{B}$, and let $\Gamma_1 := \Gamma_{\mathcal{B}}, \Gamma_2 := [B]_\Gamma$. Suppose that $\Gamma \cong \Gamma_1[\Gamma_2]$. Then both Γ_1, Γ_2 are self-complementary and vertex-transitive.*

Proof. It follows by the vertex-transitivity of Γ that Γ_1, Γ_2 are vertex-transitive. Moreover, Γ_2 is self-complementary by [31, Lemma 4.1], so we need only to show that Γ_1 is self-complementary. Let $B, C \in \mathcal{B}$, and let $\alpha \in B, \beta \in C$. Assume that B, C are adjacent in Γ_1. Then $\{\alpha, \beta\}$ is an edge in Γ, and $\{\alpha, \beta\}^\sigma = \{\alpha^\sigma, \beta^\sigma\}$ is a nonedge in Γ. It implies that $[B^\sigma, C^\sigma]$ is empty. Similar argument shows that if $[B, C]$ is empty then $[B^\sigma, C^\sigma] \cong \mathbf{K}_{n,n}$, where $n = |B|$. Thus, σ induces a map from Γ_1 to its complement. Furthermore, B, C are adjacent in Γ_1 if and only if B^σ, C^σ are adjacent in $\overline{\Gamma_1}$, so σ induces an isomorphism between Γ_1 and $\overline{\Gamma_1}$, and Γ_1 is self-complementary. □

[1] http://en.wikipedia.org/wiki/Lexicographic_product_of_graphs

The lexicographic product also preserves some metacirculants.

Lemma 4.2.3. *Let $\Gamma_1 = (V_1, E_1), \Gamma_2 = (V_2, E_2)$ be self-complementary metacirculants of coprime orders. Then $\Gamma = \Gamma_1[\Gamma_2]$ is a self-complementary metacirculant.*

Proof. Let

$$R_1 = \mathbb{Z}_a.\mathbb{Z}_b \leq \mathsf{Aut}\Gamma_1,\ R_2 = \mathbb{Z}_c.\mathbb{Z}_d \leq \mathsf{Aut}\Gamma_2$$

be transitive on V_1, V_2 respectively. Consider that $\mathsf{Aut}\Gamma \geq \mathsf{Aut}\Gamma_2 \wr \mathsf{Aut}\Gamma_1$. Let $\bar{x} = (x, \ldots, x)$ be a diagonal element in the base group of the wreath product, where $x \in R_2$. Then for each $y \in R_1$, y permutes the coordinates of $\bar{x}$ but fixes $\bar{x}$. So $\mathsf{Aut}\Gamma$ contains a transitive subgroup $R := \langle \bar{x}, y | x \in R_2, y \in R_1 \rangle \cong R_1 \times R_2$. Note that $R = (\mathbb{Z}_a.\mathbb{Z}_b) \times (\mathbb{Z}_c.\mathbb{Z}_d)$. Then R contains a normal subgroup $N \cong \mathbb{Z}_a \times \mathbb{Z}_c$, and $R/N \cong \mathbb{Z}_b \times \mathbb{Z}_d$. Since $(ab, cd) = 1$, we further have $N \cong \mathbb{Z}_{ac}, R/N \cong \mathbb{Z}_{bd}$, so that R is metacyclic. □

Chapter 5

Self-Complementary Vertex-Primitive Graphs

5.1 Overview and Main Results

Let $\Gamma = (V, E)$ be a self-complementary graph, and let σ be a complementing isomorphism. Then $\sigma^2 \in \mathsf{Aut}\Gamma$, and hence σ normalises $\mathsf{Aut}\Gamma$. Let $G = \mathsf{Aut}\Gamma$, and let $X = \langle G, \sigma \rangle$. Then G is a normal subgroup of X of index 2, and $X = G.\mathbb{Z}_2$.

Assume that X is primitive on the vertex set V. Recall from Theorem 5 that

(i) X is an affine group with socle of odd order; or

(ii) X is in product action with socle $\mathrm{PSL}(2, q^2)^\ell$, and $|V| = (q^2(q^2+1)/2)^\ell$, where q is odd and $\ell \geq 2$.

The triple (G, X, Γ) in item (ii) is in some sense known, which gives rise to vertex-transitive self-complementary graphs that are not Cayley graphs, refer to [22] and [29]. On the other hand, the graphs in item (i) are all Cayley graphs of elementary abelian p-groups. In this chapter, we present a generic construction for this type of self-complementary graphs.

Theorem 5.1.1. *Let $\Gamma = (V, E)$ be a self-complementary graph such that $\mathsf{Aut}\Gamma$ is a primitive affine group on V. Then $|V| = p^d \equiv 1 \pmod 4$ with p prime, and for $d \geq 2$, identifying V with a vector space on $\mathbb{F}_p$ of dimension d, a complementing isomorphism σ has the form*

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_r),$$

where $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$ such that V_i is a subspace of dimension 2^{e_i} and $d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r}$, and

(i) *if $e_i = 1$ and $p \equiv 3 \pmod 4$, then $\sigma_i \in \mathrm{GL}(V_i)$ is a primitive element of a 2-power order divisible by 4;*

(ii) *if e_i and p are not as in* (i)*, then σ_i is a primitive element of* $\mathrm{GL}(1, p^{2^{e_i}})$ *of order* $2^{e_i-1}(p^2-1)_2$.

We remark that, although Theorem 5.1.1 provides a generic construction method for self-complementary vertex-primitive graphs of affine type, not every example constructed in this way is vertex-primitive. This motivated us to propose a problem.

Problem 5.1.2. Given a fixed-point-free linear transformation σ of $\mathbb{F}_p^d$, determine irreducible subgroups H of $\mathrm{GL}(d,p)$ such that σ normalises H, $\sigma^2 \in H$, and σ fixes no orbit of H on $V \setminus \{0\}$.

5.2 Constructions

Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph with a complementing isomorphism σ. Suppose that the group $X = \langle \mathsf{Aut}\Gamma, \sigma \rangle$ is of affine type. Then we can identify the vertex set V with a vector space $\mathbb{F}_p^d$ with p prime. Then the vertices form an additive group which is isomorphic to the elementary abelian group $\mathbb{Z}_p^d$. Since $|V| \equiv 1 \pmod 4$, the prime p is odd. The complementing isomorphism $\sigma \in \mathrm{GL}(d,p)$ is a linear transformation of V, and fixes no nonzero vector in V.

Construction 5.2.1. Using the notation defined above, let

$$d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r},$$
$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r,$$

where V_i is a subspace of V of dimension 2^{e_i}. If $e_i = 1$ and $p \equiv 3 \pmod 4$, let $\sigma_i \in \mathrm{GL}(V_i)$ be a primitive element of order a 2-power divisible by 4; otherwise let $\sigma_i \in \mathrm{GL}(V_i)$ be a primitive element of order $2^{e_i-1}(p^2-1)_2$. Let

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_r).$$

Since every σ_i is a scalar transformation of V_i, it fixes no non-identity vector of V_i. By Lemma 3.2.4, σ fixes no non-identity vector of V.

Let p be a prime and let $m \in \mathbb{N}$. A positive integer d is said to be a *primitive divisor* of $p^m - 1$ if it satisfies

$$d \mid (p^m - 1), \text{ and } d \nmid (p^i - 1) \quad \text{for all } i < m.$$

Irreducible representations of cyclic groups are characterised by primitive divisors.

Lemma 5.2.2. *Let p be a prime. The cyclic group $\mathbb{Z}_d$ is faithful and irreducible on a vector space V of dimension m over the field $\mathbb{F}_p$ if and only if d is a primitive divisor of $p^m - 1$.*

Proof. By Lemma 2.6.5, for each positive integer $i \leq m$, the group $\mathrm{GL}(i,p)$ contains a Singer subgroup $\mathrm{GL}(1, p^i) \cong \mathbb{Z}_{p^i-1}$. Now the result follows by the fact that each $\mathrm{GL}(i,p)$ acts on a vector space of dimension i over the field $\mathbb{F}_p$, which is a subspace of V. □

The next lemma shows that every complementing isomorphism of a primitive affine self-complementary graph is as in Construction 5.2.1.

Lemma 5.2.3. *Assume that X is a primitive affine group on the vertex set V. Then each complementing isomorphism has the form given in Construction 5.2.1.*

Proof. Let σ be a complementing isomorphism between Γ and $\overline{\Gamma}$. As mentioned before, we may assume that σ is of order 2^f with $f \geq 2$. Let N be the unique minimal normal subgroup of X. Then $N \cong \mathbb{Z}_p^d$ is regular on the vertex set V, and is normalised by σ. Let

$$Y = \langle N, \sigma \rangle = N{:}\langle \sigma \rangle \cong \mathbb{Z}_p^d{:}\mathbb{Z}_{2^f}.$$

Then Y is a subgroup of X, and vertex-transitive on the graph Γ.

Case 1. Assume that Y is primitive on the vertex set V. Then the cyclic group $\langle \sigma \rangle$ is irreducible on V, and hence the order 2^f is a primitive divisor of $p^d - 1$, that is,

$$2^f \,\big|\, (p^d - 1), \text{ but } 2^f \nmid (p^i - 1) \text{ for any } i < d.$$

First, suppose that d is odd. Then

$$p^d - 1 = (p-1)(p^{d-1} + \cdots + p + 1) = (p-1)\ell,$$

and ℓ is odd. Thus $2^f \,\big|\, (p-1)$, and since 2^f is a primitive divisor of $p^d - 1$, we conclude that $d = 1$, and σ is as in Construction 5.2.1 with $r = 1$.

Assume next that d is even. Write $d = 2^k m$, where m is odd. Then

$$p^d - 1 = p^{2^k m} - 1 = (p^{2^k} - 1)((p^{2^k})^{m-1} + \cdots + p^{2^k} + 1),$$

and $(p^{2^k})^{m-1} + \cdots + p^{2^k} + 1$ is odd. Thus we have $2^f \,\big|\, (p^{2^k} - 1)$. Since 2^f is a primitive divisor of $p^d - 1$, we have that $m = 1$, and

$$d = 2^k.$$

If $k = 1$, then

$$p^d - 1 = p^2 - 1 = (p-1)(p+1).$$

Since p is odd, we have $p \equiv \pm 1 \pmod 4$.

(i) If $p \equiv 1 \pmod 4$, then $p + 1 \equiv 2 \pmod 4$, and $(p+1)_2 = 2$. So σ is as in Construction 5.2.1.

(ii) If $p \equiv -1 \pmod 4$, then $p - 1 \equiv 2 \pmod 4$, and $(p-1)_2 = 2$. This yields that $4 \,\big|\, o(\sigma)$, as in Construction 5.2.1.

Suppose that $k \geq 2$. Then

$$p^d - 1 = p^{2^k} - 1 = (p^{2^{k-1}} + 1)(p^{2^{k-1}} - 1),$$

and $p^{2^{k-1}} - 1$ is divisible by 4. It implies that $p^{2^{k-1}} + 1$ is not divisible by 4. Therefore, if $2^f < (p^d - 1)_2$, then 2^f divides $p^{2^{k-1}} - 1$, which contradicts the fact that 2^f is a prime divisor of $p^d - 1$. So 2^f equals the 2-part $(p^d - 1)_2$. Moreover,

$$p^{2^k} - 1 = (p^{2^{k-1}} + 1) \dots (p^2 + 1)(p^2 - 1),$$

and as $(p^{2^i} + 1)_2 = 2$ for $i \geq 1$, we have $o(\sigma) = (p^{2^k} - 1)_2 = 2^{k-1}(p^2 - 1)_2$, as claimed in the lemma.

Case 2. Assume that Y is imprimitive. Then the cyclic group $\langle \sigma \rangle$ is reducible on V. By Maschke's theorem, the space V is a direct sum

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

such that $\langle \sigma \rangle$ fixes and irreducible on each subspace V_i, where $1 \leq i \leq r$. Since σ fixes no nonzero vector of V, σ fixes no nonzero vector of the subspace V_i. Let σ_i be the linear transformation of V_i induced by σ. Then V_i and σ_i satisfy Case 1, and we conclude that

$$V_i = \mathbb{F}_p^{2^{e_i}}, \text{ where } e_i \geq 0,$$

and $\sigma_i \in \mathrm{GL}(1, p^{2^{e_i}})$ is of order $2^{e_i - 1}(p^2 - 1)_2$. Now the dimension

$$d = 2^{e_1} + 2^{e_2} + \cdots + 2^{e_r},$$

and the complementing isomorphism σ can be expressed as

$$\sigma = (\sigma_1, \sigma_2, \dots, \sigma_r).$$

This completes the proof. □

Proof of Theorem 5.1.1. Let Γ be a self-complementary graph with a complementing isomorphism. Suppose that $X = \langle \mathsf{Aut}\Gamma, \sigma \rangle$ is an affine primitive group on V. Then σ is a linear transformation as in Construction 5.2.1. Now the result follows from Lemma 5.2.3. □

5.3 An Example

We present an example of self-complementary vertex-transitive graphs whose complementing isomorphisms are as in Construction 5.2.1.

Let $R = \mathbb{Z}_p^2$ with p prime. Then $\mathsf{Aut}(R) = \mathrm{GL}(2, p)$. Assume that $p \equiv \pm 1 \pmod{10}$. Then $\mathrm{GL}(2, p)$ contains an irreducible subgroup $\mathrm{SL}(2, 5)$, see [52, page 411]. Assume further that $p \equiv 1 \pmod 8$. Then the centre $\mathbf{Z}(\mathrm{GL}(2, p)) \cong \mathbb{Z}_{p-1}$ has order divisible by 8. Recall that an element $g \in \mathsf{Aut}(R)$ is *fixed-point-free* if and only if g does not fix any non-identity elements of R. Let σ be a 2-element of $\mathbf{Z}(\mathrm{GL}(2, p))$ which has order at least 8. Since σ is a scalar matrix, its action on R is fixed-point-free. Then $\langle \sigma, \mathrm{SL}(2, 5) \rangle = \langle \sigma \rangle \circ \mathrm{SL}(2, 5)$ is a subgroup of $\mathrm{GL}(2, p)$.

We first establish a basic fact about $\mathrm{SL}(2, 5)$.

Lemma 5.3.1. *The group* $\mathrm{SL}(2,5)$ *does not contain an element of order* 8.

Proof. Note that $\mathrm{SL}(2,5) = \mathbb{Z}_2.\mathrm{A}_5$ and the Sylow 2-subgroups of A_5 are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, so the Sylow 2-subgroups of $\mathrm{SL}(2,5)$ are isomorphic to $\mathbb{Z}_2.(\mathbb{Z}_2 \times \mathbb{Z}_2)$. On the other hand, $\mathbb{Z}_8 \neq \mathbb{Z}_2.(\mathbb{Z}_2 \times \mathbb{Z}_2)$, then the result follows. □

Lemma 5.3.2. *Let* $M = \langle \sigma^2, \mathrm{SL}(2,5) \rangle$ *and* $H = \langle \sigma, \mathrm{SL}(2,5) \rangle$. *Then* M *divides each* H*-orbit on* $R^\#$ *into two parts of equal size.*

Proof. Let Δ be an H-orbit on $R^\#$, and let $x \in \Delta$. Then $x^\sigma \in \Delta$. Suppose that M is transitive on Δ. Then there exists an element $g \in M$ such that $x^g = x^\sigma$. Thus $x^{\sigma g^{-1}} = x$. Since σ is in the centre of H, $\sigma g^{-1} = g^{-1}\sigma$. Hence $(\sigma g^{-1})^{o(g)} = \sigma^{o(g)}(g^{-1})^{o(g)} = \sigma^{o(g)}$. By Lemma 5.3.1 the element $\sigma^{o(g)}$ is not the identity. Since σg^{-1} fixes x, so does the power $(\sigma g^{-1})^{o(g)} = \sigma^{o(g)}$. This is not possible since the scalar $\sigma^{o(g)}$ is a fixed-point-free automorphism of R. Therefore, M is not transitive on Δ. Since M is a normal subgroup of H of index 2, M acts on Δ half-transitively, and has exactly two equal size orbits. □

Recall from Subsection 3.1 that Construction 3.1.3 provides a method for constructing self-complementary Cayley graphs. By Lemma 5.3.2 we can in fact generalise Construction 3.1.3 as follows.

Construction 5.3.3. Using the notation above, we define a graph as below.

(1) Let $\Delta_1, \cdots, \Delta_r$ be the orbits of H acting on $R^\#$, and let Δ_i^+ and Δ_i^- be the two orbits of M on Δ_i, where $1 \leq i \leq r$.

(2) Let $S = \cup_{i=1}^r \Delta_i^{\varepsilon_i}$, where $\varepsilon_i = +$ or $-$, and let $\Gamma = \mathrm{Cay}(R, S)$.

Lemma 5.3.4. *Let* Γ *be a Cayley graph constructed in Construction* 5.3.3. *Then* Γ *is a self-complementary metacirculant with insoluble automorphism group* $\mathsf{Aut}\Gamma \geq \mathbb{Z}_p^2{:}(\langle \sigma^2 \rangle \circ \mathrm{SL}(2,5))$, *and* σ *is a complementing isomorphism.*

Proof. We claim that Γ is self-complementary. By definition, σ interchanges Δ_i^+ and Δ_i^- where $1 \leq i \leq r$. Thus,

$$S^\sigma = \cup_{i=1}^r (\Delta_i^{\varepsilon_i})^\sigma = \cup_{i=1}^r \Delta_i^{-\varepsilon_i} = R^\# \setminus S, \text{ and}$$
$$\Gamma = \mathrm{Cay}(R, S) \cong \mathrm{Cay}(R, S^\sigma) = \mathrm{Cay}(R, R^\# \setminus S) = \overline{\Gamma}.$$

Since σ is a scalar of order divisible by 8, the power $\sigma^{o(\sigma)/2}$ maps every element $x \in R$ into the inverse x^{-1}. Hence each Δ_i is self-inverse, and so is S. So Γ is undirected, and is self-complementary with σ being a complementing isomorphism. Since R is metacyclic, the Cayley graph Γ of R is a metacirculant. Moreover, $\mathsf{Aut}\Gamma \geq R{:}M = \mathbb{Z}_p^2{:}\langle \sigma^2, \mathrm{SL}(2,5) \rangle = \mathbb{Z}_p^2{:}(\langle \sigma^2 \rangle \circ \mathrm{SL}(2,5))$ is insoluble. □

In terms of Construction 5.2.1, we have $r = 2$ and $\sigma = (\sigma_1, \sigma_2)$, where both σ_i are elements of $\mathrm{GL}(1, p)$ of order $o(\sigma)$. Moreover, since $\mathrm{SL}(2, 5)$ is irreducible on $\mathbb{Z}_p^2$, $\mathsf{Aut}\Gamma$ is primitive on the vertex set.

Remark. Note that the condition that $p \equiv \pm 1 \pmod{10}$ and $p \equiv 1 \pmod{8}$ is equivalent to $p \equiv 1$ or $9 \pmod{40}$. According to Lemma 4.2.3, by iteratively taking the lexicographic products of graphs constructed via Construction 5.3.3, we can in fact construct self-complementary metacirculants with insoluble automorphism groups, that are Cayley graphs on $\mathbb{Z}_n^2$ where $n = p_1 \dots p_t$, and p_i are distinct primes such that $p_i \equiv 1$ or $9 \pmod{40}$ for each i.

As a result of Lemma 5.3.4 we have the following:

Corollary 5.3.5. *There exist self-complementary Cayley graphs whose automorphism groups are insoluble.*

Chapter 6

The pq-Case

6.1 Overview and Main Results

The problem of characterising self-complementary vertex-transitive graphs of order pq with p, q being primes has received attention in the literature. For instance, self-complementary vertex-transitive graphs of prime order are well understood (see [4]); and back to 1997, Koolen [26] used combinatorial techniques to show that there are no self-complementary vertex-transitive graphs of order $3p$. In 1979, Zelinka [55] conjectured that if there is a self-complementary vertex-transitive graph of order pq with p, q distinct primes then both p, q are congruent to 1 modulo 4. This conjecture was verified in [27]; and later, Muzychuck [43] found a much stronger result. However, the structural description of these graphs was left open until [33] published as a partial result of this PhD project.

In this chapter, we present our characterisation of self-complementary vertex-transitive graphs of order pq, with p, q being primes, not necessarily distinct.

Theorem 6.1.1. *Let Γ be a self-complementary vertex-transitive graph of order a product of two primes. Then Γ is one of the following:*

(i) *a lexicographic product of two self-complementary vertex-transitive graphs,*

(ii) *a normal Cayley graph of an abelian group.*

A *circulant* is a graph Γ such that $\mathsf{Aut}\Gamma$ contains a cyclic subgroup which is transitive on the vertices. Circulants are vertex-transitive graphs. The first family of self-complementary vertex-transitive graphs was constructed as circulants by Sachs in 1962, and later, Zelinka (1979), Mathon (1985, 1988), Rao (1985), Suprunenko (1985), Liskovets-Poschel (2000) and Jajcay-Li (2001) also studied self-complementary circulants. A consequence of Theorem 6.1.1 is the following.

Corollary 6.1.2. *Self-complementary vertex-transitive graphs of order a product of two distinct primes are circulants.*

We make some remarks on Theorem 6.1.1. By the characterisation of Theorem 6.1.1, we can construct all such graphs: if Γ is a lexicographic product, the self-complementary vertex-transitive graphs of prime order are all well characterised, see [4]; if Γ is a normal Cayley graphs, it can be easily constructed by the definite group, see Section 3.1.

Notations. In the remainder of this chapter, we shall use the following notations. Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph of order pq with p, q prime. Let $G = \mathsf{Aut}\Gamma$, let σ be a complementing isomorphism between Γ and $\overline{\Gamma}$, and let $X = \langle G, \sigma\rangle$. Then $\sigma^2 \in G$, $X = G.\mathbb{Z}_2$. We choose σ such that $o(\sigma) = 2^f$ where $f \geq 2$. Since G is vertex-transitive, without loss of generality, we assume that σ fixes a vertex $v \in V$, and so $X_v = \langle G_v, \sigma\rangle$.

6.2 The Primitive Case

We first consider the vertex-primitive case.

Lemma 6.2.1. *Assume that X is primitive on the vertex set V. Then $p = q$, and X is affine of degree p^2. Moreover, the vertex stabiliser X_v satisfies one of the following:*

(i) $X_v \leq \mathrm{GL}(1,p) \wr \mathrm{S}_2$, *and* $X_v \not\leq \mathrm{GL}(1,p) \times \mathrm{GL}(1,p)$;

(ii) $X_v \leq \Gamma\mathrm{L}(1,p^2)$, *and* $(|X_v|, p+1) > 2$;

(iii) $\mathrm{Q}_8 \leq X_v \leq \mathbb{Z}_{p-1} \circ \mathrm{GL}(2,3)$;

(iv) $\mathrm{SL}(2,5) < X_v \leq \mathbb{Z}_{p-1} \circ \mathrm{SL}(2,5)$, *where $p = 5$ or $p \equiv \pm 1 \pmod{10}$.*

Proof. By Theorem 2.11.4, the group X is affine, or in product action with the socle $\mathrm{PSL}(2,r^2)^\ell$, where r is a power of an odd prime, and $\ell \geq 2$. If X is in product action, then $|V| = (\frac{1}{2}r^2(r^2+1))^\ell$, which is not a product of two primes, a contradiction. So X is affine of degree $|V| = p^2$, and $p = q \geq 3$.

Identifying the vertex set V with a vector space $\mathbb{F}_p^2$. Then $X = \mathbb{Z}_p^2{:}X_v$ where $X_v \leq \mathrm{GL}(2,p)$ is irreducible on V. In particular, σ^2 is a fixed-point-free automorphism of $\mathbb{Z}_p^2$. Since G is transitive on V, by Theorem 2.2.2

$$|X_v : G_v| = \frac{|X_v|}{|G_v|} = \frac{|X|/|v^X|}{|G|/|v^G|} = \frac{|X|}{|G|} = |X : G| = 2.$$

Let M be a maximal subgroup of $\mathrm{GL}(2,p)$ containing X_v. Then M is one of the following (see [52, p. 417]):

(a) $\mathrm{GL}(1,p) \wr \mathrm{S}_2$;

(b) $\Gamma\mathrm{L}(1,p^2)$;

(c) $\mathbb{Z}_{p-1} \circ \mathrm{GL}(2,3)$;

(d) $\mathbb{Z}_{p-1} \circ \mathrm{SL}(2,5)$ with $p = 5$ or $p \equiv \pm 1 \pmod 5$.

If $M = \mathrm{GL}(1,p) \wr \mathrm{S}_2$, since X_v is irreducible, $X_v \not\leq \mathrm{GL}(1,p) \times \mathrm{GL}(1,p)$, as in part (i). For the case $M = \Gamma\mathrm{L}(1,p^2)$, if $(|X_v|, p+1) \leq 2$, then X_v is conjugate to a subgroup of $\mathrm{GL}(1,p) \wr \mathrm{S}_2$, and so part (i) or (ii) is satisfied. For the case $M = \mathbb{Z}_{p-1} \circ \mathrm{GL}(2,3)$, if X_v does not contain Q_8, then part (i) or (ii) is satisfied, and if $X_v \geq \mathrm{Q}_8$, then part (iii) is satisfied. Finally, for $M = \mathbb{Z}_{p-1} \circ \mathrm{SL}(2,5)$, we may assume that X_v is not a subgroup of $\mathrm{GL}(1,p) \wr \mathrm{S}_2$, $\Gamma\mathrm{L}(1,p^2)$ and $\mathbb{Z}_{p-1} \circ \mathrm{GL}(2,3)$. Thus, X_v is insoluble and contains $\mathrm{SL}(2,5)$, and as X_v has a subgroup G_v of index 2, we further have $X_v > \mathrm{SL}(2,5)$, as in part (iv). □

6.3 The Imprimitive Case

In this subsection, we consider the case when X is imprimitive on V. Let $\mathcal{B}$ be a non-trivial block system, and let $B \in \mathcal{B}$ be a block. Without loss of generality, we assume $|\mathcal{B}| = q$. Then $|B| = p$. Denote $[B]_\Gamma$ the *induced subgraph* of Γ on B, namely, the graph whose vertex set is B and the edge set consists of all edges of Γ which lie inside B. The *quotient graph* $\Gamma_{\mathcal{B}}$ of Γ is the graph with vertex set $\mathcal{B}$ such that two vertices $B, C \in \mathcal{B}$ are adjacent if and only if some $u \in B$ and some $v \in C$ are adjacent in Γ.

The following lemma characterises X_B^B and $X^{\mathcal{B}}$.

Lemma 6.3.1. *Using the notation defined above, we have* $\mathbb{Z}_p \lhd X_B^B \leq \mathrm{AGL}(1,p)$, *and* $\mathbb{Z}_q \lhd X^{\mathcal{B}} \leq \mathrm{AGL}(1,q)$.

Proof. By Theorem 2.11.5 (i) the induced subgraph $[B]_\Gamma$ on B is self-complementary. Thus, G_B^B is not 2-transitive. Since $|B| = p$, it follows from Theorem 2.2.7 that $\mathbb{Z}_p \lhd X_B^B \leq \mathrm{AGL}(1,p)$.

Similarly, by Theorem 2.11.5 (ii), $G^{\mathcal{B}}$ is not 2-transitive. Hence we conclude that $\mathbb{Z}_q \lhd X^{\mathcal{B}} \leq \mathrm{AGL}(1,q)$. □

Lemma 6.3.2. *The action of* X *on* $\mathcal{B}$ *is unfaithful.*

Proof. To the contrary, suppose that $X \cong X^{\mathcal{B}}$ is faithful. By Lemma 6.3.1, we have $X \cong X^{\mathcal{B}} \leq \mathrm{AGL}(1,q) \cong \mathbb{Z}_q{:}\mathbb{Z}_{q-1}$, and all the q'-subgroups of X are cyclic by Theorem 2.4.4. Note that the stabiliser G_v is core-free in G, by Theorem 2.11.7 (ii), σ fixes no double cosets $G_v g G_v$, that is,

$$G_v g^\sigma G_v \neq G_v g G_v \quad \text{for each } g \in G \setminus G_v.$$

Since $|X : X_v| = pq$, so $G_v < X_v$ is properly contained in a Hall q'-subgroup $X_{q'}$ by Theorem 2.4.4, that is, $G_v < X_{q'} \leq \mathbb{Z}_{q-1}$. Note that $\sigma \in X_v < X_{q'}$, so σ centralises all elements in $X_{q'}$. In particular, we have

$$G_v h^\sigma G_v = G_v h G_v \quad \text{for all } h \in (X_{q'} \cap G) \setminus G_v,$$

which is not possible. Therefore, X is not faithful on $\mathcal{B}$. □

Let $K = X_{(\mathcal{B})}$ be the kernel of X acting on $\mathcal{B}$. Then $1 \neq K \lhd X$ by Lemma 6.3.2, and $1 \neq K^B \lhd X^B_B$ for some $B \in \mathcal{B}$. Thus, $K^B = \mathbb{Z}_p{:}\mathbb{Z}_r$ for some r dividing $p-1$ by Theorem 2.2.7. For two blocks $B, C \in \mathcal{B}$, we denote by $[B, C]$ the subgraph of Γ with vertex set $B \cup C$ and edge set consisting of all the edges of Γ between B and C.

Lemma 6.3.3. *If $p^2 \,\big|\, |K|$, then $\Gamma = \Gamma_1[\Gamma_2]$, where Γ_1 and Γ_2 are self-complementary circulants of order q and p, respectively.*

Proof. Let $B_1 = B$ and let $B_2 \in \mathcal{B}$ be distinct from B. Consider the subgraph $[B_1, B_2]$. Since X is transitive on the q blocks and q is a prime, relabelling if necessary, we assume $\mathcal{B} = \{B_1, B_2, \ldots, B_q\}$ such that $[B_i, B_{i+1}] \cong [B_1, B_2]$ for all $i \in \{1, \cdots, q-1\}$. Let P be a Sylow p-subgroup of K, and let $P_{(B)}$ be the kernel of P acting on B. Then $P/P_{(B)} \cong P^B \cong \mathbb{Z}_p$, and $P_{(B)} \neq 1$. Hence $P_{(B)}$ acts non-trivially on some B_k with $k \neq 1$. Without loss of generality, assume that k is the smallest integer with this property. Then $P_{(B)} \leq P_{(B_{k-1})}$ is transitive on B_k as $|B_k| = p$. Notice that K is transitive on B_{k-1}. If $[B_1, B_2]$ is non-empty, then so is $[B_{k-1}, B_k]$, and we have $[B_1, B_2] \cong [B_{k-1}, B_k] = \mathbf{K}_{p,p}$. Therefore, for any two blocks $B, C \in \mathcal{B}$, either $[B, C]$ is empty, or $[B, C] = \mathbf{K}_{p,p}$. Let $E' = E \setminus (\cup_{i=1}^{q} B_i \times B_i)$. Then $\Gamma' = (V, E') \cong \Gamma_{\mathcal{B}}[\overline{\mathbf{K}_p}]$.

Let $\Gamma_1 = \Gamma_{\mathcal{B}}$, and $\Gamma_2 = [B]_\Gamma$. Then $\Gamma = \Gamma_1[\Gamma_2]$. Let v be a vertex in B. By Theorem 2.11.5 the induced subgraph $[B]_\Gamma = \Gamma_2$ is self-complementary, and v has valency $\frac{p-1}{2}$ in $[B]_\Gamma$. Notice that the vertex v has valency $\frac{p^2-1}{2}$, so v is adjacent to exactly $\left(\frac{p^2-1}{2} - \frac{p-1}{2}\right)\Big/p = \frac{p-1}{2}$ blocks. Since σ preserves the block system $\mathcal{B}$ and $\Gamma_{\mathcal{B}}$ is a Cayley graph, σ induces a complementing isomorphism on $\Gamma_{\mathcal{B}}$, and so $\Gamma_1 = \Gamma_{\mathcal{B}}$ is self-complementary. Thus, we complete the proof. □

Lemma 6.3.4. *Assume that p^2 does not divide $|K|$. Then $X = R{:}X_v$, where R is abelian of order pq, and regular on V.*

Proof. Suppose that $1 \neq K_{(B)} \lhd K$. Then there exists $B' \in \mathcal{B}$ such that $K_{(B)}$ acts on B' transitively, and hence $p \,\big|\, |K_{(B)}|$ by Theorem 2.2.2. It yields that p^2 divides $|K|$, which is a contradiction. So $K \cong K^B = \mathbb{Z}_p{:}\mathbb{Z}_r$ for some r dividing $p-1$. Now $X^{\mathcal{B}} = \mathbb{Z}_q{:}\mathbb{Z}_s$ with $s \,\big|\, (q-1)$ and $s \neq 1$. Consider that

$$X = K.X^{\mathcal{B}} = (\mathbb{Z}_p{:}\mathbb{Z}_r).(\mathbb{Z}_q{:}\mathbb{Z}_s).$$

In the following we shall show that X contains a normal subgroup R of order pq. Let P be a Sylow p-subgroup of K. Since $P \lhd K$, it follows from Theorem 2.4.2 (ii) that P is characteristic in K, and so P is normal in X by Lemma 2.1.2. Let $\overline{\mathbf{C}} = \mathbf{C}_X(P)/P$, $\overline{K} = K/P$, and let $\overline{X} = X/P$. Then $\mathbf{C}_X(P) \lhd X$, and $\overline{\mathbf{C}} \lhd \overline{X} = \mathbb{Z}_r.(\mathbb{Z}_q{:}\mathbb{Z}_s)$. Note that $X/\mathbf{C}_X(P) \leq \mathsf{Aut}(P) = \mathbb{Z}_{p-1}$ is abelian, so $\mathbf{C}_X(P) \geq X' > P$, and $\overline{\mathbf{C}} \neq 1$. Also note that $\mathbf{C}_X(P) \cap K = P$, we have $\overline{\mathbf{C}} \cap \overline{K} = 1$, and

$$\overline{\mathbf{C}} = \overline{\mathbf{C}}\big/\big(\overline{\mathbf{C}} \cap \overline{K}\big) \cong \overline{\mathbf{C}K}\big/\overline{K} \lhd \overline{X}\big/\overline{K} = \mathbb{Z}_q{:}\mathbb{Z}_s.$$

Hence $\overline{\mathbf{C}} = \mathbb{Z}_q{:}\mathbb{Z}_t$ for some t dividing s, and $\mathbf{C}_X(P) = \mathbb{Z}_p.(\mathbb{Z}_q{:}\mathbb{Z}_t)$. Let $\mathbf{C}'$ be the derived group of $\mathbf{C}_X(P)$. If $t = 1$, then $R = \mathbf{C}_X(P)$. Thus, we assume that $t \neq 1$. If $\mathbf{C}' > P$, then $\mathbf{C}'/P \lhd \mathbf{C}_X(P)/P = \mathbb{Z}_q{:}\mathbb{Z}_t$, and $\mathbf{C}' = \mathbb{Z}_p.\mathbb{Z}_q$. Since $\mathbf{C}'$ is characteristic in $\mathbf{C}_X(P)$, so $R = \mathbf{C}'$ is normal in X. Finally, we assume that $\mathbf{C}' \cap P = 1$. Then $P \times \mathbf{C}' \lhd \mathbf{C}_X(P)$, and $\mathbf{C}' \lhd \overline{\mathbf{C}} = \mathbb{Z}_q{:}\mathbb{Z}_t$. Let Q be the unique Sylow q-subgroup of $\mathbf{C}'$. Then Q is characteristic in $\mathbf{C}_X(P)$, and so $Q \lhd X$. Thus, $R = P \times Q$ is normal in X. Moreover, in any of these cases $R \leq \mathbf{C}_X(P)$, so R is abelian, and $X = R{:}X_v$. □

6.4 Proofs of the Main Results

Proof of Theorem 6.1.1. Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph of order pq with p, q prime. Let $G = \mathsf{Aut}\Gamma$, and let σ be a complementing isomorphism between Γ and $\overline{\Gamma}$. Let $X = \langle G, \sigma \rangle$.

If X is primitive on the vertex set V, then by Lemma 6.2.1, Γ is a normal Cayley graph of $\mathbb{Z}_p^2$.

If X is imprimitive on V, then by Lemmas 6.3.3 and 6.3.4 the statement of Theorem 6.1.1 holds. □

The proof of Corollary 6.1.2 follows from the lemma below.

Lemma 6.4.1. *If $p \neq q$, then*

(i) *either $\Gamma = \Gamma_1[\Gamma_2]$, where Γ_1 and Γ_2 are self-complementary circulants of order q and p, respectively; or*

(ii) $\mathsf{Aut}\Gamma = \mathbb{Z}_{pq}{:}H$, *where* $H < \mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$.

In particular, Γ is a circulant.

Proof. Since $p \neq q$, by Lemma 6.2.1 we have X is imprimitive. Then by Lemmas 6.3.3 and 6.3.4, either part (i) or part (ii) is satisfied. □

Chapter 7

Self-Complementary Metacirculants

7.1 Overview and Main Results

Recall that a group R is *metacyclic* if R has a normal subgroup N such that both N and R/N are cyclic; and a graph $\Gamma = (V, E)$ is said to be a *metacirculant* if $\mathsf{Aut}\Gamma$ contains a metacyclic subgroup R which is transitive on V. To emphasise the metacyclic group, we sometimes call Γ a *metacirculant of* R. We remark that a metacirculant defined in this way is not necessarily a metacirculant in the definition of Alspach-Parsons in [5], refer to [35].

In this chapter, we study metacirculants that are self-complementary, which will be called *self-complementary metacirculants*.

A special subclass of metacirculants consists of *circulants*, whose automorphism group contains a transitive cyclic subgroup. Self-complementary circulants have been studied for a long time, and have been taken as good models for studying other combinatorial objects, such as Ramsey numbers and communication networks. The first family of self-complementary circulants was constructed by Sachs in 1962, and since then self-complementary circulants have been widely studied, see [14, 42, 46, 50, 51, 55] for the work till 1980s. In 1990s, the orders of self-complementary circulants were determined, see [4] for Alspach-Morris-Vilfred's proof, and [15] for an alternative approach. Some special families of self-complementary circulants are constructed in [25, 38, 45]. More recently, it was proved that the automorphism groups of self-complementary circulants are soluble by Li and Praeger in [32], and self-complementary circulants of prime-power order are characterised in [36].

Recall that for a group G and subgroups $K \lhd H \leq G$, the quotient group H/K is called a *section* of G. The main result of this chapter gives a characterisation of the automorphism groups of self-complementary metacirculants.

Theorem 7.1.1. *Let Γ be a self-complementary metacirculant of R. Then either $\mathsf{Aut}\Gamma$ is soluble, or the following hold:*

(i) *the only insoluble composition factor of $\mathsf{Aut}\Gamma$ is the alternating group A_5; and*

(ii) *$\mathsf{Aut}\Gamma$ has a section that is of the form $\mathbb{Z}_p^2{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$ such that $\mathbb{Z}_p^2$ is a*

section of R, where p is a prime number and $p \equiv 1$ or $9 \pmod{40}$, and ℓ divides $p-1$ and is divisible by 4.

Remark. Recall from Section 5.3 that we have constructed an example of self-complementary metacirculant as Theorem 7.1.1, where A_5 is the only insoluble composition factor of $\mathsf{Aut}\Gamma$. Furthermore, we shall generalise this example in Section 7.2 such that the insoluble factor A_5 can appear multiple times, see Lemma 7.2.2.

Li and Praeger in [32] proved that the automorphism group of a self-complementary circulant is soluble. A metacirculant Γ is called a *Sylow-circulant* if $\mathsf{Aut}\Gamma$ has a transitive metacyclic subgroup of which all Sylow subgroups are cyclic. By Theorem 7.1.1, if $\mathsf{Aut}\Gamma$ is insoluble, then a Sylow p-subgroup of $\mathsf{Aut}\Gamma$ is not cyclic. Therefore, a consequence of Theorem 7.1.1 is the following corollary, which extends the result for circulants.

Corollary 7.1.2. *If Γ is a self-complementary Sylow-circulant, then $\mathsf{Aut}\Gamma$ is soluble. In particular, if Γ is a self-complementary metacirculant of square free order, then $\mathsf{Aut}\Gamma$ is soluble.*

We end this section with a conjecture.

Conjecture. Self-complementary metacirculants are Cayley graphs.

7.2 Examples with Insoluble Automorphism Groups

Recall from Section 5.3 that we constructed an example of self-complementary metacirculants which have insoluble automorphism groups. We next give another construction of self-complementary metacirculants of which the automorphism groups contain a section $\mathrm{A}_5 \times \cdots \times \mathrm{A}_5$.

Let $p_1, \cdots, p_t$ be distinct primes such that $p_i \equiv 1$ or $9 \pmod{40}$ for each $i \in \{1, \cdots, t\}$. Let $R_i = \mathbb{Z}_{p_i}^2$, and let $L_i < \mathsf{Aut}(R_i) = \mathrm{GL}(2, p_i)$ be isomorphic to $\mathrm{SL}(2,5)$. Let $\sigma_i \in \mathbf{Z}(\mathsf{Aut}(R_i))$ have order divisible by 8. Let $R = R_1 \times \cdots \times R_t$, $L = L_1 \times \cdots \times L_t$, and $\sigma = (\sigma_1, \ldots, \sigma_t) \in \mathsf{Aut}(R)$. Let $H = R{:}(\langle\sigma\rangle \circ L)$ and $M = R{:}(\langle\sigma^2\rangle \circ L)$.

Lemma 7.2.1. *The subgroup M divides every H-orbit on $R^{\#}$ into two parts of equal size.*

Proof. Let Δ be an H-orbit on $R^{\#}$, and let $(x_1, \ldots, x_t) \in \Delta$. Suppose that there is an element $g \in M$ such that $(x_1, \ldots, x_t)^g = (x_1, \ldots, x_t)^\sigma$. Then $(x_1, \ldots, x_t)^{\sigma g^{-1}} = (x_1, \ldots, x_t)$. As $\sigma g^{-1} = g^{-1}\sigma$, we have $(\sigma g^{-1})^{o(g)} = \sigma^{o(g)}(g^{-1})^{o(g)} = \sigma^{o(g)}$. Noticing that no element of L has order divisible by 8, we know $\sigma^{o(g)} \neq 1$. Since σg^{-1} fixes $(x_1, \ldots, x_t)$, so does the power $\sigma^{o(g)}$. Now some $x_i \neq 1$, and $x_i^{\sigma_i^{o(g)}} = x_i$, which contradicts that the scalar $\sigma_i^{o(g)}$ is a fixed-point-free automorphism of R_i. So M is intransitive on Δ, and has exactly two orbits of equal size. □

Thus applying Construction 5.3.3 with H, M defined before Lemma 7.2.1 produces examples of self-complementary metacirculants of which the automorphism groups have a section A_5^t for any positive integer t.

Lemma 7.2.2. *Let $p_1, \cdots, p_t$ be distinct primes such that $p_i \equiv 1$ or $9 \pmod{40}$ for every $i \in \{1, \cdots, t\}$. Then there exist self-complementary metacirculants Γ of order $p_1^2 \cdots p_t^2$ such that $\mathsf{Aut}\Gamma \geq \mathbb{Z}_{p_1 \cdots p_t}^2{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5)^t)$, where $\ell \,\big|\, (p_i - 1)$ for each i and $8 \,\big|\, \ell$.*

7.3 The Primitive Case

Notations. In the remainder of this chapter we shall use the following notations. Let $\Gamma = (V, E)$ be a self-complementary metacirculant of a metacyclic group R. Due to the result of [32], we suppose that R is not cyclic. Let $G = \mathsf{Aut}\Gamma$, and let σ be a complementing isomorphism of Γ. Let $X = \langle G, \sigma \rangle$. Then $\sigma^2 \in G$, and $X = G.\mathbb{Z}_2$. Let n be a positive integer, and let p be a prime factor of n. Recall that n_p denotes the highest power of p that divides n, so that p and n/n_p are coprime.

We consider first the vertex-primitive case. Suppose that X is primitive on V. Then by Theorem 2.11.4 either X is affine, or the socle $\mathsf{soc}(X) = \mathrm{PSL}(2, q^2)^\ell$ and $|V| = (\frac{1}{2}q^2(q^2+1))^\ell$ where q is odd and $\ell \geq 2$. The latter case is ruled out by the following lemma.

Lemma 7.3.1. *The group X is affine.*

Proof. Suppose that X has socle $N = \mathrm{PSL}(2, q^2)^\ell$, and $|V| = (\frac{1}{2}q^2(q^2+1))^\ell$. Since R is transitive on V, it follows that $q^{2\ell}$ divides $|R|$. Let $q = p^f$ with p prime and $f \geq 1$. Since R is metacyclic, R contains an element x of order $q^\ell = p^{f\ell}$. Let K be the largest subgroup of X which normalises each direct factor of N. Then $N \lhd K \leq \mathrm{P\Gamma L}(2, q^2)^\ell$. Note that $\mathrm{P\Gamma L}(2, q^2) = \mathrm{PGL}(2, q^2){:}\mathbb{Z}_{2f}$, and $\mathrm{PGL}(2, q^2)$ has a Sylow p-subgroup $\mathbb{Z}_p^{2f}$. Hence a p-element of K has order at most pf_p. Thus

$$X/K \geq \langle x \rangle K/K \cong \langle x \rangle / (\langle x \rangle \cap K) \,,$$

and so $X/K \leq S_\ell$ contains an element of order $p^{f\ell-1}/f_p$. However, $p^{f\ell-1}/f_p$ does not divide $|\mathrm{S}_\ell| = \ell!$, which is a contradiction. □

We now show that only affine groups of dimension 1 or 2 can appear.

Lemma 7.3.2. *The primitive group X is affine of dimension 1 or 2.*

Proof. By Lemma 7.3.1 the socle $N = \mathsf{soc}(X) = \mathbb{Z}_p^d$, where p is a prime and $d \geq 1$. Then $X \leq \mathrm{AGL}(d, p)$, and p^d divides $|R|$. Since R is metacyclic, there exists an element $g \in R$ of order divisible by $p^{\lceil \frac{d}{2} \rceil}$. Recall from Lemma 2.6.4 that $\mathrm{AGL}(d, p) < \mathrm{GL}(d+1, p)$, and both $\mathrm{GL}(d+1, p)$ and $\mathrm{AGL}(d, p)$ have isomorphic Sylow p-subgroups. Hence, by Lemma 2.6.2, the largest order p^e of the p-elements

of $\mathrm{AGL}(d,p)$ is such that $p^e \geq d+1 > p^{e-1}$. Thus $p^{\lceil \frac{d}{2} \rceil - 1} \leq p^{e-1} < d+1$. Noticing that $p \geq 3$, this implies that $d \leq 4$.

Suppose that $d = 3$. Then $p^{\lceil \frac{d}{2} \rceil} = p^2 \leq p^e$, and $p \leq p^{e-1} < d+1 = 4$. Thus $p = 3$, and $|V| = 3^3 \not\equiv 1 \pmod 4$, which is not possible by Theorem 2.11.2.

Suppose that $d = 4$. Then $\lceil \frac{d}{2} \rceil = 2$, and it follows that $p \leq p^{e-1} < d+1 = 5$. Thus $p = 3$, and $|V| = 3^4$. By Lemma 2.4.3, we may assume that R is a 3-group. Note that $\mathrm{AGL}(4,3) < \mathrm{GL}(5,3)$, by Lemma 2.6.2 the largest order of the 3-elements of $\mathrm{GL}(5,3)$ is 9. Thus the metacyclic group $R = \mathbb{Z}_9.\mathbb{Z}_9$. However, checking the subgroups of $\mathrm{GL}(5,3)$ in GAP (see Appendix A) leads to the conclusion that $\mathrm{GL}(5,3)$ does not have a metacyclic group $\mathbb{Z}_9.\mathbb{Z}_9$.

We therefore conclude that $d = 1$ or 2, as claimed in the lemma. □

Next, we determine the insoluble case.

Lemma 7.3.3. *Assume that X is primitive and insoluble. Then we have*

$$X = \mathbb{Z}_p^2{:}\,(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5)), \quad \text{and } G = \mathbb{Z}_p^2{:}(\mathbb{Z}_{\ell/2} \circ \mathrm{SL}(2,5)),$$

where $p \equiv 1$ or $9 \pmod{40}$, and ℓ divides $p-1$ and is divisible by 8.

Proof. Since X is primitive and insoluble, by Lemma 7.3.2, we have $|V| = p^2$, and $X \leq \mathrm{AGL}(2,p)$, and the stabiliser X_v is an irreducible subgroup of $\mathrm{GL}(2,p)$. Now $\mathsf{soc}(X) = \mathbb{Z}_p^2$ is regular on V, so $R = \mathsf{soc}(X)$, and Γ is a Cayley graph of R, say

$$\Gamma = \mathrm{Cay}(R, S).$$

Notice that G has index 2 in X and is not 2-transitive on V, so G_v does not contain $\mathrm{SL}(2,p)$. Inspecting the subgroups of $\mathrm{SL}(2,p)$ listed in [52, Theorem 6.17], we conclude that X_v contains a subgroup isomorphic to $\mathrm{SL}(2,5)$ with $p = 5$ or $p \equiv \pm 1 \pmod 5$. Noting that $\mathbb{Z}_{p-1} \circ \mathrm{SL}(2,5)$ is maximal in $\mathbb{Z}_{p-1} \circ \mathrm{SL}(2,p)$ and there is no element of $\mathrm{GL}(2,p) \setminus (\mathbb{Z}_{p-1} \circ \mathrm{SL}(2,5))$ which normalises $\mathrm{SL}(2,5)$, we have that

$$X_v = \langle z \rangle \circ \mathrm{SL}(2,5) = \mathbb{Z}_\ell \circ \mathrm{SL}(2,5),$$

where z is a scalar of order ℓ dividing $p-1$. Since G is transitive on V, by Theorem 2.2.2 the index

$$|X_v : G_v| = \frac{|X|/|v^X|}{|G|/|v^G|} = \frac{|X|}{|G|} = |X : G| = 2.$$

We may assume $\sigma \in X_v$. As $\mathrm{SL}(2,5)$ has no subgroup of index 2, $\sigma \notin \mathrm{SL}(2,5)$. Since σ normalises G_v, σ normalises $\mathrm{SL}(2,5)$, and we may choose $\sigma \in \langle z \rangle$. Then $\sigma \notin \langle z^2 \rangle$, and $G_v = \langle z^2 \rangle \circ \mathrm{SL}(2,5)$. By Lemma 2.11.3, the order $o(\sigma)$ is divisible by 4.

Suppose that ℓ is not divisible by 8. Then since $\sigma \in \mathbb{Z}_\ell$, σ is of order $4m$ with m odd, and

$$X_v = \langle \sigma^4 \rangle \times (\mathbb{Z}_4 \circ \mathrm{SL}(2,5)) = \mathbb{Z}_m \times (\mathbb{Z}_4 \circ \mathrm{SL}(2,5)),$$

and $G_v = \mathbb{Z}_m \times \mathrm{SL}(2,5)$. Let $\tau = \sigma^m \in \langle z \rangle$. Then τ is of order 4, and $X_v = \langle \tau \rangle \circ G_v$. For every element $x \in R$, we have $x^\tau = x^j$ for some integer j which has order 4 in the multiplicative group $\mathbb{F}_p^*$ of $\mathbb{F}_p$.

Let $y \in G_v$ be of order 4. Since 4 divides $p-1$, the group $\langle y \rangle$ is reducible on $R = \mathsf{soc}(X)$. Thus y normalises a cyclic subgroup $\langle w \rangle \cong \mathbb{Z}_p$, where $w \in R$, and y induces an automorphism of $\langle w \rangle$ of order 4. So $w^y = w^k$, for some integer k which has order 4 in $\mathbb{F}_p^*$. Since $\mathbb{F}_p^*$ has a unique subgroup of order 4, $k = j$ or j^{-1} in $\mathbb{F}_p^*$. Thus $w^\tau = w^y$ or $w^{y^{-1}}$, respectively. Without loss of generality, assume that $w \in S$. Since $y \in G$, both w^y and $w^{y^{-1}}$ belong to S. However, $w^\tau \in S^\tau = R^\# \setminus S$, which is a contradiction. Hence 8 divides $o(\sigma)$, and $p \equiv 1 \pmod 8$.

Finally, since $p = 5$ or $p \equiv \pm 1 \pmod 5$, it follows that $p \equiv 1$ or $9 \pmod{40}$. The proof is completed. □

7.4 Proof of Theorem 7.1.1

In order to prove Theorem 7.1.1, we assume that X is insoluble. We complete our proof by induction on the order $|V|$.

If X is primitive on V, then by Lemmas 7.3.2 and 7.3.3, the statement of Theorem 7.1.1 is true. We thus assume that X is imprimitive on V, and further assume that Theorem 7.1.1 holds for any self-complementary metacirculants of order properly dividing $|V|$.

Let $\mathcal{B}$ be a block system of V under the action of X, and let B be a block of $\mathcal{B}$. Let $[B]_\Gamma$ denote the induced subgraph of Γ on B. Recall from Theorem 2.11.5 that $G_B^B \le \mathsf{Aut}[B]_\Gamma$; and there exists a self-complementary graph Σ such that $G^{\mathcal{B}} \le \mathsf{Aut}\Sigma$.

Let $K = X_{(\mathcal{B})}$ be the kernel of X acting on $\mathcal{B}$. Then, as $|\mathcal{B}|$ properly divides $|V|$, by our assumption, Theorem 7.1.1 holds for $X^{\mathcal{B}}$, that is, if $X^{\mathcal{B}}$ is insoluble, then A_5 is the only insoluble composition factor of $X^{\mathcal{B}}$, and $X^{\mathcal{B}}$ has a section which has the form

$$\mathbb{Z}_q^2{:}(\mathbb{Z}_m \circ \mathrm{SL}(2,5)),$$

where q is a prime, $8 \,\big|\, m$ and $m \,\big|\, (q-1)$, and $\mathbb{Z}_q^2$ is a section of $R^{\mathcal{B}}$.

If K is soluble, then $X = K.X^{\mathcal{B}}$ satisfies Theorem 7.1.1. We thus assume that K is insoluble. Then K^B is insoluble, and so is X_B^B.

To complete the proof, we may further assume that $\mathcal{B}$ is a minimal block system of X, that is, for a block $B \in \mathcal{B}$, the induced action X_B^B is primitive. By Lemmas 7.3.2 and 7.3.3, we have X_B^B is affine of degree p or p^2 with p prime, and as X_B^B is insoluble,

$$X_B^B = \mathbb{Z}_p^2{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5)),$$

and $R_B^B = \mathbb{Z}_p^2$, where $p \equiv 1$ or $9 \pmod{40}$ is a prime, as in part (ii) of Theorem 7.1.1.

Since $K \lhd X_B$ is insoluble, $K^B = \mathbb{Z}_p^2{:}(\mathbb{Z}_{\ell'} \circ \mathrm{SL}(2,5))$, where $\ell' \,\big|\, \ell$. Furthermore, by Lemma 2.10.2 we have $K \le K^{B_1} \times \cdots \times K^{B_t}$ where $\mathcal{B} = \{B_1, \ldots, B_t\}$, so A_5 is the only insoluble composition factor of K. Finally, since $X = K.X^{\mathcal{B}}$ is an extension of K by $X^{\mathcal{B}}$, every composition factor of X is a composition factor of K or $X^{\mathcal{B}}$. Therefore, A_5 is the only insoluble composition factor of X. This completes the proof of our theorem. □

Chapter 8

The p^3-Case

8.1 Overview and Main Results

It is known [41] that vertex-transitive graphs of prime-cube order are all Cayley graphs. The main purpose of this chapter is to characterise self-complementary vertex-transitive graphs of order p^3, where p is a prime.

In Section 8.2 and Section 8.3 we derive the following result.

Theorem 8.1.1. *For each group R of order p^3 with p prime, there exist self-complementary Cayley graphs of R if and only if $p \equiv 1 \pmod 4$.*

Remark. There are five non-isomorphic groups of p^3. Four of them have normal complementing isomorphisms, and the fifth one (non-abelian metacyclic) does not have a normal complementing isomorphism.

The next theorem gives a characterisation of self-complementary vertex-transitive graphs of prime-cube order.

Theorem 8.1.2. *Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph of order p^3, with p prime. Then Γ is a Cayley graph, p is congruent to 1 modulo 4, and one of the following holds:*

(i) *Γ is a normal Cayley graph of a group,*

(ii) *Γ is a lexicographic of two self-complementary vertex-transitive graphs, one of which is of order p and the other is of order p^2,*

(iii) *$\mathsf{Aut}\Gamma$ is soluble, and V has block systems of size p and p^2.*

There are graphs of order p^3 which are self-complementary and vertex-transitive and have insoluble automorphism groups, see Lemma 8.4.2 and 8.4.3. Theorem 8.1.2 gives a well-characterisation for these graphs.

8.2 Normal Complementing Isomorphisms

In this section, we study further normal complementing isomorphisms, and apply them to construct various examples of self-complementary Cayley graphs.

It is worth mentioning that Construction 3.1.3 leads to the following lemma.

Lemma 8.2.1. *Let R be a group which has an automorphism σ of order a power of 2 such that σ^2 is fixed-point-free. Then there exist Cayley graphs of R which are self-complementary with σ being a complementing isomorphism.*

It is known that there are five types of groups of order p^3 with p prime:

$$\mathbb{Z}_p^3,\ \mathbb{Z}_p \times \mathbb{Z}_{p^2},\ \mathbb{Z}_{p^3},\ \mathbb{Z}_p^2{:}\mathbb{Z}_p,\ \mathbb{Z}_{p^2}{:}\mathbb{Z}_p.$$

The first three are abelian, and the other two are non-abelian. The last group $\mathbb{Z}_{p^2}{:}\mathbb{Z}_p$ is metacyclic, and has no fixed-point-free automorphism by Theorem 3.2.3. Thus there is no Cayley graph for this group which is self-complementary associated with a normal complementing isomorphism. In the rest of this section, we shall show that each of the other four groups has fixed-point-free automorphisms of 2-power order.

8.2.1 The abelian groups

If $R = \mathbb{Z}_{p^3}$ is cyclic, then $\mathsf{Aut}(R) = \mathbb{Z}_{p^2(p-1)}$, and each automorphism of order coprime to p is fixed-point-free. This provides normal complementing isomorphisms for self-complementary circulants (Cayley graphs of cyclic groups).

Recall Lemma 3.2.4 that fixed-point-free automorphisms of groups A and B give rise to a fixed-point-free automorphism of the direct product $A \times B$. The following is an immediate consequence of this lemma.

Corollary 8.2.2. *Let $\sigma_1, \sigma_2, \sigma_3$ be fixed-point-free automorphisms of $\mathbb{Z}_p$, and τ be a fixed-point-free automorphism of $\mathbb{Z}_{p^2}$. Then $(\sigma_1, \sigma_2, \sigma_3)$ is a fixed-point-free automorphism of $\mathbb{Z}_p^3$, and (σ_1, τ) is a fixed-point-free automorphism of $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$.*

8.2.2 The non-abelian non-metacyclic groups

Let $R = \mathbb{Z}_p^2{:}\mathbb{Z}_p$ be non-abelian. Then R is of exponent p, and is often denoted by p_+^{1+2}. By Winter [54], the automorphism group

$$\mathsf{Aut}(R) = \mathbb{Z}_p^2.\mathrm{Sp}(2,p).\mathbb{Z}_{p-1} \cong \mathrm{AGL}(2,p).$$

The following lemma shows that R has fixed-point-free automorphisms of 2-power order.

Lemma 8.2.3. *The group p_+^{1+2} with $p \equiv 1 \pmod 4$ has fixed-point-free automorphisms of 2-power order, which are of order dividing the 2-part $(p-1)_2$.*

Proof. Let $R = \langle a, b, c\rangle = \langle a, c\rangle{:}\langle b\rangle \cong \mathbb{Z}_p^2{:}\mathbb{Z}_p$. Then b can be viewed as an automorphism of $\langle a, c\rangle \cong \mathbb{Z}_p^2$, and thus $b \in \mathsf{Aut}(\langle a, c\rangle) \cong \mathrm{GL}(2, p)$. Noticing that $\mathrm{GL}(2, p)$ has only one conjugacy class of subgroups of order p, $\langle b\rangle$ is embedded into a subgroup $H < \mathsf{Aut}(\langle a, c\rangle) = \mathrm{GL}(2, p)$ which is isomorphic to $\mathrm{AGL}(1, p) = \mathbb{Z}_p{:}\mathbb{Z}_{p-1}$.

Let σ be a 2-element of H of order k dividing $\frac{1}{2}(p-1)_2$. Then

$$b^\sigma = b^\lambda,$$

where $1 < \lambda \leq p-1$ such that k is the smallest positive integer satisfying that $\lambda^k \equiv 1 \pmod{p}$. Let z be a 2-element of $\mathbf{Z}(\mathsf{Aut}(\langle a, c\rangle)) = \mathbf{Z}(\mathrm{GL}(2, p)$ of order ℓ. Then $zb = bz$ and $z\sigma = \sigma z$. Then z can be viewed as an automorphism of R, and $\ell \,\big|\, (p-1)_2$. Assume that $\ell \geq 2k$, and let $\tau = z\sigma$. Then τ is an automorphism of R and fixes the subgroup $\langle a, c\rangle$. Now $\tau^k = (z\sigma)^k = z^k\sigma^k = z^k$ since $\sigma z = z\sigma$, and hence the order of τ equals the order of z which equals ℓ. Since $\ell \geq 2k$, we have that $\tau^k = z^k$ is a non-identity element of $\mathbf{Z}(\mathrm{GL}(2, p))$. Thus, for any $x \in \langle a, c\rangle$, we have

$$x^{\tau^k} = x^{z^k} = x^\mu, \quad \text{where } 1 < \mu \leq p-1.$$

In particular, τ^k fixes no non-identity element of $\langle a, c\rangle$, and so does τ.

We further claim that τ fixes no non-identity element of R. Let y be an arbitrary element of $R \setminus \langle a, c\rangle$. Then $y = xb^i$, where $x \in \langle a, c\rangle$ and $1 \leq i \leq p-1$, and

$$(xb^i)^\tau = (xb^i)^{z\sigma} = x^\tau (b^i)^\sigma = x^\tau b^{i\lambda}.$$

Suppose that $(xb^i)^\tau = y^\tau = y = xb^i$. Then $xb^i = x^\tau b^{i\lambda}$, and so $x^{-1}x^\tau = b^{i(1-\lambda)}$. Since $x^\tau \in \langle a, c\rangle$, we have $x^{-1}x^\tau \in \langle a, c\rangle$, and as $\langle a, c\rangle \cap \langle b\rangle = 1$, we conclude that $i(1-\lambda) \equiv 0 \pmod{p}$, which is not possible. Therefore, τ is a fixed-point-free automorphism of R. □

8.3 The Non-Abelian Metacyclic Groups

Let $R = \mathbb{Z}_{p^2}{:}\mathbb{Z}_p$ be non-abelian metacyclic, where $p \equiv 1 \pmod 4$ is a prime. Then by Theorem 3.2.3 the group R has no fixed-point-free automorphisms. We construct self-complementary Cayley graphs of R in this section.

Write

$$R = \langle a\rangle{:}\langle b\rangle \cong \mathbb{Z}_{p^2}{:}\mathbb{Z}_p,$$

where $a^b = a^{1+p}$. Let $c = a^p$. Then $\langle c\rangle = \mathbf{Z}(R) \cong \mathbb{Z}_p$. Let σ be an automorphism of $\langle c, b\rangle$, and τ be an automorphism of $\langle a\rangle$ such that

$$c^\sigma = c^\lambda, \quad b^\sigma = b^\lambda, \quad a^\tau = a^\lambda.$$

We notice that $\langle b, c\rangle \cap \langle a\rangle = \langle c\rangle$, and $c^\sigma = c^\tau$, that is, the restrictions of σ and τ to the subgroup $\langle c\rangle$ are equal.

Here we remark that in Section 4.1 we define σ to be an automorphism of $\langle a\rangle$, which is a cyclic group; in contrast, in this construction we define σ be an automorphism of $\langle c, b\rangle$, which is an elementary abelian p-group. Therefore, the construction

in this section will indeed produce self-complementary graphs that are different from those in Section 4.1.

Let S_1 be a SC-subset of $\langle c, b\rangle$ with respect to σ. Then $S_1^\sigma = \langle c, b\rangle^\# \setminus S_1$, and so for any elements $x = c^{i_1}b^{j_1}$ and $y = c^{i_2}b^{j_2}$, where $0 \le i_1, j_1, i_2, j_2 \le p-1$, we have

$$yx^{-1} \in S_1 \Longleftrightarrow y^\lambda x^{-\lambda} = y^\sigma (x^\sigma)^{-1} \notin S_1.$$

Thus the Cayley graph $\Gamma_1 = \mathrm{Cay}(\langle c, b\rangle, S_1)$ is self-complementary, and σ is a normal complementing isomorphism.

Let $\overline{R} = R/\langle c\rangle = \langle \overline{a}, \overline{b}\rangle \cong \mathbb{Z}_p^2$, and let $\overline{\rho} \in \mathsf{Aut}(\overline{R})$ be such that $\overline{a}^{\overline{\rho}} = \overline{a}^\lambda$ and $\overline{b}^{\overline{\rho}} = \overline{b}^\lambda$. Let $\overline{S}_2 \subset \langle \overline{a}, \overline{b}\rangle$ be a SC-subset with respect to $\overline{\rho}$, namely, $\overline{S}_2^{\overline{\rho}} = \langle \overline{a}, \overline{b}\rangle^\# \setminus \overline{S}_2$. Let

$$\Sigma = \mathrm{Cay}(\langle \overline{a}, \overline{b}\rangle, \overline{S}_2).$$

Then Σ is a self-complementary graph associated with the normal complementing isomorphism $\overline{\rho}$. Let $I = \{(i, j) \mid \overline{a}^i\overline{b}^j \in \overline{S}_2\}$, and let

$$S_2 = \bigcup_{(i,j)\in I} a^i b^j \langle c\rangle.$$

Then the Cayley graph $\Gamma_2 = \mathrm{Cay}(R, S_2)$ is a lexicographic product $\Sigma[\overline{\mathbf{K}}_p]$.

Lemma 8.3.1. *For any elements $x = a^{i_1}b^{j_1}c^{k_1}$ and $y = a^{i_2}b^{j_2}c^{k_2}$ such that $i_1 \neq i_2$,*

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} \notin \overline{S}_2.$$

Now we are ready to present a construction of self-complementary Cayley graphs of R. We remark that c is in the centre $\mathbf{Z}(R)$, and as $a^p = c$, each element of R can be uniquely written as $a^ib^jc^k$ with $0 \le i, j, k \le p-1$.

Construction 8.3.2. Using the notation defined above, let

$$S = S_1 \cup (S_2 \setminus \langle b, c\rangle),$$

and $\Gamma = \mathrm{Cay}(R, S)$. Define a map ρ:

$$\rho : \quad a^ib^jc^k \mapsto a^{i\lambda}b^{j\lambda}c^{k\lambda}, \quad \text{where } 0 \le i, j, k \le p-1.$$

Lemma 8.3.3. *The Cayley graph Γ defined in Construction 8.3.2 is self-complementary, and ρ is a complementing isomorphism.*

Proof. Pick two vertices $x = a^{i_1}b^{j_1}c^{k_1}$, and $y = a^{i_2}b^{j_2}c^{k_2}$ with $0 \le i_1, j_1, k_1, i_2, j_2, k_2 \le p-1$. Then as $c = a^p$ is in the centre of R, we have

$$\begin{aligned}
yx^{-1} &= (a^{i_2}b^{j_2}c^{k_2})(a^{i_1}b^{j_1}c^{k_1})^{-1} \\
&= a^{i_2}b^{(j_2-j_1)}a^{-i_1}c^{(k_2-k_1)} \\
&= a^{i_2-i_1}a^{-i_1(j_2-j_1)p}b^{j_2-j_1}c^{k_2-k_1} \\
&= a^{i_2-i_1}b^{j_2-j_1}c^{-i_1(j_2-j_1)+(k_2-k_1)}. \\
y^\rho(x^\rho)^{-1} &= (a^{i_2\lambda}b^{j_2\lambda}c^{k_2\lambda})(a^{i_1\lambda}b^{j_1\lambda}c^{k_1\lambda})^{-1} \\
&= a^{i_2\lambda}b^{(j_2-j_1)\lambda}a^{-i_1\lambda}c^{(k_2-k_1)\lambda} \\
&= a^{(i_2-i_1)\lambda}b^{(j_2-j_1)\lambda}c^{-i_1(j_2-j_1)\lambda+(k_2-k_1)\lambda}.
\end{aligned}$$

First assume that $i_2 = i_1$. Then we have

$$yx^{-1} = b^{(j_2-j_1)}c^{-i_1(j_2-j_1)+(k_2-k_1)},$$
$$y^\rho(x^\rho)^{-1} = b^{(j_2-j_1)\lambda}c^{-i_1(j_2-j_1)\lambda+(k_2-k_1)\lambda} = y^\sigma(x^\sigma)^{-1}.$$

Both yx^{-1} and $y^\rho(x^\rho)^{-1} \in \langle b, c\rangle$. By the definition of σ, we have $yx^{-1} \in S_1$ if and only if $y^\rho(x^\rho)^{-1} = y^\sigma(x^\sigma)^{-1} \notin S_1$.

Assume now that $i_2 \neq i_1$. Then we have

$$yx^{-1} \in S_2 \Longleftrightarrow \overline{y}\,\overline{x}^{-1} \in \overline{S}_2 \Longleftrightarrow \overline{y}^{\overline{\rho}}(\overline{x}^{\overline{\rho}})^{-1} \notin \overline{S}_2 \Longleftrightarrow y^\rho(x^\rho)^{-1} \notin S_2.$$

Therefore, the vertices x and y are adjacent in Γ if and only if x^ρ and y^ρ are not adjacent Γ, and so ρ is an isomorphism from Γ to the complement $\overline{\Gamma}$, namely, Γ is self-complementary and ρ is a complementing isomorphism. □

Proof of Theorem 8.1.1. Let R be a group of order p^3, where p is a prime. By Theorem 2.11.2, if a Cayley graph of R is self-complementary, then $p^3 \equiv 1 \pmod 4$, and so $p \equiv 1 \pmod 4$. Conversely,

(i) if R is abelian, then self-complementary Cayley graphs of R can be constructed by Corollary 8.2.2;

(ii) if R is non-abelian and non-metacyclic, then self-complementary Cayley graphs of R can be constructed by Lemma 8.2.3;

(iii) if R is non-abelian metacyclic, then self-complementary Cayley graphs of R can be constructed by Construction 8.3.2.

Therefore, we complete the proof. □

8.4 Self-Complementary Normal Cayley Graphs

We study normal Cayley graphs of order p^3 which are self-complementary in this section. For a group G, denote by $G^{(\infty)}$ the smallest normal subgroup of G such that $G/G^{(\infty)}$ is soluble. We first give a technical lemma for constructing self-complementary normal Cayley graphs.

Lemma 8.4.1. *Let σ be a fixed-point-free automorphism of a group R of order 2-power. For a subgroup $H \leq \mathsf{Aut}(R)$ which is normalised by σ, there exists a self-complementary Cayley graph $\Gamma = \mathrm{Cay}(R, S)$ such that $H \leq \mathsf{Aut}\Gamma$ and σ is a complementing isomorphism if and only if none of the $\langle\sigma\rangle$-orbits on $R^\#$ is contained in an orbit of H.*

Proof. Let $K = \langle H, \sigma\rangle$, and $L = \langle H, \sigma^2\rangle$. Then L is of index 2 in K.

Assume that there exists a self-complementary Cayley graph $\Gamma = \mathrm{Cay}(R, S)$ such that H is a subgroup of $\mathsf{Aut}\Gamma$ and σ is a complementing isomorphism. Then H fixes S setwise, and so does L. Since σ is a complementing isomorphism, σ maps

S to $R^\# \setminus S$. Since $S \cap (R^\# \setminus S) = \emptyset$, none of the $\langle\sigma\rangle$-orbits on S is a subset of an orbit of H. Similarly, none of the $\langle\sigma\rangle$-orbits on $R^\# \setminus S$ is a subset of an orbit of H. So no $\langle\sigma\rangle$-orbit on $R^\#$ is contained in any orbit of H.

Conversely, assume that none of the $\langle\sigma\rangle$-orbits on $R^\#$ is contained in an orbit of H. Then L is intransitive on each K-orbit on $R^\#$. Since L is a normal subgroup of K of index 2, L divides each K-orbit on $R^\#$ into two orbits which are equivalent by σ. Let S be the set of R which contains exactly one of the two orbits of L on each K-orbits. Then $S^\sigma = R^\# \setminus S$, and so $\Gamma = \mathrm{Cay}(R, S)$ is self-complementary with σ being a complementing isomorphism. □

Let $\Gamma = (V, E)$ be a self-complementary graph of order p^3 with p prime, and let σ be a complementing isomorphism. Let $G = \mathsf{Aut}\Gamma$, and let $X = \langle G, \sigma\rangle$.

Now we determine the case where $\mathsf{Aut}\Gamma$ is insoluble and primitive. Recall that the insoluble and primitive case for the graphs of order p^2 has already been determined in Lemma 7.3.3.

Lemma 8.4.2. *Assume that X is insoluble and primitive on V. Then $N = \mathsf{soc}(X) = \mathbb{Z}_p^3$, $X = N{:}X_\alpha$, and $\mathbb{Z}_{2^f} \circ X^{(\infty)} \le X_\alpha \le \mathbb{Z}_{p-1} \circ X^{(\infty)}$, where $2^f \le (p-1)_2$, and one of the following holds:*

(a) $X^{(\infty)} = \mathrm{PSL}(2,7)$, *and* $p \equiv 1, 9, 25 \pmod{56}$;

(b) $X^{(\infty)} = 3.\mathrm{A}_6$, *and* $p \equiv 1, 49 \pmod{120}$;

(c) $X^{(\infty)} = \mathrm{A}_5$, *and either* $p \equiv 1, 49 \pmod{60}$, *or* $p \equiv 1, 9 \pmod{20}$.

Moreover, for each of these three cases, examples exist.

Proof. Let X_α be the stabiliser of the vertex $\alpha \in V$ in the group X. Identify V with a vector space $\mathrm{GF}(p)^3$. Then X_α is an insoluble subgroup of $\mathrm{GL}(3,p)$. Since X is primitive on V, X_α is irreducible, and since G is not 2-transitive on V, $X_\alpha \not\ge \mathrm{SL}(3,p)$. Inspecting the subgroups of $\mathrm{GL}(3,p)$, given in [9, Tables 8.3, 8.7], one of the following holds, where $C = \mathbf{Z}(\mathrm{GL}(3,p)) = \mathbb{Z}_{p-1}$,

(i) $\mathrm{PSL}(2,7) \lhd X_\alpha \lhd C \times \mathrm{PSL}(2,7)$, and $p \equiv 1, 2, 4 \pmod 7$, or

(ii) $3.\mathrm{A}_6 \lhd X_\alpha \lhd C \circ (3.\mathrm{A}_6)$, where $p \equiv 1, 4 \pmod{15}$, or

(iii) $\mathrm{A}_5 \lhd X_\alpha \lhd C \times \mathrm{A}_5$, where $p \equiv 1, 4 \pmod{15}$ and A_5 is embedded in $3.\mathrm{A}_6$,

(iv) $\mathrm{A}_5 \lhd X_\alpha \lhd C \times \mathrm{A}_5$, where $p \equiv 1, 9 \pmod{10}$ and A_5 is embedded in $\Omega_3(p)$.

Let $K = X_\alpha^{(\infty)}$, the smallest normal subgroup of X_α such that X_α/K is soluble. Then $K = \mathrm{PSL}(2,7)$, $3.\mathrm{A}_6$, or A_5.

Since X is vertex-transitive, we may choose α which is fixed by the complementing isomorphism σ. Then $\sigma \in X_\alpha$, and $\sigma = cz$, where $c \in C$ and $z \in K$. As G_α is of index 2 in X_α, we have $K \le G_\alpha$. Thus $c \ne 1$. Since $cz = zc$ and $o(\sigma)$ is a power of

2, we may choose c, z such that both $o(c)$ and $o(z)$ are powers of 2. Then the order $o(\sigma) = \max\{o(c), o(z)\}$. Clearly, $o(c)$ divides $p-1$, and $o(z)$ divides 4.

By Lemma 2.11.2, $p \equiv 1 \pmod 4$. By Theorem 2.7.1, $\langle z \rangle$ preserves a direct sum $V = \langle \mathbf{v}_1 \rangle \oplus \langle \mathbf{v}_2 \rangle \oplus \langle \mathbf{v}_3 \rangle$ of 1-subspaces. Since $\langle z \rangle$ is faithful on V, it is faithful on at least one of these three subspaces, say $\langle \mathbf{v}_1 \rangle$, namely, $\mathbf{v}_1^z = \lambda \mathbf{v}_1$ where $1 \leq \lambda \leq p-1$. Noticing that the linear transformations of $\langle \mathbf{v}_1 \rangle$ form a cyclic group $\mathrm{GL}(\langle \mathbf{v}_1 \rangle) = \mathbb{Z}_{p-1}$, the restrictions $z|_{\langle \mathbf{v}_1 \rangle}$ and $c|_{\langle \mathbf{v}_1 \rangle}$ lie in the unique Sylow 2-subgroup of $\mathrm{GL}(\langle \mathbf{v}_1 \rangle)$. Suppose that $o(\sigma) = o(z)$. Then the restrictions $c_{\langle \mathbf{v}_1 \rangle}$ and $z_{\langle \tau \rangle}$ have equal order dividing 4 since $o(z) \,\big|\, 4$. It implies that the product $c|_{\langle \mathbf{v}_1 \rangle} z|_{\langle \mathbf{v}_1 \rangle} = \sigma|_{\langle \mathbf{v}_1 \rangle}$ has order 1 or 2, which is a contradiction since $\sigma|^2_{\langle \mathbf{v}_1 \rangle}$ should fix no non-zero vector of V by Lemma 2.11.3. Therefore, $o(c) \neq o(z)$.

Suppose that c is an involution. Then $\mathbf{v}_1^c = -\mathbf{v}_1$, and z is of order 4 and so is $\sigma = cz$. Now $\mathbf{v}_1^\sigma = \mathbf{v}_1^{cz} = -\lambda \mathbf{v}_1 = -\mathbf{v}_1^z$. It implies that the orbits $\mathbf{v}_1^{\langle \sigma \rangle}$ and $\mathbf{v}_1^{\langle z \rangle}$ are the same, which contradicts Lemma 8.4.1. Therefore, c is of order $2^f \geq 4$.

Assume that $2^f = 4$. Since $o(z) \,\big|\, 4$ and $o(z) \neq o(c)$, we have $z = 1$ or z is an involution. Hence $\sigma = cz$ is of order 4. Suppose that K has an element of order 4. Then $K = \mathrm{PSL}(2,7)$ or $3.\mathrm{A}_6$, and all involutions of K are conjugate. Let $g \in K$ be of order 4 such that $z \in \langle g \rangle$. Let $U = \langle \mathbf{v} \rangle$ be a 1-subspace of V which is fixed by g and is such that $\langle g \rangle$ is faithful on U. Then the restrictions $g|_U$ and $\sigma|_U$ are two elements of $\mathrm{GL}(\langle \mathbf{v} \rangle)$ of order 4, and hence $\sigma|_U = g|_U$ or $g|_U^{-1}$. Therefore, the orbits $\mathbf{v}^{\langle \sigma \rangle}$ and $\mathbf{v}^{\langle g \rangle}$ are the same, contradicting Lemma 8.4.1. Thus K has no element of order 4, and so $K = \mathrm{A}_5$. By Lemma 2.11.2, $p \equiv 1 \pmod 4$, and consequently, we conclude that

(I) if $p \equiv 1, 4 \pmod{15}$, then $p \equiv 1, 49 \pmod{60}$;

(II) if $p \equiv 1, 9 \pmod{10}$, then $p \equiv 1, 9 \pmod{20}$.

On the other hand, if $K = \mathrm{PSL}(2,7)$ or $3.\mathrm{A}_6$, the order of c is $2^f \geq 8$, and in particular, $p \equiv 1 \pmod 8$. For $K = \mathrm{PSL}(2,7)$, the equivalence equations $p \equiv 1 \pmod 8$ and $p \equiv 1, 2, 4 \pmod 7$ imply $p \equiv 1, 9, 25 \pmod{56}$. For $K = 3.\mathrm{A}_6$, the equivalence equations $p \equiv 1 \pmod 8$ and $p \equiv 1, 4 \pmod{15}$ imply $p \equiv 1, 49 \pmod{120}$.

Finally, let K be a subgroup of $\mathrm{GL}(3,p)$ satisfying one of parts (a)-(c) of the lemma. Let $\sigma \in \mathbf{Z}(\mathrm{GL}(3,p))$ be of order 2^f such that $f \geq 2$ for $K = \mathrm{A}_5$ and $f \geq 3$ for the other two groups. Then σ normalises K, and each $\langle \sigma \rangle$-orbit on $R^\#$ has length 2^f and is a subset of a cyclic subgroup of R. Let Δ be an orbit of K on R. Since $K \leq \mathsf{Aut}(R)$, we can partition Δ into

$$\Delta = \bigcup_{x \in \Delta} (\Delta \cap \langle x \rangle).$$

The setwise stabiliser of a part $B_x = \Delta \cap \langle x \rangle$ is a cyclic subgroup of order dividing $p-1$. If $|B_x|$ is divisible by 2^f, then there is an element of order 2^f which lies in K, which is not possible. Therefore, $|B_x|$ is not divisible by 2^f, and since each orbit of

$\langle\sigma\rangle$ has size divisible by 2^f, none of the $\langle\sigma\rangle$-orbits is contained in an orbit of K. By Lemma 8.4.1, there exists a self-complementary Cayley graph of R with σ being a complementing isomorphism. □

The next lemma determines the case where $\mathsf{Aut}\Gamma$ is insoluble and imprimitive.

Lemma 8.4.3. *Assume that X is insoluble and imprimitive on V, and has a normal subgroup R which is regular on V. Then $p \equiv 1, 9 \pmod{40}$, and for a vertex $\alpha \in V$, either*

(i) *$R = \mathbb{Z}_p^3$, and $X_\alpha = \mathbb{Z}_m \times \mathbb{Z}_\ell \circ \mathrm{SL}(2,5)$ or $p^2{:}(\mathbb{Z}_m \times \mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$, where both m and ℓ divide $p-1$, and ℓ is divisible by 8, or*

(ii) *$R = p_+^{1+2}$, and $X = p_+^{1+2}{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$ or $(p_+^{1+2} \circ p_+^{1+2}){:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$, where ℓ divides $p-1$ and is divisible by 8.*

Proof. Since R is normal in X and regular on V, we have $X = R{:}X_\alpha$, where $X_\alpha \le \mathsf{Aut}(R)$. Since X_α is insoluble, $R = \mathbb{Z}_p^3$ or p_+^{1+2}.

(1). Assume first that $R = \mathbb{Z}_p^3$. Identify V with a vector space $\mathrm{GF}(p)^3$. Since X is imprimitive on V, X_α is a reducible subgroup of $\mathrm{GL}(3,p)$, and fixes a 1-subspace U. Thus $X_\alpha \le p^2{:}(\mathrm{GL}(1,p) \times \mathrm{GL}(2,p))$. Since X_α is insoluble, it implies that $X_\alpha^{(\infty)} = p^2{:}\mathrm{SL}(2,p)$, $p^2{:}\mathrm{SL}(2,5)$, $\mathrm{SL}(2,p)$ or $\mathrm{SL}(2,5)$, see [9, Tables 8.1-8.2]. Since $\mathrm{GL}(U) \cong \mathbb{Z}_{p-1}$, the action of $X_\alpha^{(\infty)}$ on U is trivial, and hence $X^{(\infty)} = \mathbb{Z}_p^2{:}X_\alpha^{(\infty)}$. Suppose that $X_\alpha^{(\infty)} = p^2{:}\mathrm{SL}(2,p)$ or $\mathrm{SL}(2,p)$. Let $\mathcal{B}$ be the set of $X^{(\infty)}$-orbits on V, and let $B \in \mathcal{B}$. Then $|B| = p^2$, and $X^{(\infty)}$ acting on B is 2-transitive. So X_B^B is 2-transitive, and it implies that G_B^B is 2-transitive, which contradicts Theorem 2.11.5. We thus have $X_\alpha^{(\infty)} = p^2{:}\mathrm{SL}(2,5)$ or $\mathrm{SL}(2,5)$. Since $\mathrm{SL}(2,5)$ is a maximal subgroup of $\mathrm{SL}(2,p)$, it follows that $X_\alpha \le p^2{:}(\mathrm{GL}(1,p) \times (\mathrm{GL}(1,p) \circ \mathrm{SL}(2,5)))$. Moreover, since X_α is insoluble and $X_\alpha^{(\infty)} \le G_\alpha$ by Corollary 2.11.6, we have that $G_\alpha \ge \mathrm{SL}(2,5)$. By Lemma 8.4.1, it implies that $X_\alpha = \langle G_\alpha, \sigma\rangle \ge \mathbb{Z}_{2^f} \circ \mathrm{SL}(2,5)$ such that $o(\sigma) = 2^f \ge 8$. It is now easily shown that $X_\alpha = \mathbb{Z}_m \times \mathbb{Z}_\ell \circ \mathrm{SL}(2,5)$, or $p^2{:}(\mathbb{Z}_m \times \mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$, where both m and ℓ divide $p-1$, and ℓ is divisible by 8. Furthermore, the congruence equations $p \equiv 1 \pmod 8$ and $p \equiv 1, 9 \pmod{10}$ imply $p \equiv 1, 9 \pmod{40}$, as in part (i).

(2). Next assume that $R = p_+^{1+2}$. Then by Winter [54], the automorphism group $\mathsf{Aut}(R) = p^2{:}\mathrm{GL}(2,p)$. Since X is insoluble, so is X_α, which is a subgroup of $\mathsf{Aut}(R)$. Thus $X_\alpha^{(\infty)} = \mathrm{SL}(2,p)$, $p^2{:}\mathrm{SL}(2,p)$, $\mathrm{SL}(2,5)$, or $p^2{:}\mathrm{SL}(2,5)$.

Suppose that $X_\alpha^{(\infty)} = \mathrm{SL}(2,p)$ or $p^2{:}\mathrm{SL}(2,p)$. Let N be the centre $\mathbf{Z}(R) \cong \mathbb{Z}_p$. Then $N \lhd X$. Let $\mathcal{B}$ be the set of N-orbits on the vertex set V, and let $K = X_{(\mathcal{B})}$. By Theorem 2.11.5, there exists a self-complementary graph with vertex set $\mathcal{B}$ which is G/N-vertex-transitive and σ induces a complementing isomorphism. For a block $B \in \mathcal{B}$, the size $|B| = p$, and by Theorem 2.11.5, we have $K^B \lhd G_B^B$ is soluble, and so is K. Thus G/K and X/K are insoluble, and so $X^{\mathcal{B}} \ge p^2{:}\mathrm{SL}(2,p)$. It implies that $G^{\mathcal{B}} \ge p^2{:}\mathrm{SL}(2,p)$ is 2-transitive on $\mathcal{B}$, which contradicts Theorem 2.11.5.

We thus conclude that $X^{\mathcal{B}} \geq p^2{:}\mathrm{SL}(2,5)$, and $p \equiv 1 \pmod 8$. So $X_\alpha^{(\infty)} = \mathrm{SL}(2,5)$ or $p^2{:}\mathrm{SL}(2,5)$. Then X_α is contained in the normaliser of $X_\alpha^{(\infty)}$ in $\mathsf{Aut}(R) = p^2{:}\mathrm{GL}(2,p)$, and it follows that $X_\alpha \leq \mathrm{GL}(1,p) \circ \mathrm{SL}(2,5)$, or $p^2{:}(\mathrm{GL}(1,p) \circ \mathrm{SL}(2,5))$, respectively. For the former, $X = R{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))$, where ℓ divides $p-1$ and is divisible by 8. For the latter,

$$X = R{:}(p^2{:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5))) = (R \circ R){:}(\mathbb{Z}_\ell \circ \mathrm{SL}(2,5)).$$

This completes the proof. □

8.5 Two-Step-Primitive Self-Complementary Graphs

A transitive permutation group $X \leq \mathrm{Sym}(V)$ is called 2-*step-primitive* if there is a non-trivial block system $\mathcal{B}$ such that $X^{\mathcal{B}}$ is primitive and for a block $B \in \mathcal{B}$, the induced permutation group X_B^B is also primitive.

Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph. Let $G = \mathsf{Aut}\Gamma$, and let σ be a complementing isomorphism. As before, let $X = \langle G, \sigma \rangle$. Then $\sigma^2 \in G$, and G is a normal subgroup of X of index 2.

Lemma 8.5.1. *Assume that X is a 2-step-primitive group on V with respect to the block system $\mathcal{B}$. Let B be a block in $\mathcal{B}$. Then either*

(i) *the kernel $X_{(\mathcal{B})}$ is faithful on the block B, or*

(ii) *Γ is a lexicographic product of two vertex-primitive self-complementary graphs.*

Proof. Let $K = X_{(\mathcal{B})}$ be the kernel of X acting on $\mathcal{B}$. Then $X/K \cong X^{\mathcal{B}}$. Let $\mathcal{B} = \{B_0, B_1, \ldots, B_{m-1}\}$, and let $B = B_0$.

Assume that K is not faithful on B, namely, the kernel $K_{(B)} \neq 1$. Then $X_{(\mathcal{B})} = K \neq 1$. It implies that $K^B \neq 1$. Since X_B^B is primitive, K^B is transitive. Hence $\mathcal{B}$ is the set of K-orbits on V, namely, $\mathcal{B}$ is a normal partition.

Moreover, since $K_{(B)} \neq 1$, it implies that $K_{(B)}$ acts nontrivially on some block B_i with $i \neq 0$. Without loss of generality, suppose that $i = 1$. Since X^V is 2-step-primitive, the induced permutation group $X_{B_1}^{B_1}$ is primitive, and hence the normal subgroup $K_{(B)}^{B_1}$ is transitive on B_1.

Let Σ be an undirected orbital graph of X which contains an edge $\{\alpha, \beta\}$, where $\alpha \in B_0$ and $\beta \in B_1$. Suppose that Σ is disconnected. Let $\Sigma_0, \ldots, \Sigma_{n-1}$ be the connected components, and let C_j be the vertex set of Σ_j with $0 \leq j \leq n-1$. By Lemma 2.10.1, for each j with $1 \leq j \leq n-1$, the intersection $C_j \cap B_i \neq \emptyset$ for all i with $0 \leq i \leq n-1$. Clearly, $C_j \cap B_i$ is a block. Since X is 2-step-primitive with respect to $\mathcal{B}$, the intersection $B_i \cap C_j$ is a trivial block of $X_{B_i}^{B_i}$. Thus, either $|B_i \cap C_j| = 1$, or $B_i \subset C_j$. The latter is not possible since $X^{\mathcal{B}}$ is primitive, and so $|B_i \cap C_j| = 1$. Without loss of generality, let $\alpha \in C_0$. Then $\Sigma(\alpha)$ contains exactly one vertex in each block B_j. The subgroup K_α fixes the component C_0 and each block B_j, and hence K_α fixes the unique vertex in the intersection $\Sigma(\alpha) \cap B_1$, which contradicts that K_α is transitive on B_1. Therefore, Σ is a connected graph.

Let $\alpha_0 = \alpha, \alpha_1, \ldots, \alpha_\ell$ be a path of Σ such that $\alpha_i \in B_{j_i}$ and $K_{(B)}$ fixes B_{j_i} pointwise for $j_i \leq \ell - 1$ but not B_{j_ℓ}. Then each vertex in $B_{j_{\ell-1}}$ is adjacent in Σ to all vertices in B_{j_ℓ}, and the induced subgraph over $B_{j_{\ell-1}} \cup B_{j_\ell}$ of Σ is $\mathbf{K}_{b,b}$, where $b = |B|$. So $\Sigma = \Sigma_{\mathcal{B}}[\overline{\mathbf{K}}_b]$.

By Corollary 2.11.6, the kernel K is a subgroup of G, and so is K_α. Thus the induced subgraph $\mathbf{K}_{b,b}$ on $B_i \cup B_j$ is a subgraph of Γ or $\overline{\Gamma}$. The group G has index 2 in X, and the G-action on Σ divides Σ into two undirected orbital graphs Γ_1 and Γ_2 which are subgraphs of Γ and $\overline{\Gamma}$, respectively. Hence the complementing σ is an isomorphism between Γ_1 and Γ_2. Furthermore, σ induces an isomorphism between the quotient graphs $(\Gamma_1)_{\mathcal{B}}$ and $(\Gamma_2)_{\mathcal{B}}$. It follows that Γ_1 is a lexicographic product of the quotient graph $(\Gamma_1)_{\mathcal{B}}$ and $\overline{\mathbf{K}}_b$, namely, $\Gamma_1 = (\Gamma_1)_{\mathcal{B}}[\overline{\mathbf{K}}_b]$. We therefore conclude that $\Gamma = \Gamma_{\mathcal{B}}[\Gamma_0]$, where Γ_0 is the induced subgraph of Γ on the block B. □

8.6 Proof of Theorem 8.1.2

Let $\Gamma = (V, E)$ be a self-complementary vertex-transitive graph of order p^3, where p is a prime, and let σ be a complementing isomorphism. By Lemma 2.11.2, p is congruent to 1 modulo 4. Set $G = \mathsf{Aut}\Gamma$, and $X = \langle G, \sigma \rangle$.

Suppose that X is primitive on V. Recall from Theorem 2.11.4 that either

(i) X is an affine group; or

(ii) X is in product action with socle $\mathrm{PSL}(2, q^2)^\ell$, and $|V| = (q^2(q^2+1)/2)^\ell$, where q is odd and $\ell \geq 2$.

It is easily shown that the number $(q^2(q^2+1)/2)^\ell$ does not have the form p^3. Thus X is affine, and so Γ is a normal Cayley graph of the elementary abelian group $\mathbb{Z}_p^3$, as in part (i) of the theorem.

Next, assume that X is a 2-step primitive group on V. Suppose further that Γ is not a lexicographic product of two vertex-transitive self-complementary graphs. Let $\mathcal{B}$ be a block system of X acting on V, and let $K = X_{(\mathcal{B})}$ be the kernel of X acting on $\mathcal{B}$. By Lemma 8.5.1, the kernel $K = X_{(\mathcal{B})}$ is faithful on the block B, namely, $K \cong K^B$.

By Theorem 2.11.5, there exists a self-complementary graph with vertex set $\mathcal{B}$ which is (GK/K)-vertex-transitive and each element of $X \setminus G$ induces a complementing isomorphism. Since X is 2-step-primitive, $X^{\mathcal{B}}$ is primitive of degree p or p^2. By Lemma 6.2.1, $X^{\mathcal{B}}$ is affine, and p^3 does not divide the order $|X^{\mathcal{B}}|$. It follows that $X \ncong X^{\mathcal{B}}$ since the order $|X|$ is divisible by p^3. Thus $K \neq 1$.

Since $K \cong K^B$ and X is 2-step-primitive, K is a normal subgroup of the primitive permutation group X_B^B. By Lemma 6.2.1, X_B^B is affine, and the normal subgroup K contains the socle $N = \mathsf{soc}(X)$. Thus $K = N{:}K_v$, where $K_v \leq \mathsf{Aut}(N)$.

Assume that $|B| = p$. Then $K \lhd X_B^B \leq \mathrm{AGL}(1, p)$, and hence $K = N{:}K_v = \mathbb{Z}_p{:}\mathbb{Z}_k$, where k divides $p - 1$. Now $|\mathcal{B}| = p^2$, and the extension

$$X = K.X^{\mathcal{B}} = (N{:}K_v).(M{:}H) = (N.M).(K_v.H) = (\mathbb{Z}_p.\mathbb{Z}_p^2).(K_v.H),$$

and the normal subgroup $N.M = \mathbb{Z}_p.\mathbb{Z}_p^2$ is regular on the vertex set V.

Assume now that $|B| = p^2$. Then $K = N{:}K_v$ is such that $N = \mathbb{Z}_p^2$ and $K_v < \mathrm{GL}(2,p)$. Now $|\mathcal{B}| = p$, and $X^{\mathcal{B}} = M{:}H$ is such that $M = \mathbb{Z}_p$ and $H \leq \mathbb{Z}_{p-1}$. We consider the extension $X = K.X^{\mathcal{B}} = (N{:}K_v).(M{:}H) = (\mathbb{Z}_p^2{:}K_v).(\mathbb{Z}_p{:}H)$. Let $C = \mathbf{C}_X(N)$, the centraliser of N in X. Then $X/C \leq \mathsf{Aut}(N) \cong \mathrm{GL}(2,p)$. If $M < C$, then $N.M$ is a normal subgroup of X and is regular on V, we are done. Suppose that $M \not< C$. Then $K_v.M < \mathrm{GL}(2,p)$. Inspecting the subgroups of $\mathrm{GL}(2,p)$ (refer to [9, Tables 8.1-8.2]), we conclude that $K_v.M = K_v \times M$, and hence $N.M$ is normal in X. Thus $N.M = \mathbb{Z}_p.\mathbb{Z}_p$ is regular on V.

Finally, assume that X is neither primitive nor 2-step-primitive on V. Let $\mathcal{B}$ be a non-trivial block system of X on V such that $X^{\mathcal{B}}$ is imprimitive. Then $|\mathcal{B}| = p^2$ as $|V| = p^3$. Let $B \in \mathcal{B}$. Then $|B| = p$, and so X_B^B is primitive. Since $X^{\mathcal{B}}$ is imprimitive, it implies that there is a block system $\mathcal{C}$ of X such that $|\mathcal{C}| = p$, and hence a block has size p^2. By Lemma 8.4.3, X is a 2-step-primitive group. □

Appendix A

GAP Codes

The software we used is GAP (Version 4.7.2 of 01-Dec-2013) [16]. The meaning of each command is explained after the # symbol.

```
gap> G:=GL(5,3); # define the group GL(5,3)
GL(5,3)
gap> L:=Filtered(ConjugacyClasses(G),x->Order(Representative(x))=9);
# define the conjugacy classes of the elements that has order 9
[ [ [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3), 0*Z(3) ],
      [ Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3) ],
      [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), Z(3)^0, Z(3)^0, 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ] ]^G,
  [ [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0, Z(3) ] ]^G ]
gap> reps:=List(L,Representative);
# fix the representatives for the conjugacy classes
[ [ [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3), 0*Z(3) ],
      [ Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3) ],
      [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), Z(3)^0, Z(3)^0, 0*Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ] ],
  [ [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), Z(3)^0 ],
      [ 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), Z(3) ],
      [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0, Z(3) ] ] ]
gap> quotient:=List(reps,g->FactorGroup(Normalizer(G,Group(g)),Group(g)));
# define the quotient group N_G(<x>)/<x>
```

```
[ Group([ <identity> of ..., <identity> of ..., f5, f6^2, f4, f3, f4*f7^2,
      f2, f1^2*f2*f4 ]),
  Group([ <identity> of ..., <identity> of ..., f5, f4, f2, f1^2*f2 ]) ]
gap> List(quotient,StructureDescription);
# calculate the structure of the quotient groups
[ "C3 x C6 x S3 x S3", "C2 x C2 x ((C3 x C3) : C3)" ]
```

Bibliography

[1] Graph theory. http://en.wikipedia.org/wiki/Graph_theory#Applications. Accessed: 2014.

[2] Shannon capacity of a graph. http://en.wikipedia.org/wiki/Shannon_capacity_of_a_graph#cite_note-5. Accessed: 2014.

[3] J. L. Alperin and Rowen B. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[4] Brian Alspach, Joy Morris, and V. Vilfred. Self-complementary circulant graphs. *Ars Combin.*, 53:187–191, 1999.

[5] Brian Alspach and T. D. Parsons. A construction for vertex-transitive graphs. *Canad. J. Math.*, 34(2):307–318, 1982.

[6] Robert A. Beezer. Sylow subgraphs in self-complementary vertex transitive graphs. *Expo. Math.*, 24(2):185–194, 2006.

[7] Ja. G. Berkovič. Finite metacyclic groups. *Sakharth. SSR Mecn. Akad. Moambe*, 68:529–532, 1972.

[8] Norman Biggs. *Algebraic graph theory*. Cambridge University Press, London, 1974. Cambridge Tracts in Mathematics, No. 67.

[9] J.N. Bray, D.F. Holt, and C.M. Roney-Dougal. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2013.

[10] V. Chvátal, P. Erdős, and Z. Hedrlín. Ramsey's theorem and self-complementary graphs. *Discrete Math.*, 3:301–304, 1972.

[11] C. R. J. Clapham. A class of self-complementary graphs and lower bounds of some Ramsey numbers. *J. Graph Theory*, 3(3):287–289, 1979.

[12] Marlene Jones Colbourn and Charles J. Colbourn. Graph isomorphism and self-complementary graphs. *SIGACT News*, 10(1):25–29, April 1978.

[13] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[14] Raúl Figueroa and Reinaldo E. Giudici. Group generation of self-complementary graphs. In *Combinatorics and graph theory (Hefei, 1992)*, pages 131–140. World Sci. Publ., River Edge, NJ, 1993.

[15] Dalibor Fronček, Alexander Rosa, and Jozef Širáň. The existence of selfcomplementary circulant graphs. *European J. Combin.*, 17(7):625–628, 1996.

[16] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.5*, 2014.

[17] Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., New York, NY, USA, 1990.

[18] Michael Giudici, Cai Heng Li, Primo Potonik, and Cheryl E. Praeger. Homogeneous factorisations of graphs and digraphs. *European Journal of Combinatorics*, 27(1):11 – 37, 2006.

[19] C. Godsil and G.F. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics. Springer New York, 2001.

[20] C. D. Godsil. On the full automorphism group of a graph. *Combinatorica*, 1(3):243–256, 1981.

[21] Daniel Gorenstein and I. N. Herstein. Finite groups admitting a fixed-point-free automorphism of order 4. *Amer. J. Math.*, 83:71–78, 1961.

[22] R. M. Guralnick, Cai Heng Li, Cheryl E. Praeger, and J. Saxl. On orbital partitions and exceptionality of primitive permutation groups. *Trans. Amer. Math. Soc.*, 356(12):4857–4872, 2004.

[23] W. Su H. Luo and Z. Li. The properties of self-complementary graphs and new lower bounds for diagonal ramsey numbers. *Austral. J. Combin.*, 25:103 – 116, 2002.

[24] E. I. Huhro. Finite groups that admit a 2-automorphism without fixed points. *Mat. Zametki*, 23(5):651–657, 1978.

[25] Robert Jajcay and Cai Heng Li. Constructions of self-complementary circulants with no multiplicative isomorphisms. *European J. Combin.*, 22(8):1093–1100, 2001.

[26] J. H. Koolen. On selfcomploementary vertex-transitive graphs. 1997.

[27] Cai Heng Li. On self-complementary vertex-transitive graphs. *Comm. Algebra*, 25(12):3903–3908, 1997.

[28] Cai Heng Li. On finite graphs that are self-complementary and vertex-transitive. *Australas. J. Combin.*, 18:147–155, 1998.

[29] Cai Heng Li and Cheryl E. Praeger. Self-complementary vertex-transitive graphs need not be Cayley graphs. *Bull. London Math. Soc.*, 33(6):653–661, 2001.

[30] Cai Heng Li and Cheryl E. Praeger. Constructing homogeneous factorisations of complete graphs and digraphs. *Graphs Combin.*, 18(4):757–761, 2002. Graph theory and discrete geometry (Manila, 2001).

[31] Cai Heng Li and Cheryl E. Praeger. On partitioning the orbitals of a transitive permutation group. *Trans. Amer. Math. Soc.*, 355(2):637–653 (electronic), 2003.

[32] Cai Heng Li and Cheryl E. Praeger. On finite permutation groups with a transitive cyclic subgroup. *J. Algebra*, 349:117–127, 2012.

[33] Cai Heng Li and Guang Rao. Self-complementary vertex-transitive graphs of order a product of two primes. *Bull. Aust. Math. Soc.*, 89(2):322–330, 2014.

[34] Cai Heng Li, Guang Rao, and ShuJiao Song. On finite self-complementary metacirculants. *Journal of Algebraic Combinatorics*, pages 1–10, 2014.

[35] Cai Heng Li, Shu Jiao Song, and Dian Jun Wang. A characterization of metacirculants. *Journal of Combinatorial Theory, Series A*, 120(1):39 – 48, 2013.

[36] Cai Heng Li, Shaohui Sun, and Jing Xu. Self-complementary circulants of prime-power order. *SIAM J. Discrete Math.*, 28(1):8–17, 2014.

[37] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On the o'nan-scott theorem for finite primitive permutation groups. *Journal of the Australian Mathematical Society (Series A)*, 44:389–396, 6 1988.

[38] Valery Liskovets and Reinhard Pöschel. Non-cayley-isomorphic self-complementary circulant graphs. *J. Graph Theory*, 34(2):128–141, 2000.

[39] Peter Lorimer. Vertex-transitive graphs: symmetric graphs of prime valency. *J. Graph Theory*, 8(1):55–68, 1984.

[40] L. Lovasz. On the shannon capacity of a graph. *IEEE Trans. Inf. Theor.*, 25(1):1–7, September 2006.

[41] D. Marušič. Vertex transitive graphs and digraphs of order p^k. In *Cycles in graphs (Burnaby, B.C., 1982)*, volume 115 of *North-Holland Math. Stud.*, pages 115–128. North-Holland, Amsterdam, 1985.

[42] Rudolf Mathon. On self-complementary strongly regular graphs. *Discrete Math.*, 69(3):263–281, 1988.

[43] Mikhail Muzychuk. On Sylow subgraphs of vertex-transitive self-complementary graphs. *Bull. London Math. Soc.*, 31(5):531–533, 1999.

[44] Wojciech Peisert. All self-complementary symmetric graphs. *J. Algebra*, 240(1):209–229, 2001.

[45] Cheryl Praeger, Cai Heng Li, and Linda Stringer. Common circulant homogeneous factorisations of the complete digraph. *Discrete Mathematics*, 309(10):3006 – 3012, 2009.

[46] S. B. Rao. On regular and strongly-regular self-complementary graphs. *Discrete Math.*, 54(1):73–82, 1985.

[47] R. C. Read. On the number of self-complementary graphs and digraphs. *J. London Math. Soc.*, 38:99–104, 1963.

[48] Derek John Scott Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

[49] Gert Sabidussi. Vertex-transitive graphs. *Monatsh. Math.*, 68:426–438, 1964.

[50] Horst Sachs. Über selbstkomplementäre Graphen. *Publ. Math. Debrecen*, 9:270–288, 1962.

[51] D. A. Suprunenko. Self-complementary graphs. *Kibernetika (Kiev)*, (5):i, 1–6, 24, 133, 1985.

[52] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1982. Translated from the Japanese by the author.

[53] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

[54] David L. Winter. The automorphism group of an extraspecial p-group. *Rocky Mountain J. Math.*, 2(2):159–168, 1972.

[55] Bohdan Zelinka. Self-complementary vertex-transitive undirected graphs. *Math. Slovaca*, 29(1):91–95, 1979.

[56] Hong Zhang. Self-complementary symmetric graphs. *J. Graph Theory*, 16(1):1–5, 1992.

[57] Hong Zhang. On edge transitive circulant graphs. *Tokyo Journal of Mathematics*, 19(1):51–55, 06 1996.