Commuting Graphs of Finite Groups

Timothy Jon Woodcock
Belchertown, Massachusetts

Master of Science, University of Virginia, 2003
Bachelor of Science, Stonehill College, 1993

A Dissertation presented to the Graduate Faculty
of the University of Virginia in Candidacy for the Degree of
Doctor of Philosophy

Department of Mathematics

University of Virginia
December, 2010

Andrei Rapinchuk

Mikhail Ershov

Abstract

The commuting graph of a finite group is defined to have the nontrivial elements of the group as its vertices, and an edge joining each commuting pair of elements. We explore the structure of the commuting graph for a variety of groups. In particular, the diameter of the commuting graph of the symmetric group S_n is precisely described, based on the nature of n and $n - 1$. Furthermore the connected components of this graph are completely classified. We continue by establishing upper bounds on the diameter of the commuting graph for a certain class of solvable groups. Finally, we provide a structure theorem for groups of order $p^a q^b$ that consist strictly of p- and q-elements, including a description of the commuting graph of such a group.

Contents

For my wife, Suzanne,

my children,

and my parents.

Chapter 1

Introduction

1.1 Definitions

Given a finite group G, we let G^* denote the set of all nontrivial elements of G. For a nonempty subset X of G^*, let E_X denote the collection of all 2-element subsets $\{g, h\}$ of X such that g and h commute, under the product of G. We define the **commuting graph** of X, denoted by Δ_X, to be the ordered pair (X, E_X). We remark that as we make use of this notation in our work of the following chapters, the group G will be understood from context.

A sequence of elements $(x_0, x_1, \ldots, x_i)$ over X is called a **commuting path** in Δ_X, or a commuting path from x_0 to x_i, if for $j < i$, $\{x_j, x_{j+1}\} \in E_X$ or $x_j = x_{j+1}$. The **length** of a commuting path $(x_0, x_1, \ldots, x_i)$ is defined to be equal to the nonnegative integer i, which is one less than the number of terms in the path.

For an arbitrary pair of elements $g, h \in X$, possibly alike, we define the **distance** between g and h in Δ_X to be the minimum length of a commuting path from g to h, provided that one exists. We denote this distance by $d_{\Delta_X}(g, h)$. If there is no commuting path from g to h, we let $d_{\Delta_X}(g,h) = \infty$, and take the convention that $i < \infty$ for all nonnegative integers i. We note that $d_{\Delta_X}(g,h) = d_{\Delta_X}(h,g)$ in general, because $(g, x_1, \ldots, x_{i-1}, h)$ is a commuting path in Δ_X if and only if $(h, x_{i-1}, \ldots, x_1, g)$ is as such.

If $d_{\Delta_X}(g,h) < \infty$ for all $g, h \in X$, then we say that Δ_X is **connected**. Otherwise, Δ_X is said to be **disconnected**. If Y is a maximal subset of X such that Δ_Y is connected, then Δ_Y is called a **connected component**, or just a component, of Δ_X. We define the **diameter** of Δ_X to be the maximum value of $d_{\Delta_X}(g,h)$, taken over all pairs of elements g and h of X, notably a finite set. We remark that Δ_X is connected if and only if its diameter is $< \infty$.

1.2 History

Commuting graphs were first studied by Y. Segev in the paper [11]. There the following concept was introduced, in advance of the main result 1.2.2.

Definition 1.2.1. *Let G be a nontrivial finite group. Then the commuting graph Δ_{G^*} is called* ***balanced*** *if there exist elements g and h in G^* such that $d_{\Delta_{G^*}}(x,y) \geq 3$ for each pair $\{x,y\} \in \{\{g,h\},\ \{g,gh\},\ \{h,gh\},\ \{g,g^{-1}h\},\ \{h,g^{-1}h\}\}$.*

Theorem 1.2.2 (Segev)**.** *Let G be a nonabelian finite simple group, and D a finite dimensional division algebra over an arbitrary field. If Δ_{G^*} is balanced or has diameter > 4, then G cannot be isomorphic to a quotient of the multiplicative group of D.*

In the subsequent paper [12], a complementary result was realized.

Theorem 1.2.3 (Segev, Seitz)**.** *If G is a nonabelian finite simple group, then Δ_{G^*} is balanced or has diameter > 4.*

In combination, 1.2.2 and 1.2.3 resolved a conjecture of [7], having an unexpected relationship to commuting graphs and their diameters.

Conjecture 1.2.4 (Potapchik, Rapinchuk)**.** *Let D be a finite dimensional division algebra over an arbitrary field. Then no quotient of the multiplicative group of D is a nonabelian finite simple group.*

A further connection between division algebras and commuting graphs was exhibited in the following result of [8].

Theorem 1.2.5 (Rapinchuk, Segev)**.** *Let D be a finite dimensional division algebra over a finitely generated field, and let $D^{\#}$ be the multiplicative group of D. Let N be a normal subgroup of $D^{\#}$ of finite index. If $\Delta_{\left(D^{\#}/N\right)^*}$ has diameter ≥ 4, then N is open in D with respect to a nontrivial (height one) valuation of D.*

Commuting graphs were also key in realizing the culminating result in this line of research, found in [9].

Theorem 1.2.6 (Rapinchuk, Segev, Seitz)**.** *Let D be a finite dimensional division algebra. Then any finite quotient of the multiplicative group of D is solvable.*

More recently, the study of commuting graphs has gained independent combinatorial interest. For example, the following result was proved in the paper [1].

Theorem 1.2.7 (Bates, Bundy, Perkins, Rowley). *For positive integers $n \geq 2$ and $m \leq n/2$, let X_m be the set of all products of m disjoint transpositions in the symmetric group S_n. Then Δ_{X_m} is disconnected if and only if $n = 2m + 1$ or $n = 4$ and $m = 1$. Furthermore if Δ_{X_m} is connected, then the diameter of Δ_{X_m} is ≤ 3, unless $2m + 2 = n \in \{6, 8, 10\}$, in which case the diameter of Δ_{X_m} is 4.*

In the follow-up paper [2], Bundy examines the commuting graph Δ_X for an arbitrary conjugacy class $X \subseteq S_n$. In particular, a necessary and sufficient condition for connectivity of Δ_X is given, based on the cycle structure of X.

1.3 Overview

The main contribution of this dissertation, in Chapter 2, is a complete classification of the structure of $\Delta_{S_n^*}$, based on the nature of n. In particular each connected component is identified, along with its diameter. Especially noteworthy is that regardless of the value of n, no component has diameter > 5. In fact the typical case is that $\Delta_{S_n^*}$ is connected of diameter 5. Among our arguments, we develop a construction that yields a new proof of a result first obtained by Bates et al., in their paper [1]. We remark that the alternating groups A_n were explored by Segev and Seitz in [12]. But only a lower bound on the diameter of $\Delta_{A_n^*}$ was given, and moreover our approach to understanding $\Delta_{S_n^*}$ is essentially different, and more elementary.

In Chapter 3, we show that if G is a finite group with a nontrivial abelian normal subgroup, and if for all primes p dividing the order of G, each Sylow p-subgroup of G has multiple subgroups of order p, then Δ_{G^*} is connected of diameter ≤ 7. We remark that the structure possibilities for a finite p-group with only a single subgroup of order p are completely understood. In particular, such a group is either cyclic, or a generalized quaternion group. A more detailed discussion of this classification is given in Chapter 3, or one may consult [10, pp.141–143]. We note that if G is a nontrivial finite solvable group with derived series $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_{i-1} \supsetneq G_i = \{1_G\}$, then G_{i-1} is a nontrivial abelian normal subgroup of G. (Refer to the proof of 3.1.3.) Thus as a corollary to the chapter's main result, we realize an absolute bound on the diameter of Δ_{G^*}, for a solvable group with no cyclic or generalized quaternion Sylow subgroups.

Chapter 4 is an investigation of groups whose order is divisible by exactly two distinct primes. If G is a group of order $p^a q^b$, where p and q are prime and $p \neq q$, then G is solvable by Burnside's Theorem. Thus the bound of Chapter 3 applies to the diameter of Δ_{G^*}, provided that the Sylow p- and q-subgroups are suitable. However, we give a precise condition for connectivity. In particular, the bound of 7 on the diameter of Δ_{G^*} applies as long as G possesses an element of mixed order, that is, of order divisible by both p and q. But if G is comprised of p- and q-elements only, then Δ_{G^*} is disconnected. For disconnected cases, we give a complete description of the structure of the group G.

Chapter 2

Symmetric Groups

2.1 Main result

Definition 2.1.1. *For a positive integer n, we define the* ***symmetric group on*** $\mathbf{n}$ ***elements****, denoted* $\mathbf{S_n}$*, to be the set of all bijective functions on the set* $\{1, 2, \ldots, n\}$*. For $n \geq 2$ and $m \in \{2, 3, \ldots, n\}$, we let* $\mathbf{C_n^m}$ *denote the set of all cycles of length m in S_n. Also, we define* $\mathbf{R_n} = S_n^* \setminus (C_n^n \cup C_n^{n-1})$*.*

Theorem 2.1.2. *Suppose that $n \geq 3$, so that $\Delta_{S_n^*}$ is nontrivial.*

- ***a.*** *If $n-1$ and n are composite numbers, then $\Delta_{S_n^*}$ is connected of diameter 5.*

- ***b.*** *If $n-1$ is a prime, then $\Delta_{S_n^*}$ has connected components $\Delta_{R_n \cup C_n^n}$, and $\Delta_{\langle\gamma\rangle^*}$, $\gamma \in C_n^{n-1}$. The diameter of $\Delta_{R_n \cup C_n^n}$ is 1, 3, or 4 according as n is 3, 4, or > 4. The diameter of each $\Delta_{\langle\gamma\rangle^*}$ is 0 or 1, according as n is 3 or > 3.*

- ***c.*** *If n is a prime, $n > 3$, then $\Delta_{S_n^*}$ has connected components $\Delta_{R_n \cup C_n^{n-1}}$, and $\Delta_{\langle\gamma\rangle^*}$, $\gamma \in C_n^n$. The diameter of $\Delta_{R_n \cup C_n^{n-1}}$ is 5; the diameter of each $\Delta_{\langle\gamma\rangle^*}$ is 1.*

We shall realize the theorem through a number of sections. For more on S_n, refer to [4, p.46], for instance. Throughout the chapter, n denotes a positive integer.

2.2 Commuting elements of S_n

The results developed here are well known, but included for completeness.

Definition 2.2.1. *Suppose that π and ρ are elements of S_n. We say that π* ***induces a cycle map*** *on ρ if, for each cycle $(a_0\ a_1\ \cdots\ a_{i-1})$ in the decomposition of ρ, $(\pi(a_0)\ \pi(a_1)\ \cdots\ \pi(a_{i-1}))$ is a cycle of ρ as well.*

Proposition 2.2.2. *Let π and ρ be elements of S_n. Then π and ρ commute if and only if π induces a cycle map on ρ.*

Proof. Suppose that π and ρ are commuting elements, and let $(a_0\ a_1\ \cdots\ a_{i-1})$ be a cycle of ρ, possibly with $i = 1$. Then $\rho(a_j) = a_{(j+1) \bmod i}$ for $0 \leq j < i$. Therefore,

$$\rho\left(\pi(a_j)\right) \;=\; \pi\left(\rho(a_j)\right) \;=\; \pi\left(a_{(j+1) \bmod i}\right).$$

Hence $(\pi(a_0)\ \pi(a_1)\ \cdots\ \pi(a_{i-1}))$ is a cycle of ρ.

Now assume that π induces a cycle map on ρ, and let $a \in \{1, 2, \ldots, n\}$. Suppose that $(a_0\ a_1\ \cdots\ a_{i-1})$ is the cycle of ρ containing a; assume that $a_j = a$. We observe that $\rho(a_j) = a_{(j+1) \bmod i}$, thus $(\pi\rho)(a_j) = \pi(a_{(j+1) \bmod i})$. Since π induces a cycle map on ρ, $(\pi(a_0)\ \pi(a_1)\ \cdots\ \pi(a_{i-1}))$ is a cycle of ρ. Thus $\rho\left(\pi(a_j)\right) = \pi(a_{(j+1) \bmod i})$, in particular. Therefore $(\pi\rho)(a_j) = (\rho\pi)(a_j)$. We conclude that π and ρ are commuting elements, because a was chosen arbitrarily from $\{1, 2, \ldots, n\}$, and $a_j = a$. □

We remark that the statement of 2.2.2 is symmetric with respect to π and ρ. Therefore, we realize that π induces a cycle map on ρ if and only if ρ induces a cycle map on π.

Proposition 2.2.3. *Let $\pi \in S_n$, and let γ be a cycle in the decomposition of π. Then π commutes with γ.*

Proof. Suppose that $\gamma = (a_0\ a_1\ \cdots\ a_{i-1})$. Then for $0 \leq j < i$, we have $\pi(a_j) = \gamma(a_j)$, because γ is a cycle of π. Therefore,

$$(\pi(a_0)\ \pi(a_1)\ \cdots\ \pi(a_{i-1})) \;=\; (a_1\ a_2\ \cdots\ a_{i-1}\ a_0) \;=\; \gamma.$$

Hence π induces a cycle map on γ, and so π and γ commute by 2.2.2. □

Proposition 2.2.4. *Suppose that π and ρ are commuting elements of S_n, and let $\gamma = (a_0\ a_1\ \cdots\ a_{i-1})$ be a cycle in the decomposition of π. Assume that γ has unique length among all of cycles of π. Then ρ acts on $\{a_0, a_1, \ldots, a_{i-1}\}$ as a power of γ.*

Proof. Since π and ρ commute, $(\rho(a_0)\ \rho(a_1)\ \cdots\ \rho(a_{i-1}))$ is a cycle of π by 2.2.2. Therefore $(\rho(a_0)\ \rho(a_1)\ \cdots\ \rho(a_{i-1})) = \gamma$, because of the unique length of γ. Assuming that $\rho(a_0) = a_k$, we observe that γ may also be expressed as

$$\left(a_k\ a_{(k+1) \bmod i}\ \cdots\ a_{(k+i-1) \bmod i}\right).$$

Hence we conclude that $\rho(a_j) = a_{(k+j) \bmod i}$ for $0 \leq j < i$. In other words, ρ acts on $\{a_0, a_1, \ldots, a_{i-1}\}$ in precisely the same manner as γ^k. □

Definition 2.2.5. *Let $\pi \in S_n$. We define the **fixed set** of π to be the set of all elements $a \in \{1, 2, \ldots, n\}$ such that $\pi(a) = a$. We denote this set by $F(\pi)$.*

Proposition 2.2.6. *Suppose that $\pi, \rho \in S_n$ are commuting elements. Also assume that $F(\pi)$ contains exactly one element, say a. Then $a \in F(\rho)$ as well.*

Proof. We observe that the element a constitutes a trivial cycle of π, since $a \in F(\pi)$. Furthermore this is true of the element $\rho(a)$, by 2.2.2. But π has only one trivial cycle, because $F(\pi)$ contains just a single element. Hence we conclude that $\rho(a) = a$. □

Definition 2.2.7. *Let $\pi \in S_n$. We define the **moved set** of π to be complement of the fixed set of π, with respect to $\{1, 2, \ldots, n\}$. We denote the moved set by $M(\pi)$.*

Definition 2.2.8. *Let $\pi, \rho \in S_n$. We say that π and ρ are **disjoint elements** if $M(\pi) \cap M(\rho)$ is empty.*

Proposition 2.2.9. *Assume that π and ρ are disjoint elements of S_n. Then π and ρ commute.*

Proof. Since π and ρ are disjoint, π acts as the identity on $M(\rho)$. Thus π induces a function on $F(\rho)$. Likewise, ρ acts on $F(\pi)$. Now let $a \in \{1, 2, \ldots, n\}$. We observe that a is fixed by π or ρ, because π and ρ are disjoint elements. If $a \in F(\pi)$, then $(\rho\pi)(a) = \rho(a)$. Moreover we have $(\pi\rho)(a) = \rho(a)$, since $\rho(a) \in F(\pi)$ as well. Hence $(\rho\pi)(a) = (\pi\rho)(a)$. This conclusion is drawn similarly if $a \in F(\rho)$; thus $(\rho\pi)(a) = (\pi\rho)(a)$ holds in general. Therefore π and ρ are commuting elements. □

Definition 2.2.10. *Let H be a subgroup of S_n. For an element $a \in \{1, 2, \ldots, n\}$, we define its **orbit under the natural action of** $\mathbf{H}$ to be the set $\{\pi(a) \mid \pi \in H\}$. We denote this set by $[a]_H$.*

Proposition 2.2.11. *Let H be a subgroup of S_n. Then the family of all orbits under the natural action of H, $\{[a]_H \mid a \in \{1, 2, \ldots, n\}\}$, forms a partition of $\{1, 2, \ldots, n\}$ such that $a \in [a]_H$ for all $a \in \{1, 2, \ldots, n\}$.*

Proof. Since H is a subgroup of S_n, H contains the identity function. Hence, for $a \in \{1, 2, \ldots, n\}$, we have $a \in [a]_H$. Suppose $b \in \{1, 2, \ldots, n\}$ as well, and assume that $[a]_H \cap [b]_H$ is nonempty. Select $x \in [a]_H \cap [b]_H$, and suppose that $\pi(a) = \rho(b) = x$, where $\pi, \rho \in H$. Furthermore let $y \in [a]_H$, and assume that $y = \varphi(a)$, where $\varphi \in H$. Then we have

$$\left(\varphi\pi^{-1}\rho\right)(b) \;=\; \left(\varphi\pi^{-1}\right)(x) \;=\; \varphi(a) \;=\; y.$$

Also, $\varphi\pi^{-1}\rho \in H$, because H is a group. Therefore $y \in [b]_H$, hence $[a]_H \subseteq [b]_H$. And the reverse containment is established by analogy. Thus $[a]_H = [b]_H$. □

Proposition 2.2.12. *Let H be a subgroup of S_n. Assume that π is a member of the center of H, and suppose that $a \in F(\pi)$. Then $[a]_H \subseteq F(\pi)$.*

Proof. Let $b \in [a]_H$, and suppose that $\rho(a) = b$, where $\rho \in H$. Since π is an element of the center of H, π and ρ are commuting elements. Therefore,

$$\pi(b) \;=\; \pi(\rho(a)) \;=\; \rho(\pi(a)) \;=\; \rho(a) \;=\; b.$$

The lemma follows. □

2.3 The commuting graph Δ_{R_n}

Theorem 2.3.1. *Suppose that $n \geq 4$. Then Δ_{R_n} is connected. Furthermore, the diameter of Δ_{R_n} is 3 or 4, according as $n = 4$ or $n > 4$.*

The proof of the theorem is realized via a sequence of results. We remark that R_n is empty for $n \in \{1, 2, 3\}$.

Proposition 2.3.2. *The diameter of Δ_{R_4} is 3.*

Proof. Let us define

$$\begin{aligned} T &= \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\}, \\ D &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}. \end{aligned}$$

We observe that T is the set of all transpositions in S_4, and D is the set of all double transpositions. Also, any element of S_4^* that is neither a cycle of length 3 nor a cycle of length 4 is a member of $T \cup D$. Therefore $R_4 = T \cup D$.

We claim that any $\pi \in R_4$ commutes with an element $\varphi \in D$. If $\pi \in D$, we may take $\varphi = \pi$, because a group element commutes with itself. Given that $\pi \in T$, let us assume that $\pi = (a\ b)$. Then by 2.2.3, π commutes with $\varphi = (a\ b)(c\ d) \in D$, where c and d are the elements of $\{1, 2, 3, 4\} \setminus \{a, b\}$ in arbitrary order. Thus we have our claim. Moreover we realize that the elements of D mutually commute. For it is easily seen that each member of D induces a cycle map on each of the other members; hence we appeal to 2.2.2.

Let π and φ be as above, and let $\rho \in R_4$ as well. Also, assume that $\psi \in D$ commutes with ρ. Then $(\pi, \varphi, \psi, \rho)$ is a commuting path in Δ_{R_4}, because φ and ψ commute. Therefore $d_{\Delta_{R_4}}(\pi, \rho) \leq 3$, and so the diameter of Δ_{R_4} is at most 3.

Now consider the particular pair of elements $\sigma = (1\ 2)$ and $\tau = (1\ 3)$ of R_4. Suppose that $\chi \in S_4$ commutes σ and τ. Then by 2.2.2, χ induces a cycle map on σ, and likewise on τ. Thus χ maps the set $\{1, 2\}$ to itself, and the same goes for $\{1, 3\}$. It follows that $\{1, 2, 3\} \subseteq F(\chi)$. Hence χ induces a function on $\{1, 2, 3, 4\} \setminus \{1, 2, 3\}$; that is, $4 \in F(\chi)$. We conclude that χ is the identity element of S_4. Hence there is no commuting path of the form (σ, χ, τ) in $\Delta_{S_4^*}$. Therefore $d_{\Delta_{S_4^*}}(\sigma, \tau) \geq 3$, which implies that $d_{\Delta_{R_4}}(\sigma, \tau) \geq 3$. Thus, the diameter of Δ_{R_4} is at least 3. □

Lemma 2.3.3. *Suppose that $n > 4$, and let $\pi \in R_n$. Then π is a product of two disjoint cycles, each of length $n/2$, or π commutes with a nontrivial cycle of length $< n/2$. In any case, π commutes with a nontrivial cycle of length $\leq n/2$.*

Proof. First assume that π is itself a cycle. Then by the definition of R_n, π fixes at least two elements, say $a, b \in \{1, 2, \dots, n\}$. We observe that π commutes with $(a\ b)$, by 2.2.9. Also the length of $(a\ b)$, namely 2, is $< n/2$ because $n > 4$.

Now assume that π is neither a cycle, nor a product of two disjoint cycles of length $n/2$ each. Let γ be a nontrivial cycle of minimum length over the decomposition of π. Then the length of γ is obviously $< n/2$. And γ commutes with π, by 2.2.3.

Finally, if the decomposition of π consists of two disjoint cycles, each of length $n/2$, then by 2.2.3, π commutes with at least two nontrivial cycles of length $\leq n/2$. □

Proposition 2.3.4. *For $n > 4$, the diameter of Δ_{R_n} is ≤ 4.*

Proof. Let $\pi, \rho \in R_n$. First suppose that at least one of π and ρ, say π, commutes with a cycle $\gamma \in R_n$ of length $< n/2$. We observe that ρ commutes with a cycle $\delta \in R_n$ of length $\leq n/2$, by 2.3.3. If γ and δ are disjoint, on the one hand, then these cycles commute by 2.2.9. Thus $(\pi, \gamma, \delta, \rho)$ is a commuting path in Δ_{R_n}, and so $d_{\Delta_{R_n}}(\pi, \rho) \leq 3$. On the other hand if $M(\gamma) \cap M(\delta)$ is nonempty, then

$$|M(\gamma) \cup M(\delta)| \;\; \leq \;\; |M(\gamma)| + |M(\delta)| - 1 \;\; < \;\; 2(n/2) - 1 \;\; = \;\; n - 1.$$

Therefore $F(\gamma) \cap F(\delta)$ contains at least two elements, say a and b. We define $\sigma = (a \; b) \in R_n$, and observe that σ commutes with γ and δ by 2.2.9. Moreover, $(\pi, \gamma, \sigma, \delta, \rho)$ is a commuting path in Δ_{R_n}. Thus $d_{\Delta_{R_n}}(\pi, \rho) \leq 4$.

Now assume that neither π nor ρ commutes with a cycle of length $< n/2$. Then π is a product of two disjoint cycles, each of length $n/2$, by 2.3.3. Likewise, this is true of ρ. Assume that

$$\begin{aligned} \pi &= \left(a_1 \; a_2 \; \cdots \; a_{n/2}\right) \left(b_1 \; b_2 \; \cdots \; b_{n/2}\right), \\ \rho &= \left(c_1 \; c_2 \; \cdots \; c_{n/2}\right) \left(d_1 \; d_2 \; \cdots \; d_{n/2}\right). \end{aligned}$$

Since $M(\pi) = M(\rho) = \{1, 2, \ldots, n\}$, we may take $a_1 = c_1$. Therefore there exists $i \in \{1, 2, \ldots, n/2\}$ such that $b_i \notin \{c_j \,|\, 1 \leq j \leq n/2\}$. Hence $b_i \in \{d_j \,|\, 1 \leq j \leq n/2\}$, and thus we may suppose that $b_1 = d_1$. Let us define

$$\begin{aligned} \varphi &= (a_1\ b_1)(a_2\ b_2)\cdots(a_{n/2}\ b_{n/2}), \\ \tau &= (a_1\ b_1) \ = \ (c_1\ d_1), \\ \psi &= (c_1\ d_1)(c_2\ d_2)\cdots(c_{n/2}\ d_{n/2}). \end{aligned}$$

Then obviously φ, τ, and ψ are elements of R_n. Moreover we claim that $(\pi, \varphi, \tau, \psi, \rho)$ is a commuting path in Δ_{R_n}. We have

$$\begin{aligned} \big(\varphi(a_1)\ \varphi(a_2)\ \cdots\ \varphi(a_{n/2})\big) &= \big(b_1\ b_2\ \cdots\ b_{n/2}\big)\,, \\ \big(\varphi(b_1)\ \varphi(b_2)\ \cdots\ \varphi(b_{n/2})\big) &= \big(a_1\ a_2\ \cdots\ a_{n/2}\big)\,. \end{aligned}$$

Thus φ induces a cycle map on π; hence φ and π are commuting elements by 2.2.2. This similarly holds for ψ and ρ. And τ, being a cycle in the decomposition of both φ and ψ, commutes with each of these elements by 2.2.3. Therefore we have our claim; hence $d_{\Delta_{R_n}}(\pi, \rho) \leq 4$. And via our cases, we have now shown that this bound holds for a general pair $\pi, \rho \in R_n$. Thus we have the proposition. □

Proposition 2.3.5. *Suppose $n > 4$. Let m be the odd element of the set $\{n-1, n\}$, and define*

$$\pi \ = \ (1\ 2\ \cdots\ m-2)(m-1\ m) \in R_n, \quad \rho \ = \ (2\ 3\ \cdots\ m-1)(1\ m) \in R_n.$$

Then $d_{\Delta_{S_n^*}}(\pi, \rho) \geq 4$.

Proof. Suppose that $d_{\Delta_{S_n^*}}(\pi, \rho) \leq 3$. Let $(\pi, \varphi, \psi, \rho)$ be a commuting path in $\Delta_{S_n^*}$. We observe that $m \geq 5$; hence the cycles of π, including a trivial one if n is even, have distinct lengths. Therefore by 2.2.4, there exist positive integers r and s such that

$$\varphi \;=\; (1\ 2\ \cdots\ m-2)^r(m-1\ m)^s.$$

Similarly, there exist $t, u \in \mathbb{N}$ such that

$$\psi \;=\; (2\ 3\ \cdots\ m-1)^t(1\ m)^u.$$

We also note that φ and ψ are nontrivial, being elements of S_n^*. Moreover they are commuting elements, by our assumption that they appear consecutively in a commuting path.

Since $m-2$ is odd, the cycle decomposition of $(1\ 2\ \cdots\ m-2)^r$ does not contain a transposition. Therefore $(m-1\ m)$ is the only potential transposition among the cycles of φ. So, if $(m-1\ m)$ is a cycle of φ, then $(\psi(m-1)\ \psi(m)) = (m-1\ m)$ by 2.2.2. But clearly $\psi(m-1) \neq m$. Thus $m-1$ and m are fixed by ψ. However, this implies that ψ is the identity on all of $\{1, 2, \ldots, n\}$, contradicting that ψ is nontrivial. Hence $(m-1\ m)$ must not be a cycle of φ, and we therefore conclude that $m-1$ and m are fixed by φ. By a parallel argument, ψ fixes the elements 1 and m. Thus

$$\varphi \;=\; (1\ 2\ \cdots\ m-2)^r, \quad \psi \;=\; (2\ 3\ \cdots\ m-1)^t.$$

Now on the one hand, we observe that $\varphi(1) \in \{2, 3, \ldots, m-2\}$, because φ is nontrivial. On the other hand, since φ and ψ commute, and ψ^{-1} fixes 1, we have $\varphi(1) = (\psi\varphi\psi^{-1})(1) = \psi(\varphi(1))$. Therefore ψ fixes an element of $\{2, 3, \ldots, m-2\}$. But then $\psi = \mathrm{id}$, a contradiction. $\square$

We may now give an argument for **Theorem 2.3.1**.

Proof. We obtain the result by combining 2.3.2, 2.3.4, and 2.3.5. We note that 2.3.5 implies that π and ρ are at distance ≥ 4 in Δ_{R_n}, a subgraph of $\Delta_{S_n^*}$. □

2.4 The commuting graph $\Delta_{R_n \cup C_n^n}$ for even n

We shall prove that if n is even, the result of Theorem 2.3.1 applies to the larger graph $\Delta_{R_n \cup C_n^n}$.

Theorem 2.4.1. *Suppose that n is even, $n \geq 4$. Then $\Delta_{R_n \cup C_n^n}$ is connected. Moreover the diameter of the commuting graph is 3 or 4, according as $n = 4$ or $n > 4$.*

Once again, the theorem is realized through several propositions.

Proposition 2.4.2. *The diameter of $\Delta_{R_4 \cup C_4^4}$ is 3.*

Proof. From the proof of 2.3.2, we recall that D denotes the set of all double transpositions in S_4. In the proof we argued that Δ_{R_4} has diameter ≤ 3 through two observations. In particular, the elements of D mutually commute, and each element of R_4 commutes with an element of D. The second of these observations extends to include C_4^4. Indeed, given $\gamma = (a\ b\ c\ d) \in C_4^4$, we observe that γ commutes with $\gamma^2 = (a\ c)(b\ d) \in D$. Thus, as in the proof of 2.3.2, we conclude that $\Delta_{R_4 \cup C_4^4}$ has diameter ≤ 3.

Now, in demonstrating that the inequality of 2.3.2 is sharp, we defined $\sigma = (1\ 2)$ and $\tau = (2\ 3)$, elements of R_4, and argued that $d_{\Delta_{S_4^*}}(\sigma, \tau) \geq 3$. Thus the distance between σ and τ is ≥ 3 in $\Delta_{R_4 \cup C_4^4}$. We conclude that $\Delta_{R_4 \cup C_4^4}$ has diameter ≥ 3. □

Lemma 2.4.3. *Suppose that $n \geq 4$. Let $\pi \in R_n$ be a product of $i \geq 2$ disjoint nontrivial cycles of a common length. Let $\gamma \in R_n$ be a nontrivial cycle of length j, where $j \leq i$. Then there exists an element $\rho \in R_n$ that commutes with π and γ.*

Proof. We consider two possibilities. First assume that there exists a nontrivial cycle δ in the decomposition of π that is disjoint from γ. Then π and δ commute, by 2.2.3, and γ and δ commute as well, by 2.2.9. We observe that δ is an element of R_n, because its length is at most $n/i \leq n/2 \leq n-2$. Thus δ may serve as ρ.

Now let us assume that for each nontrivial cycle δ in the decomposition of π, $M(\gamma) \cap M(\delta)$ is nonempty. Then the number of nontrivial cycles of π does not exceed the length of γ. In other words $i \leq j$, and hence $i = j$, because the reverse inequality is being assumed. Let m denote the common length of the cycles of π, and suppose that in decomposed form we have

$$\pi \;=\; \prod_{k=0}^{i-1} \left(a_{k,0}\ a_{k,1}\ a_{k,2}\ \cdots\ a_{k,m-1}\right).$$

Also suppose that $\gamma = (b_0\ b_1\ b_2\ \cdots\ b_{i-1})$, and with no loss in generality, take $a_{k,0} = b_k$ for $0 \leq k < i$. Define

$$\rho \;=\; \prod_{l=0}^{m-1} \left(a_{0,l}\ a_{1,l}\ a_{2,l}\ \cdots\ a_{i-1,l}\right).$$

We observe that ρ is nontrivial, because $i \geq 2$, and not itself a cycle, because $m \geq 2$. Hence $\rho \in R_n$. Also, ρ commutes with $(a_{0,0}\ a_{1,0}\ a_{2,0}\ \cdots\ a_{i-1,0})$, one of its cycles, by 2.2.3. Thus ρ commutes with γ. Furthermore, for each $k \in \{0, 1, \ldots, i-1\}$, and each $l \in \{0, 1, \ldots, m-1\}$,

$$\begin{aligned} (\rho\pi)(a_{k,l}) &= \rho\left(a_{k,(l+1) \bmod m}\right) = a_{(k+1) \bmod i,\,(l+1) \bmod m}, \\ (\pi\rho)(a_{k,l}) &= \pi\left(a_{(k+1) \bmod i,\,l}\right) = a_{(k+1) \bmod i,\,(l+1) \bmod m}. \end{aligned}$$

Hence ρ commutes with π as well, because both of π and ρ fix each element of the set

$$\{1, 2, \ldots, n\} \setminus \{a_{k,l} \,|\, 0 \leq k < i,\ 0 \leq l < m\}. \qquad \square$$

Proposition 2.4.4. *Suppose that n is even, $n > 4$. Let $\pi \in R_n$, and $\gamma \in C_n^n$. Then the distance between π and γ in $\Delta_{R_n \cup C_n^n}$ is ≤ 4.*

Proof. Assume that $\gamma = (a_1\ a_2\ \cdots\ a_n)$. Since n is even, we have

$$\gamma^{n/2} = (a_1\ a_{n/2+1})(a_2\ a_{n/2+2})\ \cdots\ (a_{n/2}\ a_n) \in R_n.$$

We observe that γ commutes with $\gamma^{n/2}$, because a group element commutes with each of its powers. By 2.3.3, there exists a nontrivial cycle $\delta \in R_n$ of length $\leq n/2$ that commutes with π, because $\pi \in R_n$. Furthermore by 2.4.3, there exists $\rho \in R_n$ commuting with $\gamma^{n/2}$ and δ. Hence $\left(\pi, \delta, \rho, \gamma^{n/2}, \gamma\right)$ is a commuting path in $\Delta_{R_n \cup C_n^n}$. Therefore we have the proposition. $\square$

Lemma 2.4.5. *Suppose that n is even, and let $\pi \in S_n$ be a product of $n/2$ disjoint transpositions. Then the order of the centralizer of π in S_n is given by*

$$(n/2)! \cdot 2^{n/2} \;=\; (2)(4)(6)(8)\cdots(n).$$

Proof. In view of 2.2.2, we must show that the number of elements of S_n that induce a cycle map on π is $(n/2)! \cdot 2^{n/2}$. Suppose that we have the decomposition

$$\pi \;=\; (a_1\; b_1)(a_2\; b_2)\cdots(a_{n/2}\; b_{n/2}).$$

Consider a general element of S_n, written in table form as follows:

$$\rho \;=\; \begin{pmatrix} a_1 & b_1 & a_2 & b_2 & \cdots & a_{n/2} & b_{n/2} \\ x_1 & y_1 & x_2 & y_2 & \cdots & x_{n/2} & y_{n/2} \end{pmatrix}$$

We observe that ρ induces a cycle map on π if and only if

$$\big\{\{x_1, y_1\}, \{x_2, y_2\}, \ldots \{x_{n/2}, y_{n/2}\}\big\} \;=\; \big\{\{a_1, b_1\}, \{a_2, b_2\}, \ldots \{a_{n/2}, b_{n/2}\}\big\}\,.$$

To produce a table ρ that satisfies this condition, we may first arrange the sets $\{a_i, b_i\}$, $1 \leq i \leq n/2$, into a sequence, then arbitrarily order the pair of elements within each set. The number of ways to complete this process is

$$(n/2)! \cdot 2^{n/2} \;=\; (1\cdot 2)(2\cdot 2)(3\cdot 2)\cdots((n/2)\cdot 2) \;=\; (2)(4)(6)\cdots(n). \qquad \square$$

Proposition 2.4.6. *Suppose that n is even, $n > 4$. For $\gamma, \delta \in C_n^n$, the distance between γ and δ in $\Delta_{R_n \cup C_n^n}$ is ≤ 4.*

Proof. Let $\pi = \gamma^{n/2}$, and $\rho = \delta^{n/2}$. We observe that γ commutes with π, because a group element commutes with each of its powers. We also note that π is a product of $n/2$ disjoint transpositions, and in particular, $\pi \in R_n$. Likewise, δ commutes with $\rho \in R_n$, a product of $n/2$ disjoint transpositions. Let H and K be the centralizers of π and ρ in S_n, respectively. By a well-known result of finite group theory, we have

$$|HK| \;=\; \frac{|H| \cdot |K|}{|H \cap K|}\,. \tag{2.4.1}$$

(Refer to [4, p.39].) It is also well known that $|S_n| = n!$. (See [5, p.32].) Therefore $|HK| \leq n!$, because $HK \subseteq S_n$. But by 2.4.5,

$$|H| \cdot |K| \;=\; [(2)(4)(6) \cdots (n)]^2 \;>\; n!\,.$$

Hence $|H \cap K| > 1$. Let $\varphi \in (H \cap K) \setminus \{\text{id}\}$, and note that φ commutes with π and ρ. Suppose that $\varphi \in C_n^{n-1}$. Then $F(\varphi)$ contains precisely one element, say a. Therefore by 2.2.6, $a \in F(\pi) \cap F(\rho)$. However $F(\pi) = F(\rho) = \emptyset$, obviously. Thus $\varphi \notin C_n^{n-1}$, and so $\varphi \in R_n \cup C_n^n$. We now realize that $(\gamma, \pi, \varphi, \rho, \delta)$ is a commuting path in $\Delta_{R_n \cup C_n^n}$. The proposition follows. □

We may now provide an argument for **Theorem 2.4.1**.

Proof. The assertion for $n = 4$ is handled in Proposition 2.4.2. For $n > 4$ and n even, we combine the results of 2.3.4, 2.3.5, 2.4.4, and 2.4.6. □

We conclude the section by developing a second argument for Proposition 2.4.6, one which is more enlightening but also more technical. We shall illustrate the construction of a particular element φ, based on $\pi = \gamma^{n/2}$ and $\rho = \delta^{n/2}$. Especially noteworthy is that the element φ, like π and ρ, will be a product of $n/2$ disjoint transpositions.

Lemma 2.4.7. *Suppose that n is even, $n \geq 4$. Let $\pi, \rho \in S_n$. Furthermore assume that each of π and ρ is a product of $n/2$ disjoint transpositions. Then for all nonnegative integers j,*

$$F\left[\pi(\rho\pi)^j\right] \;=\; F\left[\rho(\pi\rho)^j\right] \;=\; \emptyset. \tag{2.4.2}$$

Proof. We proceed by induction on j. Clearly we have $F(\pi) = F(\rho) = \emptyset$, thus (2.4.2) holds for $j = 0$. Let j be a nonnegative integer, and inductively assume that (2.4.2) holds for this particular j. However, suppose that $F[\pi(\rho\pi)^{j+1}] \neq \emptyset$. Then there exists an element $a \in \{1, 2, \ldots, n\}$ such that $[\pi(\rho\pi)^{j+1}](a) = a$. We note that $\pi^{-1} = \pi$, because π is a product of disjoint transpositions. Therefore $[\rho(\pi\rho)^j](\pi(a)) = \pi(a)$, and hence $F[\rho(\pi\rho)^j]$ is nonempty. This is a contradiction. Thus $F[\pi(\rho\pi)^{j+1}] = \emptyset$. And by a parallel argument, $F[\rho(\pi\rho)^{j+1}] = \emptyset$. Hence we have the lemma, by induction. □

Lemma 2.4.8. *Let $n, \pi,$ and ρ be as in Lemma 2.4.7. Let H be the subgroup of S_n generated by π and ρ, and let $A \subseteq \{1, 2, \ldots, n\}$ be an orbit under the natural action of H on $\{1, 2, \ldots, n\}$. Then the elements of A may be arranged into a sequence $(x_0, x_1, \ldots, x_{2k-1})$ such that $\pi(x_{2j}) = x_{2j+1}$ and $\rho(x_{2j+1}) = x_{(2j+2) \bmod 2k}$ for $0 \leq j < k$. In particular, A has even order.*

Proof. Let x_0 be an arbitrary element of A. For each integer $j \in \mathbb{Z}$, we define

$$x_{2j} \;=\; (\rho\pi)^j(x_0), \quad x_{2j+1} = \left[\pi(\rho\pi)^j\right](x_0).$$

Then we have $x_{2j+1} = \pi(x_{2j})$, and $x_{2j+2} = (\rho\pi)(x_{2j}) = \rho(x_{2j+1})$. We note that each x_i is an element of $\{1, 2, \ldots, n\}$. Thus there exists a repeated value in the sequence $(x_0, x_1, x_2, \ldots)$. Let m be the minimum positive index such that x_m is an element of $\{x_0, x_1, \ldots, x_{m-1}\}$. In particular suppose that $x_m = x_l$, where $l \in \{0, 1, \ldots, m-1\}$.

We claim that m and l have the same parity. If l is even, say $l = 2i$, then for an arbitrary nonnegative integer j,

$$x_{l+2j+1} \;=\; \left[\pi(\rho\pi)^{i+j}\right](x_0) \;=\; \left[\pi(\rho\pi)^j(\rho\pi)^i\right](x_0) \;=\; \left[\pi(\rho\pi)^j\right](x_l).$$

And if $l = 2i + 1$,

$$x_{l+2j+1} \;=\; (\rho\pi)^{i+j+1}(x_0) \;=\; \left[\rho(\pi\rho)^j\pi(\rho\pi)^i\right](x_0) \;=\; \left[\rho(\pi\rho)^j\right](x_l).$$

But regardless of the parity of l, we see that $x_{l+2j+1} \neq x_l$, by 2.4.7. Thus we have our claim, because $x_m = x_l$. Assume that $m = l + 2k$, where k is a positive integer. Since $m - 1$ and $l - 1$ have the same parity, $x_m = \pi(x_{m-1})$ and $x_l = \pi(x_{l-1})$, or $x_m = \rho(x_{m-1})$ and $x_l = \rho(x_{l-1})$. Whichever the case, $x_{m-1} = x_{l-1}$, because π and ρ are injective. It follows that $l = 0$, because of the minimum condition that we imposed on m. Hence $m = 2k$.

Now for an arbitrary integer j, we have

$$x_{2j+2k} \;=\; (\rho\pi)^{j+k}(x_0) \;=\; (\rho\pi)^j(x_{2k}) \;=\; (\rho\pi)^j(x_0) \;=\; x_{2j}.$$

Therefore,

$$x_{(2j+1)+2k} \;=\; x_{2(j+k)+1} \;=\; \pi(x_{2j+2k}) \;=\; \pi(x_{2j}) \;=\; x_{2j+1}.$$

Hence the the function $i \mapsto x_i$, defined on $\mathbb{Z}$, has period $2k$.

We observe that $A = \{\varphi(x_0) \,|\, \varphi \in H\}$. Thus $\{x_i \,|\, i \in \mathbb{Z}\} \subseteq A$. We complete the proof by demonstrating the reverse inclusion. Let φ be an element of H. Then for some nonnegative integer t, there exist elements $\psi_s \in \{\pi, \pi^{-1}, \rho, \rho^{-1}\}$, $1 \le s \le t$, such that $\varphi = \psi_1\psi_2\psi_3 \cdots \psi_t$. (See [3, p.62].) However, $\pi^{-1} = \pi$, or equivalently $\pi^2 = \mathrm{id}$, because π is a product of disjoint transpositions. Likewise, $\rho^{-1} = \rho$. Thus by canceling successive factors of $\psi_1\psi_2\psi_3 \cdots \psi_t$ as long as possible, we obtain

$$\varphi \in \left\{(\rho\pi)^j,\ \pi(\rho\pi)^j,\ (\pi\rho)^j,\ \rho(\pi\rho)^j\right\},$$

for some nonnegative integer j. We have $(\rho\pi)^j(x_0) = x_{2j}$, and $\left[\pi(\rho\pi)^j\right](x_0) = x_{2j+1}$. Furthermore, we observe

$$\begin{aligned} (\pi\rho)^j(x_0) \;&=\; \left[\left(\rho^{-1}\pi^{-1}\right)^{-j}\right](x_0) \;=\; \left[(\rho\pi)^{-j}\right](x_0) \;=\; x_{-2j}, \\ \left[\rho(\pi\rho)^j\right](x_0) \;&=\; \left[\pi(\pi\rho)^{j+1}\right](x_0) \;=\; \pi(x_{-2(j+1)}) \;=\; x_{-2(j+1)+1}. \end{aligned}$$

Therefore $\varphi(x_0) \in \{x_i \,|\, i \in \mathbb{Z}\}$. We conclude that $A \subseteq \{x_i \,|\, i \in \mathbb{Z}\}$, as desired. □

Proposition 2.4.9. *Let n, π, and ρ be as in 2.4.7. Then there exists $\varphi \in S_n$, also a product of $n/2$ disjoint transpositions, commuting with π and ρ.*

Proof. Let H be the subgroup of S_n generated by π and ρ. Let A be an arbitrary orbit under the natural action of the subgroup H on $\{1, 2, \ldots, n\}$. Then each of the elements π and ρ maps A to itself, bijectively. Let π_A and ρ_A denote the restrictions of π and ρ to A, respectively. Let $(x_0, x_1, x_2, \ldots, x_{2k-1})$ be an arrangement of the elements of A, as in 2.4.8. For $0 \leq i < k$, define

$$\varphi_A(x_i) = x_{(2k-1)-i}, \quad \varphi_A(x_{(2k-1)-i}) = x_i.$$

Since π is a product of disjoint transpositions, and $\pi(x_{2j}) = x_{2j+1}$ for $0 \leq j < k$, by design, we see that

$$\pi_A \ = \ (x_0\ x_1)(x_2\ x_3)(x_4\ x_5)\ \cdots\ (x_{2k-2}\ x_{2k-1}).$$

Applying φ_A to the elements x_i within the respective transpositions here, we reverse the sequence of indices and obtain the product

$$(x_{2k-1}\ x_{2k-2})(x_{2k-3}\ x_{2k-4})(x_{2k-5}\ x_{2k-6})\ \cdots\ (x_1\ x_0) \ = \ \pi_A.$$

Hence φ_A induces a cycle map on π_A. Furthermore, defining $\varphi = \prod_A \varphi_A$, we realize that φ induces a cycle map on $\prod_A \pi_A = \pi$. Therefore φ and π are commuting elements, by 2.2.2.

Now, since ρ is a product of disjoint transpositions, and $\rho(x_{2j+1}) = x_{(2j+2) \bmod 2k}$, we have

$$\rho_A \ = \ (x_1\ x_2)(x_3\ x_4)(x_5\ x_6)\ \cdots\ (x_{2k-3}\ x_{2k-2})(x_{2k-1}\ x_0).$$

Applying φ_A to the respective x_i here yields

$$(x_{2k-2}\ x_{2k-3})(x_{2k-4}\ x_{2k-5})(x_{2k-6}\ x_{2k-7})\ \cdots\ (x_2\ x_1)(x_0\ x_{2k-1}) \ = \ \rho_A.$$

Therefore, we see that φ induces a cycle map on ρ, so φ and ρ are commuting elements, by 2.2.2. And φ is obviously a product of disjoint transpositions, fixing no element of $\{1, 2, \ldots, n\}$. Thus the proof is complete. □

We have now realized our goal of a more constructive route to Proposition 2.4.6. But furthermore, Proposition 2.4.9 yields a new proof of a result of [1, p.139].

Theorem 2.4.10. *Suppose that n is even, $n > 4$. Let X be the set of all products of $n/2$ disjoint transpositions in S_n. Then the commuting graph Δ_X has diameter 2.*

Proof. The diameter of Δ_X is ≤ 2 by 2.4.9. Define

$$\begin{aligned} \pi &= (1\ 2)(3\ 4)(5\ 6)\ \cdots\ (n-1\ n), \\ \rho &= (2\ 3)(4\ 5)(6\ 7)\ \cdots\ (n-2\ n-1)(1\ n), \end{aligned}$$

a particular pair of elements of X. We observe that $(\rho\pi)(1) = \rho(2) = 3$, while $(\pi\rho)(1) = \pi(n) = n - 1$. Therefore $(\rho\pi)(1) \neq (\pi\rho)(1)$, because $n > 4$. Hence π and ρ are not commuting elements. We conclude that the diameter of Δ_X is > 1. □

We remark that in the terminology of [1], Δ_X is referred to as a *commuting involution graph.*

2.5 An upper bound on the diameter of $\Delta_{S_n^*}$ for composite n and $n-1$

Theorem 2.5.1. *Suppose that each of n and $n-1$ is a composite number. Then the diameter $\Delta_{S_n^*}$ is ≤ 5.*

We remark that $n \geq 9$ here, implicitly. We obtain the theorem through two propositions, that shall accompany Theorem 2.3.1.

Proposition 2.5.2. *Suppose that $n > 4$, and $l \in \{n-1, n\}$ is a composite number. Let $\pi \in R_n$ and $\gamma \in C_n^l$. Then the distance between π and γ in $\Delta_{R_n \cup C_n^l}$ is ≤ 5.*

Proof. By 2.3.3, there exists a cycle $\delta \in R_n$ of length $\leq n/2$ that commutes with π. We have $|F(\delta)| \geq n/2$, thus $|F(\delta)| \geq 3$ because $n > 4$. Choose $a, b \in F(\delta)$, and define $\tau = (a\ b) \in R_n$. Then τ is disjoint from δ; hence τ and δ are commuting elements, by 2.2.9.

Now assume that $\gamma = (c_1\ c_2\ c_3\ \cdots\ c_l)$. Since l is composite, there exists a positive integer $i \in (1, l)$ that divides l. We observe that γ commutes with γ^i, because a group element commutes with each of its powers. In decomposed form, we have

$$\gamma^i = \prod_{j=1}^{i} \left(a_j\ a_{j+i}\ a_{j+2i}\ \cdots\ a_{j+[(l/i)-1]i}\right).$$

In particular, γ^i is a product of $i \geq 2$ disjoint cycles, each of length $l/i \geq 2$. Hence $\gamma^i \in R_n$. Moreover since τ is a cycle of length $\leq i$, there exists an element $\rho \in R_n$

commuting with γ^i and τ, by 2.4.3. Therefore, $(\pi, \delta, \tau, \rho, \gamma^i, \gamma)$ is a commuting path in $\Delta_{R_n \cup C_n^l}$. The proposition follows. $\square$

Proposition 2.5.3. *Let l and m be elements of the set $\{n-1, n\}$. Assume that $l \leq m$, and that each of l and m is a composite number. Let $\gamma \in C_n^l$, and $\delta \in C_n^m$. Then the distance between γ and δ in $\Delta_{R_n \cup C_n^l \cup C_n^m}$ is ≤ 5.*

Proof. Let $D_l \subseteq \{2, 3, \ldots, l-1\}$ be the set of all proper nontrivial divisors of l. Since l is composite, D_l is nonemtpy. Let $i = \max(D_l)$. Since $i \in D_l$, we have $l/i \in D_l$ as well. Therefore $l/i \leq i$, because i is maximal; so $\sqrt{l} \leq i$. Analogously, we let $D_m \subseteq \{2, 3, \ldots, m-1\}$ be the collection of all proper nontrivial divisors of m, nonempty because m is composite, and we let $j = \max(D_m)$. We then note that $m/j \in D_m$, and deduce that $\sqrt{m} \leq j$. Moreover we have $\sqrt{l} \leq j$, because $l \leq m$. Hence $l \leq ij$, and so $l/i \leq j$.

Now assume that

$$\gamma \;=\; (a_1\, a_2\, a_3\, \cdots\, a_l), \quad \delta \;=\; (b_1\, b_2\, b_3\, \cdots\, b_m).$$

Then we have, in decomposed form,

$$\begin{aligned} \gamma^i &= \prod_{k=1}^{i} \left(a_k\; a_{k+i}\; a_{k+2i}\; \cdots\; a_{k+[(l/i)-1]i}\right); \\ \delta^j &= \prod_{k=1}^{j} \left(b_k\; b_{k+j}\; b_{k+2j}\; \cdots\; b_{k+[(m/j)-1]j}\right). \end{aligned}$$

We observe that γ^i consists of i nontrivial cycles, each of length l/i, and δ^j consists of j nontrivial cycles, each of length m/j. So obviously, $\gamma^i, \delta^j \in R_n$. Let σ be any nontrivial cycle in the decomposition of γ^i. Then $\sigma \in R_n$, because γ^i has multiple nontrivial cycles. By 2.2.3, σ commutes with γ^i. Furthermore since $l/i \leq j$, there exists an element $\rho \in R_n$ that commutes with σ and δ^j, by 2.4.3. Hence $(\gamma, \gamma^i, \sigma, \rho, \delta^j, \delta)$ is a commuting path in $\Delta_{R_n \cup C_n^l \cup C_n^m}$, because γ and δ commute with γ^i and δ^j, respectively. Thus we have the proposition. □

We finish the section with an argument for **Theorem 2.5.1**.

Proof. As noted earlier, we have $n \geq 9$, because n and $n-1$ are composite numbers. The theorem is realized immediately by combining the results of Theorem 2.3.1, and Propositions 2.5.2 and 2.5.3. □

2.6 The existence of elements at distance 5 in $\Delta_{S_n^*}$

We exhibit two pairs of elements at distance ≥ 5 in the commuting graph $\Delta_{S_n^*}$. In each of our constructions, we shall require the following standard result.

Lemma 2.6.1. *Let G be a group. Suppose that $g \in G$ has finite order i. Then for all integers j, $\langle g^j \rangle = \left\langle g^{\gcd(i,j)} \right\rangle$.*

Proof. We observe that $\gcd(i,j)$ divides j; suppose $j = k \cdot \gcd(i,j)$, where $k \in \mathbb{Z}$. Then we have $g^j = \left(g^{\gcd(i,j)}\right)^k \in \left\langle g^{\gcd(i,j)} \right\rangle$. Thus $\langle g^j \rangle \subseteq \left\langle g^{\gcd(i,j)} \right\rangle$.

Now, by a well-known result of number theory, there exist integers x and y such that $ix + jy = \gcd(i,j)$. (See [4, p.11].) Therefore, $g^{\gcd(i,j)} = (g^i)^x (g^j)^y = (g^j)^y$, because g has order i. Hence $g^{\gcd(i,j)} \in \langle g^j \rangle$, and so $\left\langle g^{\gcd(i,j)} \right\rangle \subseteq \langle g^j \rangle$. □

Proposition 2.6.2. *Suppose that n is a positive integer, $n \geq 3$. Let*

$$\gamma \;=\; (1\,2\,3\,\cdots\,n-1) \in C_n^{n-1}, \quad \delta \;=\; (1\,2\,3\,\cdots\,n) \in C_n^n.$$

Then the distance between γ and δ in $\Delta_{S_n^*}$ is at least 5.

Proof. We note that γ and δ are in fact elements of S_n^*, because $n \geq 3$. Suppose that $d_{\Delta_{S_n^*}}(\gamma, \delta) \leq 4$. In particular, assume that $(\gamma, \varphi, \chi, \psi, \delta)$ is a commuting path in $\Delta_{S_n^*}$. Since φ and ψ commute with γ and δ, respectively, there exist positive integers s and t such that $\varphi = \gamma^s$ and $\psi = \delta^t$, by 2.2.4. Let $u = \gcd(s, n-1)$ and $v = \gcd(t, n)$; and note that u and v are proper divisors of $n-1$ and n, respectively, because φ and ψ are nontrivial elements. Let $\pi = \gamma^u$, $\rho = \delta^v$, and $H = \langle \pi, \rho \rangle$. By 2.6.1, we have $\langle \varphi \rangle = \langle \pi \rangle$ and $\langle \psi \rangle = \langle \rho \rangle$. Hence each subgroup of S_n that contains φ and ψ will also contain π and ρ, and vice-versa. Therefore, $H = \langle \varphi, \psi \rangle$.

We observe that precisely one of the integers $n-1$ and n is divisible by 2; so $u + v < (n-1)/2 + n/2$. Thus $u + v$, itself an integer, must be $\leq n - 1$. Let $m = \min(u, v)$, and let $a \in \{n-m, n-m+1, n-m+2, \ldots, n-1\}$. We observe that $n-1$ is strictly less than $a+u$ and $a+v$, but $a+u+v \leq 2(n-1)$. Therefore,

$$\begin{aligned}
(\rho\pi)(a) &= \rho[a+u-(n-1)] \;=\; a+u+v-(n-1), \\
(\pi\rho)(a+1) &= \pi[(a+1)+v-n] \;=\; \pi[a+v-(n-1)] \;=\; a+u+v-(n-1).
\end{aligned}$$

Thus $(\rho\pi)(a) = (\pi\rho)(a+1)$, and so $(\rho^{-1}\pi^{-1}\rho\pi)(a) = a+1$. Hence $a+1 \in [a]_H$, because $\rho^{-1}\pi^{-1}\rho\pi \in H$. Moreover $[a]_H = [a+1]_H$, by 2.2.11. Therefore, we conclude that

$$[n-m]_H \;=\; [n-m+1]_H \;=\; \cdots \;=\; [n-1]_H \;=\; [n]_H. \qquad (2.6.1)$$

Suppose that $b \in \{1, 2, \ldots, n-m-1\}$. We observe that $i = 0$ is a solution to $b + im < n - m$; thus there exists a maximum nonnegative integer i for which the inequality holds. For this i, we have

$$b + (i+1)m \in \{n-m, n-m+1, n-m+2, \ldots, n-1\}.$$

We observe that if $m = u$, then $\pi^{i+1}(b) = b + (i+1)m$. And if $m = v$, then $\rho^{i+1}(b) = b + (i+1)m$. Either way, we have $[b]_H = [b + (i+1)m]_H$, because each of π^{i+1} and ρ^{i+1} is an element of H. Together with (2.6.1), this implies that

$$[1]_H \;=\; [2]_H \;=\; \cdots \;=\; [n-1]_H \;=\; [n]_H.$$

Hence $[n]_H = \{1, 2, \ldots, n\}$.

Define $K = \langle \varphi, \chi, \psi \rangle$. Then K may be explicitly described as the set of all products of the form $\eta_1\eta_2 \cdots \eta_w$, where w is a positive integer, and each η_j is an element of $\{\varphi, \varphi^{-1}, \chi, \chi^{-1}, \psi, \psi^{-1}\}$. (See [3, p.62].) We recall that χ sits between φ and ψ in our commuting path; hence χ commutes with φ and ψ. Therefore χ commutes with φ^{-1} and ψ^{-1} as well. And of course χ commutes with itself and its inverse. Thus χ commutes with all products $\eta_1\eta_2 \cdots \eta_w$. In other words, χ is a member of the center of K.

Since $\varphi \in \langle \gamma \rangle \setminus \{\mathrm{id}\}$, we see that $F(\varphi) = \{n\}$. Therefore by 2.2.6, $n \in F(\chi)$, because φ and χ are commuting elements. Moreover since χ is an element of the center of K, we have $[n]_K \subseteq F(\chi)$, by 2.2.12. But H is a subgroup of K, because $H = \langle \varphi, \psi \rangle$ and $\varphi, \psi \in K$. Thus $[n]_H \subseteq [n]_K$, and so $[n]_K = \{1, 2, \ldots, n\}$. We conclude that $F(\chi) = \{1, 2, \ldots, n\}$, which implies that χ is the identity element of S_n. This is a contradiction. Hence we have the proposition. □

To prove the main result of the current chapter, we must still demonstrate the existence of a pair of elements at distance 5 in $\Delta_{R_n \cup C_n^{n-1}}$, when $n-1$ is composite. **For the remainder of the section, the following setup shall apply**.

- Let n be a positive integer such that $n-1$ is a composite number.
- Let M be the maximum proper divisor of $n-1$.
- Define the following elements of C_n^{n-1}:

$$\gamma = (1\ 2\ \cdots\ n-1); \tag{2.6.2}$$

$$\delta = (1\ 2\ \cdots\ M\ \ n\ \ M+1\ \ M+2\ \cdots\ n-2). \tag{2.6.3}$$

- Let p and q be arbitrary prime divisors of $n-1$, possibly alike.
- Let $r = (n-1)/p$, $s = (n-1)/q$, and $m = \min(r, s)$.
- Define $H = \langle \gamma^r, \delta^s \rangle$.

We note that $n \geq 5$, $M > 1$, and $m > 1$, because $n-1$ is composite. We also point out that r and s are proper divisors of $n-1$, hence $r, s \leq M$.

Lemma 2.6.3. *Suppose that a is an integer such that $M+1-m \leq a \leq M-2$. Then $[a]_H = [a+2]_H$.*

Proof. First assume that $r \leq s$. We observe that

$$M+1 \ \leq \ a+r \ \leq \ 2M-2 \ \leq \ n-3.$$

Let i be the maximum positive integer such that $M+1 \leq a+ir \leq n-2$. Then since $r \leq s$, we have $n-2 < a+ir+s \leq (n-2)+M$. Therefore

$$\left(\delta^s \gamma^{ir}\right)(a) \ = \ \delta^s(a+ir) \ = \ a+ir+s-(n-2).$$

But we have $M+1 \leq a+s \leq n-3$ as well, so

$$\left(\gamma^{ir} \delta^s\right)(a+2) \ = \ \gamma^{ir}(a+s+1) \ = \ a+ir+s+1-(n-1).$$

Hence $(\delta^s \gamma^{ir})(a) = (\gamma^{ir} \delta^s)(a+2)$, and thus $(\delta^{-s} \gamma^{-ir} \delta^s \gamma^{ir})(a) = a+2$. It follows that $[a]_H = [a+2]_H$, because $\delta^{-s} \gamma^{-ir} \delta^s \gamma^{ir} \in H$.

Now let us assume that $s < r$. Let j be the maximum positive integer such that $M+1 \leq a+js \leq n-3$. Then $n-2 < a+r+js \leq (n-3)+M$, because s is strictly less than r. Thus

$$\left(\gamma^r \delta^{js}\right)(a+2) \ = \ \gamma^r(a+js+1) \ = \ a+r+js+1-(n-1).$$

But on the other hand,

$$\left(\delta^{js} \gamma^r\right)(a) \ = \ \delta^{js}(a+r) \ = \ a+r+js-(n-2).$$

Thus $(\gamma^r \delta^{js})(a+2) = (\delta^{js} \gamma^r)(a)$. So once again, $[a]_H = [a+2]_H$. □

Lemma 2.6.4. *Suppose that a and b are integers such that $M - m + 1 \leq a, b \leq M$. Assume that a and b have opposite parity. Then $[a]_H \cup [b]_H = \{1, 2, \ldots, n\}$.*

Proof. Let i and j be the odd and even elements of the set $\{m-1, m\}$, respectively. Define

$$\begin{aligned} C &= \{M-m+1, M-m+3, M-m+5, \ldots, M-m+i\}, \\ D &= \{M-m+2, M-m+4, M-m+6, \ldots, M-m+j\}. \end{aligned}$$

We observe that $C \cup D = \{M-m+1, M-m+2, \ldots, M-1, M\}$, so $a, b \in C \cup D$. Also, either the elements of C are strictly even and those of D are strictly odd, or vice versa. Thus one of the elements a and b is a member of C, and the other is a member of D. But by 2.6.3,

$$\begin{aligned} [M-m+1]_H &= [M-m+3]_H = [M-m+5]_H = \cdots = [M-m+i]_H, \\ [M-m+2]_H &= [M-m+4]_H = [M-m+6]_H = \cdots = [M-m+j]_H. \end{aligned}$$

Therefore $C \cup D \subseteq [a]_H \cup [b]_H$.

Suppose $1 \leq x \leq M - m$. Let k be the maximum nonnegative integer such that $x + km \leq M - m$, and let $y = x + (k+1)m$. Then $y \in C \cup D$, because $C \cup D$ consists of m consecutive integers. We observe that $\gamma^{(k+1)m}(x) = \delta^{(k+1)m}(x) = y$. Also, if $m = r$ then $\gamma^{(k+1)m} = (\gamma^r)^{k+1} \in H$, and if $m = s$ then $\delta^{(k+1)m} = (\delta^s)^{k+1} \in H$. Therefore, $[x]_H = [y]_H$. But $y \in [a]_H$ or $y \in [b]_H$, because $y \in C \cup D$. Hence $x \in [a]_H$ or $x \in [b]_H$. In other words, $x \in [a]_H \cup [b]_H$.

Now assume that $M+1 \leq z \leq n-1$. Let l be the maximum nonnegative integer such that $z - lr \geq M+1$. Then $z-(l+1)r \in \{1,2,\ldots,M\}$, since $r \leq M$. And we have $\gamma^{-(l+1)r}(z) = z-(l+1)r$. Therefore $[z]_H = [z-(l+1)r]_H$, because $\gamma^{-(l+1)r} = (\gamma^r)^{-(l+1)} \in H$. But we have already shown that $\{1,2,\ldots,M\} \subseteq [a]_H \cup [b]_H$. Thus $z \in [a]_H \cup [b]_H$.

Finally, we observe that $\delta^{-s}(n) = M-s+1$. Hence $[n]_H = [M-s+1]_H$. Therefore $n \in [a]_H \cup [b]_H$, because $M-s+1 \in \{1,2,\ldots,M-1\} \subseteq [a]_H \cup [b]_H$. □

Proposition 2.6.5. *Suppose $p = 2$ or $q = 2$, but $p \neq q$. Then*

$$[n-1]_H \cup [n]_H = \{1,2,\ldots,n\}.$$

Proof. Since $2 \in \{p,q\}$, and p and q are divisors of $n-1$, we realize that $n-1$ is even. Therefore $M = (n-1)/2$.

Assume that $p = 2$. Then we have $r = M$ and $s = m$; thus $\gamma^r(n-1) = M$ and $\delta^{-s}(n) = M-m+1$. Therefore $[n-1]_H = [M]_H$, and $[n]_H = [M-m+1]_H$. Since $p \neq q$, q is an odd prime. Hence s is even, because $n-1$ is even, and so M and $M-m+1$ have opposite parity, because $s = m$. Thus by 2.6.4, we have $[M]_H \cup [M-m+1]_H = \{1,2,\ldots,n\}$, and therefore $[n-1]_H \cup [n]_H = \{1,2,\ldots,n\}$.

Now suppose that $q = 2$. Then by analogy to the above case, $r = m$ and $s = M$, and r is even. We observe that the set $\{M-m+1, M-m+2, \ldots, M\}$ consists of r consecutive integers. Therefore the set includes elements a and b such that $a \equiv 0 \pmod{r}$ and $b \equiv 1 \pmod{r}$. Let i and j be integers such that $a = ir$ and

$b = jr + 1$. Then $\gamma^{ir}(n-1) = a$, and $(\gamma^{jr}\delta^{-s})(n) = \gamma^{jr}(1) = b$, because $s = M$. Hence $[n-1]_H = [a]_H$, and $[n]_H = [b]_H$. But a and b have opposite parity, because r is even. Thus by 2.6.4 once again, we have $[n-1]_H \cup [n]_H = \{1, 2, \ldots, n\}$. □

We point out that $[n-1]_H \neq [n]_H$ is a possibility under the hypotheses of 2.6.5. For example if $n - 1 = 6$, then

$$\gamma \;=\; (1\ 2\ 3\ 4\ 5\ 6), \quad \delta \;=\; (1\ 2\ 3\ 7\ 4\ 5). \tag{2.6.4}$$

If $p = 2$ and $q = 3$, we have $r = 3$ and $s = 2$. Therefore $\gamma^r = (1\ 4)(2\ 5)(3\ 6)$, and $\delta^s = (1\ 3\ 4)(2\ 7\ 5)$. Thus

$$[6]_H = \{1, 3, 4, 6\}, \ \ [7]_H = \{2, 5, 7\}.$$

Definition 2.6.6. *If the natural action of H on $\{1, 2, \ldots, n\}$ has precisely one orbit, then we shall say that H is **transitive**.*

Proposition 2.6.7. *If $p = q = 2$, then H is transitive.*

Proof. We observe that $r = s = M = (n-1)/2$. Thus for $1 \leq a \leq M - 1$, we have

$$\left(\delta^{-s}\gamma^{r}\right)(a) \;=\; \left(\delta^{-M}\gamma^{M}\right)(a) \;=\; \delta^{-M}(a + M) \;=\; a + 1.$$

Therefore $[a]_H = [a+1]_H$, and furthermore, $[1]_H = [2]_H = \cdots = [M]_H$.

Now, for $M + 2 \leq a \leq n - 1$,

$$\left(\delta^{s}\gamma^{-r}\right)(a) \;=\; \delta^{M}(a - M) \;=\; a - 1.$$

Hence $[a]_H = [a-1]_H$, and so $[M+1]_H = [M+2]_H = \cdots = [n-1]_H$.

Finally, we notice that $\gamma^r(n-1) = M$, and $\delta^{-s}(n) = 1$. Therefore we have $[n-1]_H = [M]_H$, and $[n]_H = [1]_H$. So we conclude that

$$[1]_H = [2]_H = \cdots = [n-1]_H = [n]_H. \qquad \square$$

Lemma 2.6.8. *If each of r and s is $\leq n - M - 3$, then H is transitive.*

Proof. Let $a = M - m + 1$. Since $m \geq 2$, the set $\{M - m + 1, M - m + 2, \ldots, M\}$ contains at least two elements; thus $\{a, a+1\}$ is a subset. We point out that each of $a + r$ and $a + s$ is $\geq M + 1$, but that

$$a + r + s = M + \max(r, s) + 1 \leq M + (n - M - 3) + 1 = n - 2.$$

Therefore,

$$(\delta^s\gamma^r)(a) = \delta^s(a + r) = a + r + s,$$
$$(\gamma^r\delta^s)(a + 1) = \gamma^r(a + s) = a + r + s.$$

Hence $(\delta^{-s}\gamma^{-r}\delta^s\gamma^r)(a) = a + 1$, and so $[a]_H = [a + 1]_H$. But by 2.6.4, we have $[a]_H \cup [a + 1]_H = \{1, 2, \ldots, n\}$. Thus the lemma follows. $\square$

Proposition 2.6.9. *If $p \neq 2$ and $q \neq 2$, then H is transitive.*

Proof. We observe that $n-1$, being divisible by an odd prime, is not a power of 2. In the case of $n-1 = 6$ and $p = q = 3$, γ and δ are as in equation (2.6.4), and $r = s = 2$. Therefore $\gamma^r = (1\ 3\ 5)(2\ 4\ 6)$, and $\delta^s = (1\ 3\ 4)(2\ 7\ 5)$. Thus we obviously have

$$[1]_H = [3]_H = [5]_H, \ \ [2]_H = [4]_H = [6]_H; \ \ [1]_H = [3]_H = [4]_H, \ \ [2]_H = [7]_H = [5]_H.$$

Hence we see that $[1]_H = [2]_H = \cdots = [7]_H$, and so H is transitive.

For $n-1=9$, we have $p=q=r=s=M=3$. And for $n-1=10$, $p=q=M=5$ and $r=s=2$. But in either case, each of r and s is $< n-M-3$. Therefore H is transitive, by 2.6.8.

Now assume that $n-1 \geq 12$. Since p and q are both odd primes, each of r and s is $\leq (n-1)/3$. Therefore

$$M + \max(r,s) \;\leq\; \frac{n-1}{2} + \frac{n-1}{3} \;=\; n - \frac{n+5}{6} \;\leq\; n-3.$$

Thus by 2.6.8, H is transitive once again. □

In the proof of the culminating result of the current section, as follows, the prime numbers p and q that have been under consideration, and thus the group H, shall arise. In stating the proposition, we keep our assumptions that $n-1$ is composite, and M is the maximum proper divisor of $n-1$. The definitions of γ and δ, as in (2.6.2) and (2.6.3), remain as well. Our argument here revisits many of the techniques that we applied in the proof of 2.6.2.

Proposition 2.6.10. *The distance between γ and δ in $\Delta_{S_n^*}$ is at least 5.*

Proof. Suppose that the distance between γ and δ in $\Delta_{S_n^*}$ is ≤ 4. In particular, assume that $(\gamma, \varphi, \chi, \psi, \delta)$ is a commuting path in $\Delta_{S_n^*}$. Since φ and ψ commute with γ and δ, respectively, there exist positive integers t and u such that $\varphi = \gamma^t$ and $\psi = \delta^u$, by 2.2.4. We observe that $\gamma^{\gcd(t,n-1)} \in \langle\varphi\rangle$, and $\delta^{\gcd(u,n-1)} \in \langle\psi\rangle$, by 2.6.1. Also, $\gcd(t,n-1)$ and $\gcd(u,n-1)$ are proper divisors of $n-1$, because φ and ψ are nontrivial elements. Suppose that $n-1 = p\cdot j\cdot \gcd(t, n-1) = q\cdot k\cdot \gcd(u, n-1)$, where p and q are prime numbers, and j and k are positive integers. Since $\gamma^{\gcd(t,n-1)} \in \langle\varphi\rangle$, we have $\left(\gamma^{\gcd(t,n-1)}\right)^j = \gamma^{(n-1)/p} \in \langle\varphi\rangle$ as well. Similarly, $\delta^{(n-1)/q} \in \langle\psi\rangle$. And we note that $\gamma^{(n-1)/p}$ and $\delta^{(n-1)/q}$ are nontrivial elements, because each of $(n-1)/p$ and $(n-1)/q$ is strictly less than $n-1$.

Now given the structure of our commuting path, we see that χ commutes with φ and ψ. So furthermore, χ commutes with each element of $\langle\varphi\rangle$, and each of $\langle\psi\rangle$. Hence χ commutes with $\gamma^{(n-1)/p}$ and $\delta^{(n-1)/q}$.

Let us define

$$K = \left\langle \gamma^{(n-1)/p},\ \chi,\ \delta^{(n-1)/q} \right\rangle .$$

We observe that χ is a member of the center of K, as in the proof of 2.6.2. Also, by 2.2.6, $n-1$ and n are fixed by χ, because we obviously have $F\left(\gamma^{(n-1)/p}\right) = \{n\}$ and $F\left(\delta^{(n-1)/q}\right) = \{n-1\}$. Moreover we have $[n-1]_K \cup [n]_K \subseteq F(\chi)$, by 2.2.12. But letting $H = \left\langle \gamma^{(n-1)/p},\ \delta^{(n-1)/q}\right\rangle$, we realize that $[n-1]_H \cup [n]_H = \{1, 2, \ldots, n\}$, in view of Propositions 2.6.5, 2.6.7, and 2.6.9. Hence $[n-1]_K \cup [n]_K = \{1, 2, \ldots, n\}$, because H is a subgroup of K. We conclude that $F(\chi) = \{1, 2, \ldots, n\}$. In other words, χ is the identity element of S_n. This is a contradiction, so the proof is complete. $\square$

2.7 Proof of main result

In order to realize the main result of the current chapter, we prove one further proposition.

Proposition 2.7.1. *Suppose that $p \in \{n-1, n\}$ is a prime number. Let γ be an element of C_n^p. Then $\Delta_{\langle\gamma\rangle^*}$ is a connected component of $\Delta_{S_n^*}$. Furthermore, the diameter of $\Delta_{\langle\gamma\rangle^*}$ is 0 or 1, according as $p = 2$ or $p > 2$.*

Proof. We observe that $\langle\gamma\rangle$ is an abelian group, containing $p-1$ nontrivial elements. Thus we see that the diameter of $\Delta_{\langle\gamma\rangle^*}$ is equal to 0 if $p = 2$, but equal to 1 if $p > 2$.

Suppose that the connected component of γ in $\Delta_{S_n^*}$ strictly contains $\Delta_{\langle\gamma\rangle^*}$. Then there exists a commuting path (γ, π, ρ) in $\Delta_{S_n^*}$ such that γ and ρ are noncommuting elements. Since π commutes with γ, we have $\pi \in \langle\gamma\rangle$, by 2.2.4. Therefore the order of π is a divisor of p, the order of γ, by Lagrange's Theorem. (See [3, p.89].) Thus π has order p, because p is a prime and π is nontrivial. It follows that $\langle\pi\rangle = \langle\gamma\rangle$. Furthermore, we claim that π is itself a cycle of length p. We observe that if l is a positive integer, and $l \notin \{1, p\}$, then the decomposition of π cannot contain a cycle of length l, because the order of π is not divisible by l. Also, the decomposition of π cannot have two disjoint cycles of length p, since $2p > n$. Hence we have our claim. Therefore by 2.2.4, $\rho \in \langle\pi\rangle$, because ρ and π, being adjacent in our commuting path, are commuting elements. Thus $\rho \in \langle\gamma\rangle$. In particular, we conclude that ρ and γ are commuting elements, which is a contradiction. Thus we have the proposition. □

We may now give arguments to obtain **Theorem 2.1.2**.

Proof. We consider the three cases separately.

a. This follows at once from Theorem 2.5.1 and Proposition 2.6.2.

b. First consider the case of $n = 3$. We observe that $R_3 = \emptyset$, and

$$C_3^3 = \{(1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle^*.$$

Thus $\Delta_{R_3 \cup C_3^3}$ is a connected component of $\Delta_{S_3^*}$, of diameter 1, by 2.7.1. Also, for $\gamma \in C_3^2$, $\Delta_{\langle \gamma \rangle^*}$ is a component of $\Delta_{S_n^*}$ of diameter 0, by 2.7.1.

Regarding the $n = 4$ case, we observe that for each $\gamma \in C_4^3$, $\Delta_{\langle \gamma \rangle^*}$ is a connected component of $\Delta_{S_4^*}$, of diameter 1, by 2.7.1. And by 2.4.1, $\Delta_{R_4 \cup C_4^4}$ is connected of diameter 3. Thus we see that $\Delta_{R_4 \cup C_4^4}$ is a component of $\Delta_{S_4^*}$, in particular.

For $n > 4$, we note that n is even, because $n - 1$ is a prime. Therefore by 2.4.1 and 2.7.1, once again, we realize that the connected components of $\Delta_{S_n^*}$ are $\Delta_{R_n \cup C_n^n}$, of diameter 4, and $\Delta_{\langle \gamma \rangle^*}$ for $\gamma \in C_n^{n-1}$, each of diameter 1.

c. By 2.7.1, $\Delta_{\langle \gamma \rangle^*}$ is a connected component of $\Delta_{S_n^*}$, of diameter 1, for each $\gamma \in C_n^n$. We observe that $n - 1$ is even and > 2, because n is a prime and > 3. Hence $n - 1$ is composite. Therefore by 2.3.4, 2.5.2, 2.5.3, and 2.6.10, $\Delta_{R_n \cup C_n^{n-1}}$ is connected of diameter 5. Thus we see that $\Delta_{R_n \cup C_n^{n-1}}$ is a component of $\Delta_{S_n^*}$.

□

Chapter 3

A Diameter Bounding Result and Certain Solvable Groups

3.1 Summary

In this brief chapter, we develop an absolute bound for the commuting graphs Δ_{G^*} over a particular class of groups. We require a definition to precisely specify the class.

Definition 3.1.1. *Suppose n is an integer, $n \geq 3$. Let Q_{2^n} be the group with presentation $\left\langle x, y \,|\, x^{2^{n-1}} = 1,\; y^2 = x^{2^{n-2}},\; yx = x^{-1}y \right\rangle$. Then Q_{2^n} is called the **generalized quaternion group** of order 2^n.*

We remark that each element of Q_{2^n} may be reduced to the form $x^i y^j$, where $i \in \{0, 1, 2, \ldots, 2^{n-1}\}$ and $j \in \{0, 1\}$. Furthermore we see that if $x^{i_1}y^{j_1}$ and $x^{i_2}y^{j_2}$ have this form, then these products represent the same element if and only if $i_1 = i_2$ and $j_1 = j_2$. Thus Q_{2^n} does indeed have order 2^n. For more on generalized quaternion groups, we refer the reader to [10, pp.140–141].

The following theorem constitutes the primary result of the chapter.

Theorem 3.1.2. *Suppose that G is a finite group with a nontrivial abelian normal subgroup. Assume that G contains no cyclic or generalized quaternion Sylow subgroups. Then Δ_{G^*} is connected, of diameter ≤ 7.*

However, we take particular interest in a straightforward corollary, settling the question of connectivity for a significant collection of solvable groups.

Corollary 3.1.3. *Suppose that G is a nontrivial finite solvable group, with no cyclic or generalized quaternion Sylow subgroups. Then Δ_{G^*} is connected of diameter ≤ 7.*

3.2 Arguments

Lemma 3.2.1. *Let G be a finite group. Suppose that N and H are nontrivial abelian subgroups of G. Furthermore assume that N is normal in G, and H is noncyclic. Then there exist nontrivial commuting elements $w \in N^*$ and $h \in H^*$.*

Proof. Let p be a prime dividing the order of N, and let V be the set of all elements of N having order p, together with the identity element of N. We observe that V is nontrivial, by Cauchy's Theorem. (See [4, p.93].) Furthermore V is an abelian group, because N is an abelian group, and a product of commuting elements of order p yields an element of order dividing p. And in fact, V is normal in G. Indeed if $v \in V$, then for any $g \in G$ we have $gvg^{-1} \in N$, because $V \subseteq N$ and N is a normal subgroup of G. Hence $gvg^{-1} \in V$, because v and gvg^{-1} have the same order. Since V is abelian, we shall write its operation additively, when considered a group on its own. We observe that V is a left $\mathbb{Z}$-module in a natural way. In particular for a nonnegative integer n and $v \in V$, we define

$$n \times v \;=\; \underbrace{v + v + \cdots + v}_{n \text{ terms}},$$

where an empty sum is taken to be 0_V. And for $n < 0$, we let $n \times v = -[(-n) \times v]$.

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements, and for an arbitrary $n \in \mathbb{Z}$, let $[n]_p$ denote the coset of n in $\mathbb{F}_p$. Let $R = \mathbb{F}_p[H]$, the group ring of H over $\mathbb{F}_p$. (See [6, p.8].) We note the R is commutative, because H is abelian. For $v \in V$ and $\sum_{h \in H}[n_h]_p \cdot h \in R$, define

$$\left(\sum_{h \in H}[n_h]_p \cdot h\right) * v \;=\; \sum_{h \in H} n_h \times hvh^{-1}. \tag{3.2.1}$$

We point out that hvh^{-1} is an element of V, because V is normal in G and $H \subseteq G$. Moreover the formula of (3.2.1) is well defined, since each nontrivial element of V has order p, and $[n]_p = [m]_p$ implies that p divides $n - m$.

We claim that V is a left R-module under the product of (3.2.1). We have $1_R * v = v$ for all $v \in V$, because the identity element of H is also the identity of G. And it is easily checked that for integers n_h and m_h, $h \in H$, we have

$$\left(\sum_{h \in H}[n_h]_p \cdot h \;+\; \sum_{h \in H}[m_h]_p \cdot h\right) * v \;=\; \left(\sum_{h \in H}[n_h] \cdot h\right) * v \;+\; \left(\sum_{h \in H}[m_h] \cdot h\right) * v.$$

For $v_1, v_2 \in V$, we observe that $v_1 + v_2 = v_1 v_2$, because the operations of V and G coincide on V. Hence for $h \in H$, we have $h(v_1 + v_2)h^{-1} = hv_1h^{-1} + hv_2h^{-1}$, because each term is an element of V, and so we realize that

$$\left(\sum_{h \in H}[n_h]_p \cdot h\right) * (v_1 + v_2) \;=\; \left(\sum_{h \in H}[n_h]_p \cdot h\right) * v_1 \;+\; \left(\sum_{h \in H}[n_h]_p \cdot h\right) * v_2.$$

Finally, we have

$$\left(\sum_{g\in H}[n_g]_p \cdot g\right)\left[\left(\sum_{h\in H}[n_h]_p \cdot h\right) * v\right] \;=\; \left[\left(\sum_{g\in H}[n_g]_p \cdot g\right)\left(\sum_{h\in H}[n_h]_p \cdot h\right)\right] * v,$$

because each expression is equal to $\sum_{g,h\in H}\left[(n_g n_h) \times (gh)v(gh)^{-1}\right]$. Thus our claim is established.

Now since V is finite but nontrivial, there exists a minimal nontrivial submodule W of V, obviously. In other words, W is a simple R-module. Let E be the collection of all R-module endomorphisms of W, endowed with the operations of addition and multiplication defined as follows. For arbitrary elements $\varphi, \psi \in E$ and $w \in W$, let $(\varphi + \psi)(w) = \varphi(w) + \psi(w)$ and $(\varphi\psi)(w) = \varphi(\psi(w))$. Then by Schur's Lemma, E is a division ring under these operations. (Refer to [6, p.35].) Furthermore E is finite, because $W \subseteq G$ and G is finite. Therefore E is a field, by Wedderburn's "Little" Theorem. (See [6, p.214].) Hence the multiplicative group $E^{\#}$ is cyclic (cf. [4, p.279]).

For $h \in H$, define $\varphi_h : W \to W$ via the rule $\varphi_h(w) = ([1]_p \cdot h) * w = hwh^{-1}$, for all $w \in W$. We observe that if $x \in W$ as well, then

$$\varphi_h(w + x) \;=\; hwh^{-1} + hxh^{-1} \;=\; \varphi_h(w) + \varphi_h(x).$$

And for $\sum_{g\in H}[n_g]_p \cdot g \in R$, we have

$$\varphi_h\left[\left(\sum_{g\in H}[n_g]_p \cdot g\right) * w\right] \;=\; \sum_{g\in H} n_g \times (hg)w(hg)^{-1} \;=\; \left(\sum_{g\in H}[n_g]_p \cdot g\right) * \varphi_h(w),$$

because R is commutative. Therefore $\varphi_h \in E$. Moreover φ_h is injective, because $hwh^{-1} = hxh^{-1}$ implies $w = x$. Thus $\varphi_h \not\equiv 0_W$, and so $\varphi_h \in E^{\#}$.

Define $\Phi : H \to E^{\#}$ by $\Phi(h) = \varphi_h$, for all $h \in H$. We observe that if g is an element of H as well, and $w \in W$, then

$$\varphi_{gh}(w) \;=\; (gh)w(gh)^{-1} \;=\; g\left(hwh^{-1}\right)g^{-1} \;=\; (\varphi_g\varphi_h)(w).$$

Hence $\Phi(gh) = \Phi(g)\Phi(h)$. Therefore Φ is a group homomorphism, and so $\Phi(H)$ is a subgroup of $E^{\#}$. Furthermore $\Phi(H)$ must be cyclic, because $E^{\#}$ is cyclic, and a subgroup of a cyclic group is cyclic. (See [4, p.36].) But H is assumed to be noncyclic. Thus $\Phi(H)$ cannot be isomorphic to H, and so Φ has a nontrivial kernel. In other words, there exists a nontrivial element $h \in H^*$ such that φ_h is the identity map on W. Equivalently $hwh^{-1} = w$, or h and w are commuting elements, for all $w \in W$. Hence we have the lemma, because $W \subseteq N$ is nontrivial. □

Definition 3.2.2. *Let G be a group, and let p be a prime number. If the order of each element of G is a power of p, then G is called a p-**group**.*

We remark that $p^0 = 1$ counts as a power of p in this definition. We also note that a group G is a p-group if and only if the order of G is a power of p. This is a consequence of the theorems of Lagrange and Cauchy. (See [4, p.39 and p.93].)

We shall require two results concerning p-groups. The first is well known, and will be applied frequently; the second is more technical. We refer the reader to the literature for their arguments.

Lemma 3.2.3. *If G is a finite p-group then its center, $Z(G)$, is a nontrivial p-group.*

Proof. See [4, p.94]. □

Lemma 3.2.4. *Let G be a finite p-group. Then G has a unique subgroup of order p if and only if G is cyclic, or a generalized quaternion group.*

Proof. See [10, p.143]. □

Definition 3.2.5. *Let G be a group, and let p be a prime number. If H is a maximal p-subgroup of G, then H is called a **Sylow** p-**subgroup**.*

We note that for a finite group G of order $p^a m$, where $\gcd(p, m) = 1$, H is a Sylow p-subgroup of G if and only if H has order p^a. Furthermore, the total number of Sylow p-subgroups is $\equiv (1 \bmod p)$, and any two are conjugate, thus isomorphic. (See [4, p.95].)

We are now prepared to give an argument for **Theorem 3.1.2**.

Proof. Let N be a nontrivial abelian normal subgroup of G. Let g_1 and g_2 be arbitrary nontrivial elements of G, and let i_1 and i_2 be the orders of g_1 and g_2, respectively. Assume that $i_1 = j_1 p_1$ and $i_2 = j_2 p_2$, where j_1 and j_2 are positive integers, and p_1 and p_2 are prime numbers. We observe that for each $k \in \{1, 2\}$, the cyclic group $\left\langle g_k^{j_k} \right\rangle$ has order p_k, and thus is a p_k-subgroup of G. Let P_k be a Sylow p_k-subgroup of G containing $\left\langle g_k^{j_k} \right\rangle$. Since P_k has prime power order $p_k^{a_k}$ for some $a_k \geq 1$, $Z(P_k)$ is a nontrivial p_k-group, by 3.2.3. Let $z_k \in Z(P_k)^*$ be an element of order p_k. By hypothesis, P_k is neither a cyclic group, nor a generalized quaternion group. Thus by 3.2.4, P_k has more than one subgroup of order p_k. Hence there exists $x_k \in P_k \setminus \langle z_k \rangle$ of order p_k.

For fixed $k \in \{1,2\}$, consider two possibilities regarding $g_k^{j_k}$. First assume that $g_k^{j_k} \in \langle z_k \rangle$. Then we have $x_k \notin \langle g_k^{j_k} \rangle$. And x_k and $g_k^{j_k}$ are commuting elements, because $x_k \in P_k$ and $g_k^{j_k} \in Z(P_k)$. Therefore letting $H_k = \langle x_k \rangle \cdot \langle g_k^{j_k} \rangle$, we see that $H_k \simeq (\mathbb{Z}/p_k\mathbb{Z}) \times (\mathbb{Z}/p_k\mathbb{Z})$. In particular, H_k is a noncyclic abelian subgroup of G. Thus by 3.2.1, there exist nontrivial commuting elements $h_k \in H_k^*$ and $w_k \in N^*$. Furthermore we realize that $\left(g_k, g_k^{j_k}, h_k, w_k\right)$ is a commuting path in Δ_{G^*}, because g_k commutes with $g_k^{j_k}$, of course, and each of $g_k^{j_k}$ and h_k is an element of the abelian group H_k.

Now assume $g_k^{j_k} \notin \langle z_k \rangle$. Then $g_k^{j_k}$ and z_k generate distinct groups of order p_k. Moreover these elements commute, because $g_k^{j_k} \in P_k$ and $z_k \in Z(P_k)$. We therefore define $H_k = \langle g_k^{j_k} \rangle \cdot \langle z_k \rangle$, and observe that H_k is a noncyclic abelian subgroup of G, once again. So as above, there exist $h_k \in H_k^*$ and $w_k \in N^*$ such that $\left(g_k, g_k^{j_k}, h_k, w_k\right)$ is a commuting path in Δ_{G^*}.

Affixing our commuting paths for $k = 1$ and $k = 2$ to one another, with the $k = 2$ path on the right side and written in reverse, we obtain a new path in Δ_{G^*}, because each of w_1 and w_2 is an element of the abelian group N. In particular, the path is $\left(g_1, g_1^{j_1}, h_1, w_1, w_2, h_2, g_2^{j_2}, g_2\right)$. Therefore in view of the length of this path, the theorem is realized. □

Before giving a proof of Corollary 3.1.3, we prove a fact from group theory.

Lemma 3.2.6. *Let G be a group with derived series $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots$. Then each G_i is a normal subgroup of G.*

Proof. Let $\varphi : G \to G$ be an arbitrary homomorphism. We claim that $\varphi(G_i) \subseteq G_i$ for all $i \geq 0$. We prove this by induction on i. The claim is obviously true for $i = 0$. So assume that it holds for some particular $i \geq 0$. Since G_{i+1} is the derived subgroup of G_i, a general element of G_{i+1} may be expressed as a product of commutators, $\prod_{j=1}^{k} [g_j, h_j]$, where $g_j, h_j \in G_i$ for $1 \leq j \leq k$. We observe that

$$\varphi\left(\prod_{j=1}^{k} [g_j, h_j]\right) = \prod_{j=1}^{k} \left(\varphi(g_j)\varphi(h_j)\varphi(g_j)^{-1}\varphi(h_j)^{-1}\right) = \prod_{j=1}^{k} [\varphi(g_j), \varphi(h_j)] .$$

But by assumption, we have $\varphi(G_i) \subseteq G_i$. Thus $\varphi(g_j), \varphi(h_j) \in G_i$ for each j, and so $\prod_{j=1}^{k} [\varphi(g_j), \varphi(h_j)] \in G_{i+1}$. Therefore the claim holds for $i+1$, and hence for all nonnegative integers, by induction.

Now let $x \in G$, and define $\varphi_x : G \to G$ via the formula $\varphi_x(y) = xyx^{-1}$ for all $y \in G$. Then φ_x is a homomorphism. (In fact, φ_x is the 'inner automorphism of G induced by x'. See [4, pp.90–91].) Thus $\varphi_x(G_i) \subseteq G_i$ for all $i \geq 0$, by our above argument. The lemma follows. □

We end the chapter with an argument for **Corollary 3.1.3**.

Proof. Let $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_{i-1} \supsetneq G_i = \{1_G\}$ be the derived series of the nontrivial finite solvable group G. We observe that the subgroup G_{i-1}, obviously nontrivial, is abelian, because its commutator subgroup is trivial. Furthermore, G_{i-1} is a normal subgroup of G, by Lemma 3.2.6. Therefore since G has no cyclic or generalized quaternion Sylow subgroups, by hypothesis, we realize the corollary by applying Theorem 3.1.2. □

Chapter 4

Groups of Order $p^a q^b$

4.1 Main results

Definition 4.1.1. *Let p and q be distinct prime numbers, and let G be a group of order $p^a q^b$, where a and b are positive integers. We define $M(G)$ to be the subset of all elements of G whose order is divisible by both p and q. For $r \in \{p, q\}$, we let $\mathcal{S}_r(G)$ denote the family of all Sylow r-subgroups of G. We also define $I_r(G) = \bigcap_{R \in \mathcal{S}_r(G)} R$, and $U_r(G) = \bigcup_{R \in \mathcal{S}_r(G)} R^*$.*

Informally, $M(G)$ is the collection of elements of *mixed order* in G. We observe that each $g \in G \setminus M(G)$ is either a p- or a q-element, as implied by Lagrange's Theorem. (See [3, p.89].) In other words for some $r \in \{p, q\}$, the order of g is a power of r. We also note that each such g is contained in some $R \in \mathcal{S}_r(G)$. (See [4, p.94].) Hence $G^* \setminus M(G) = U_p(G) \cup U_q(G)$. Finally we point out that $I_r(G)$ is an r-subgroup of G, possibly trivial, because an arbitrary intersection of subgroups of G remains a subgroup, and each $R \in \mathcal{S}_r(G)$ is an r-group. (See [3, p.61].)

We shall prove the following structure results for Δ_{G^*}, and the group G itself.

Throughout the chapter, we assume that G is a group as in Definition 4.1.1, but furthermore we take $p^a > q^b$. We remark that $p^a = q^b$ is impossible, because $\mathbb{Z}$ is a unique factorization domain. (See [3, p.287].)

Theorem 4.1.2. *The commuting graph Δ_{G^*} is connected if and only if $M(G)$ is nonempty. Moreover if Δ_{G^*} is connected, then its diameter is ≤ 7.*

Theorem 4.1.3. *Suppose $M(G) = \emptyset$. Then:*

a. *The order of $\mathcal{S}_p(G)$ is equal to 1 or q^b. Moreover if $|\mathcal{S}_p(G)| = q^b$, then none of the elements $P \in \mathcal{S}_p(G)$ is a cyclic or generalized quaternion group. Also for distinct $P, P' \in \mathcal{S}_p(G)$, $P \cap P' = I_p(G)$, which is a nontrivial p-group.*

b. *The order of $\mathcal{S}_q(G)$ is equal to $|I_p(G)|$. Furthermore, each $Q \in \mathcal{S}_q(G)$ is a cyclic or generalized quaternion group, and more precisely, Q is cyclic if $|\mathcal{S}_p(G)| > 1$. In any case, for each distinct pair of elements $Q, Q' \in \mathcal{S}_q(G)$, $Q \cap Q'$ is trivial.*

c. *If $|\mathcal{S}_p(G)| > 1$, there exists a subgroup H of G such that $G \supsetneq H \supsetneq I_p(G)$ is a normal series. Furthermore, G/H is a cyclic p-group, and $H/I_p(G)$ is a cyclic q-group.*

d. *The connected components of Δ_{G^*} are $\Delta_{U_p(G)}$, and Δ_{Q^*} for $Q \in \mathcal{S}_q(G)$. Moreover $\Delta_{U_p(G)}$ has diameter ≤ 2 if $|\mathcal{S}_p(G)| = 1$, but otherwise its diameter is exactly 3. The diameter of each Δ_{Q^*} is 1 or 2, according as Q is a cyclic or generalized quaternion group, unless $q^b = 2$, in which case the diameter is 0. In particular the diameter of Δ_{Q^*} is either 0 or 1 if $|\mathcal{S}_p(G)| > 1$.*

4.2 The commuting graph Δ_{G^*} if $M(G)$ is nonempty

Our objective here is to prove

Proposition 4.2.1. *Suppose that $M(G) \neq \emptyset$. Also assume that for some $r \in \{p, q\}$, each $R \in \mathcal{S}_r(G)$ is a cyclic or generalized quaternion group. Then Δ_{G^*} is connected of diameter ≤ 6.*

We remark that, with no regard to $M(G)$, G is a solvable group by Burnside's Theorem. (See [3, p.621].) Thus if G has no cyclic or generalized quaternion Sylow subgroups, then Δ_{G^*} is connected of diameter ≤ 7 by Corollary 3.1.3. So as a consequence of Theorem 4.1.2, we shall realize that $M(G)$ is automatically nonempty in this situation. But here, assuming $M(G) \neq \emptyset$ and the opposite condition on the Sylow subgroups of G, we prove a slightly sharper bound on the diameter of Δ_{G^*}.

We give several lemmas before the proof of 4.2.1. We remark that $M(G)$ is only assumed to be nonempty when this is explicitly stated. In our arguments, we shall make use of the following notation.

Definition 4.2.2. *Suppose $r \in \{p, q\}$. If $g \in G$ has order ir, where i is a positive integer, we define $g_r = g^i$. If g is an r-element, moreover, then we let $S_r(g)$ be any fixed group of $\mathcal{S}_r(G)$ that contains g. For an arbitrary $R \in \mathcal{S}_r(G)$, we define z_R to be any particular element of $Z(R)$ of order r.*

We note that the element g_r has order r, clearly, and thus is an r-element. We also point out that if g is itself an r-element, then of course there exists a maximal

r-subgroup of G that contains g. In other words, there exists a group of $\mathcal{S}_r(G)$ containing g. Finally we remark that if $R \in \mathcal{S}_r(G)$, then $Z(R)$ is a nontrivial r-group by Lemma 3.2.3. Choosing any $z \in Z(R)^*$, we may let z_r serve as z_R.

Lemma 4.2.3. *Suppose g and g' are elements of $M(G) \cup U_p(G)$. Then the distance between g and g' in $\Delta_{M(G) \cup U_p(G)}$ is ≤ 6.*

Proof. We note that $M(G) \cup U_p(G)$ is the set of all elements of G with order divisible by p. Thus g and g' are as such. Let $P = S_p(g_p)$, and $P' = S_p(g'_p)$. Since $p^a > q^b$ by assumption, equation (2.4.1) gives

$$|PP'| = \frac{|P| \cdot |P'|}{|P \cap P'|} = \frac{(p^a)^2}{|P \cap P'|} > \frac{|G|}{|P \cap P'|}.$$

But $|PP'| \leq |G|$, because $PP' \subseteq G$. Hence $P \cap P'$ is nontrivial, and so there exists $x \in (P \cap P')^*$.

We observe that z_P, a central element of P by definition, commutes with g_p and x. Similarly, $z_{P'}$ commutes with g'_p and x. Therefore, since g_p and g'_p obviously commute with g and g', respectively, we realize that $\big(g, g_p, z_P, x, z_{P'}, g'_p, g'\big)$ is a commuting path in $\Delta_{M(G) \cup U_p(G)}$. □

Lemma 4.2.4. *Suppose that $M(G) \neq \emptyset$. Let $P \in \mathcal{S}_p(G)$ and $Q \in \mathcal{S}_q(G)$. Then there exist nontrivial commuting elements $x \in P^*$ and $y \in Q^*$.*

Proof. Let $w \in M(G)$. We observe that w_p and w_q, nontrivial p- and q-elements respectively, commute because each is a member of the abelian group $\langle w \rangle$. Let us define $P' = S_p(w_p)$, and $Q' = S_p(w_q)$. Since all Sylow p-subgroups of G are conjugate, there exists $u \in G$ such that $uP'u^{-1} = P$. (Refer to [4, p.95].) Similarly, there exists $v \in G$ such that $vQ'v^{-1} = Q$.

Now, p^a and q^b are relatively prime integers, because p and q are distinct primes. Therefore $P' \cap Q'$, a subgroup of both P' and Q', is trivial, because its order divides $|P'| = p^a$ and $|Q'| = q^b$ by Lagrange's Theorem. (See [4, p.32 and p.39].) Thus by equation (2.4.1), we have $|P'Q'| = |P'| \cdot |Q'| = p^a q^b = |G|$. Hence $P'Q'$, which is a subset of G, must coincide with G.

Since $u, v \in G$ and G is a group, we have $u^{-1}v \in G$. Select $s \in P'$ and $t \in Q'$ such that $st = u^{-1}v$. Define $g = us = vt^{-1}$. Then

$$gP'g^{-1} = uP'u^{-1} = P, \quad gQ'g^{-1} = vQ'v^{-1} = Q,$$

because obviously $sP's^{-1} = P'$ and $t^{-1}Q't = Q'$. Let $x = gw_pg^{-1}$, and $y = gw_qg^{-1}$. We note that $x \in P$ and $y \in Q$, because $w_p \in P'$ and $w_q \in Q'$. Furthermore x and y are nontrivial commuting elements, because w_p and w_q are as such, and conjugation by g induces an automorphism of G. (See [4, p.90].) Hence we have the lemma. □

In what follows, we denote the *centralizer* of an element $g \in G$ by $C_G(g)$.

Lemma 4.2.5. *Suppose that $r \in \{p, q\}$, and $R \in \mathcal{S}_r(G)$ is a cyclic or generalized quaternion group. Then $C_G(z_R) = \bigcup_{y \in R^*} C_G(y)$.*

Proof. We observe that $\langle z_R \rangle$ is a subgroup of R of order r. Thus by Lemma 3.2.4, $\langle z_R \rangle$ is unique with this property. Let $y \in R^*$, and assume that $w \in G$ commutes with y. Since $\langle y_r \rangle$ is a subgroup of R of order r, we have $\langle z_R \rangle = \langle y_r \rangle$. So z_R may be realized as a power of y, and hence we see that w commutes with z_R. Thus $C_G(z_R) \supseteq \bigcup_{y \in R^*} C_G(y)$. On the other hand, the reverse containment is immediate, because $z_R \in R^*$. □

We now proceed to the argument for **Proposition 4.2.1**.

Proof. Let g and g' be arbitrary elements of G^*. If $g, g' \in M(G) \cup U_p(G)$, then the distance between these elements in Δ_{G^*} is ≤ 6 by Lemma 4.2.3.

If $g \in M(G) \cup U_p(G)$ and $g' \in U_q(G)$, let $P = S_p(g_p)$ and $Q' = S_q(g')$. Also let $x \in P^*$ and $y' \in (Q')^*$ be commuting elements as in Lemma 4.2.4. We observe that z_P, a central element of P, commutes with g_p and x. Similarly $z_{Q'}$ commutes with g' and y'. Thus $(g, g_p, z_P, x, y', z_{Q'}, g')$ is a commuting path in Δ_{G^*}.

If $g, g' \in U_q(G)$, let $Q = S_q(g)$, and take Q' as above. Also let P be an arbitrary group of $\mathcal{S}_p(G)$. Furthermore in view of 4.2.4, let $x \in P^*$ and $y \in Q^*$ be commuting elements, and likewise for $x' \in P^*$ and $y' \in (Q')^*$. On the one hand if P is a cyclic or generalized quaternion group, then by Lemma 4.2.5, z_P commutes with each of y and y'. Hence $(g, z_Q, y, z_P, y', z_{Q'}, g')$ is a commuting path in Δ_{G^*}. On the other hand if each of Q and Q' is a cyclic or generalized quaternion group, then z_Q commutes with x, and $z_{Q'}$ with x', again by 4.2.5. Therefore $(g, z_Q, x, z_P, x', z_{Q'}, g')$ is a path in Δ_{G^*}.

We now see that in any case, the distance between g and g' in Δ_{G^*} is ≤ 6. Thus we have the proposition. □

4.3 The structure of G and Δ_{G^*} if $M(G)$ is empty

In this section, we shall ultimately prove Theorem 4.1.3. In what follows, **we assume that $M(G)$ empty**.

Lemma 4.3.1. *Suppose that x and y are nontrivial p- and q-elements of G, respectively. Then $C_G(x)$ is a p-group, and $C_G(y)$ is a q-group. Furthermore, x and y do not commute.*

Proof. Assume that $C_G(x)$ contains a nontrivial q-element w. Then the order of xw is the least common multiple of those of x and w, because x and w commute. (Refer to [3, p.156].) However the order of x is obviously divisible by p, while that of y is divisible by q. Therefore the least common multiple of the pair of orders is divisible by p and q. Hence xw has mixed order, contradicting that $M(G)$ is empty. It follows that $C_G(x)$ is a p-group, and by analogy, $C_G(y)$ is a q-group. In particular, we observe that $x \notin C_G(y)$. □

Lemma 4.3.2. *Suppose that $r_1 = p$ and $r_2 = q$, or vice versa. Assume that x is a nontrivial r_1-element of G, and R_2 is an r_2-subgroup of G. Then the function $y \mapsto yxy^{-1}$, mapping R_2 to G, is injective. Furthermore, if R_1 is a nontrivial normal r_1-subgroup of G, then $|R_2| \leq |R_1^*|$.*

Proof. Suppose y and y' are distinct elements of R_2 such that $yxy^{-1} = (y')\,x\,(y')^{-1}$. Then $(y')^{-1}\,y$ commutes with x. But $(y')^{-1}\,y \in R_2$, because $y, y' \in R_2$ and R_2 is a group. Thus $(y')^{-1}\,y$ is an r_2-element of G. Moreover $(y')^{-1}\,y$ is nontrivial, because

y and y' are distinct. Hence we have contradicted Lemma 4.3.1, and so we conclude that $y \mapsto yxy^{-1}$ is injective.

Now assuming that $x \in R_1$, we have $yxy^{-1} \in R_1$ for all $y \in R_2$, because R_1 is normal in G. Moreover yxy^{-1} is a nontrivial element, since x is nontrivial. Therefore $|R_2| \leq |R_1^*|$, because $y \mapsto yxy^{-1}$ is injective. □

Lemma 4.3.3. *There exists a nontrivial abelian normal p-subgroup N of G.*

Proof. As we have previously noted, G is solvable by Burnside's Theorem. (Again see [3, p.621].) Let $G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_{i-1} \supsetneq G_i = \{1_G\}$ be the derived series of G, and let $N = G_{i-1}$. As in the proof of Corollary 3.1.3, N is an abelian normal subgroup of G. We claim that N is a p-group, moreover. If the order of N is divisible by both p and q, then N contains nontrivial p- and q-elements x and y, by Cauchy's Theorem. (See [4, p.93].) Moreover x and y commute, because N is abelian. However, this contradicts Lemma 4.3.1.

Now assume that N is a q-group, and let P be an arbitrary member of $\mathcal{S}_p(G)$. Then by Lemma 4.3.2, we have $|P| \leq |N^*|$, because N is also normal in G. However N, like any q-subgroup of G, has order $\leq q^b$. (Refer to [4, pp.94–95].) Therefore $|N| < p^a$, because $q^b < p^a$ by assumption. But $|P| = p^a$; so we have a contradiction once again. Hence we have realized our claim, that N is a p-group. □

Lemma 4.3.4. *Suppose that $r \in \{p, q\}$, and R is an r-group. Furthermore assume that R is neither a cyclic nor a generalized quaternion group. Then R contains a noncyclic abelian subgroup H.*

Proof. We observe that $\langle z_R \rangle$ is a subgroup of R of order r, by the definition of z_R. In view of 3.2.4, let $\langle y \rangle$ be another such subgroup, distinct from $\langle z_R \rangle$. Since z_R is central in R, y and z_R commute. Therefore H, which we define to be $\langle y \rangle \cdot \langle z_R \rangle$, is an abelian subgroup of R. (See [3, p.62].) Now $\langle y \rangle \cap \langle z_R \rangle$ is a proper subgroup of each of $\langle y \rangle$ and $\langle z_R \rangle$, because an intersection of groups remains a group, and $\langle y \rangle \neq \langle z_R \rangle$. (See [3, p.61].) Therefore the order of $\langle y \rangle \cap \langle z_R \rangle$ is a proper divisor of r, the order of $\langle y \rangle$ and $\langle z_R \rangle$ alike, by Lagrange's Theorem. Hence $\langle y \rangle \cap \langle z_R \rangle$ is trivial, because r is a prime. So equation (2.4.1) implies $|H| = |\langle y \rangle| \cdot |\langle z_R \rangle| = r^2$. But for $i, j \in \mathbb{Z}$, $\left(y^i z_R^j\right)^r = (y^r)^i \left(z_R^r\right)^j = 1_R$, since y and z commute. Thus H is noncyclic. □

Lemma 4.3.5. *Each $Q \in \mathcal{S}_q(G)$ is either a cyclic or generalized quaternion group. Accordingly Δ_{Q^*} is a connected component of Δ_{G^*} of diameter 1 or 2, unless $q^b = 2$, in which case the diameter is 0.*

Proof. Assume that $Q \in \mathcal{S}_q(G)$ is neither a cyclic nor a generalized quaternion group. Then by Lemma 4.3.4, Q contains a noncyclic abelian subgroup H. Letting N be as in Lemma 4.3.3, we observe that there exist nontrivial commuting elements $x \in N^*$ and $y \in H^*$, by Lemma 3.2.1. But N is a p-group, and H is a q-group; therefore x is a p-element and y is a q-element. Thus we have contradicted Lemma 4.3.1. Hence we conclude that Q is a cyclic or generalized quaternion group.

On the one hand if Q is cyclic, then Q is abelian, and hence Δ_{Q^*} is connected of diameter 0 or 1 according as $q^b = 2$ or $q^b > 2$. On the other hand if Q is a generalized quaternion group, then Q is non-abelian; for example $yx = x^{-1}y = \left(x^{2^{n-1}-1}\right) y \neq xy$, because $2^{n-1} > 2$ for $n \geq 3$. (See Definition 3.1.1.) Hence Δ_{Q^*} has diameter > 1. But given any elements $y, y' \in Q^*$, we recall that z_Q is defined to be a nontrivial central element of Q, and we observe that (y, z_Q, y') is a commuting path in Δ_{Q^*}. Therefore Δ_{Q^*} is connected of diameter 2.

Now suppose that Δ_{Q^*} is not a connected component of Δ_{G^*}. Then there exist commuting elements $u \in Q^*$ and $t \in G \setminus Q$. By Lemma 4.2.5, z_Q commutes with t as well. Therefore $C_G(z_Q) \supsetneq Q$, because z_Q is a central element of Q. Hence $C_G(z_Q)$ is not a q-group, since Q is a maximal q-subgroup of G. So once again, we have contradicted Lemma 4.3.1. Therefore, the proof is complete. □

Lemma 4.3.6. *If $|\mathcal{S}_p(G)| = 1$, then $|\mathcal{S}_q(G)| = p^a$. Moreover, any distinct pair of Sylow q-subgroups of G has a trivial intersection.*

Proof. By Sylow theory, the number of Sylow q-subgroups of G is a divisor of p^a. (Refer to [3, p.141].) Suppose $|\mathcal{S}_q(G)| = p^e$, where e is a positive integer $\leq a$. Then we have $|U_q(G)| \leq p^e\left(q^b - 1\right)$, with equality if and only if any distinct pair of elements of $\mathcal{S}_q(G)$ has a trivial intersection. But $|U_p(G)| = p^a - 1$, because $|\mathcal{S}_p(G)| = 1$ by hypothesis. Therefore,

$$|G| \;\leq\; p^a + p^e\left(q^b - 1\right) = p^e\left(p^{a-e} + q^b - 1\right), \tag{4.3.1}$$

because $M(G)$ is assumed to be empty. Hence $p^{a-e}q^b \leq p^{a-e} + q^b - 1$, which implies that $p^{a-e}\left(q^b - 1\right) \leq q^b - 1$. Thus we have $a = e$. Furthermore, $|U_q(G)| = p^e\left(q^b - 1\right)$, because the inequality of (4.3.1) is saturated. Therefore, each distinct pair of Sylow

q-subgroups of G has a trivial intersection. $\square$

Lemma 4.3.7. *Assume that $P \in \mathcal{S}_p(G)$ is a cyclic or generalized quaternion group. Then P is normal in G, and in fact P is cyclic. Moreover each $Q \in \mathcal{S}_q(G)$ is cyclic.*

Proof. In the proof of Lemma 4.3.5, we showed that if $Q \in \mathcal{S}_q(G)$ is a cyclic or generalized quaternion group, then Δ_{Q^*} is a connected component of Δ_{G^*}. The same argument applies to P here. Supposing that $P' \in \mathcal{S}_p(G) \setminus \{P\}$, let $g \in P^*$, and $g' \in P' \setminus P$. Then by Lemma 4.2.3, g and g' are in the same connected component of Δ_{G^*}. However, this contradicts that Δ_{P^*} is itself a component of Δ_{G^*}. Therefore $\mathcal{S}_p(G) = \{P\}$, or in other words, P is a normal subgroup of G. (See [4, p.95].)

We observe that $\langle z_P \rangle$ is a subgroup of P of order p, by the definition of z_P. Moreover by Lemma 3.2.4, $\langle z_P \rangle$ is unique with this property. But we observe that for $x \in G$, $x\langle z_P \rangle x^{-1}$ is a subgroup of P of order p, because P is normal in G and conjugation by a fixed element induces an automorphism of G. (See [4, p.90].) Therefore $x\langle z_P \rangle x^{-1} = \langle z_P \rangle$, and so $\langle z_P \rangle$ is a normal subgroup of G. Thus for a fixed $Q \in \mathcal{S}_q(G)$, we have $|Q| \leq p - 1$ by Lemma 4.3.2. Since Q is nontrivial, it follows that $p \neq 2$. Therefore P is not a generalized quaternion group, and so P is cyclic in view of our hypothesis. Let us assume that $P = \langle x \rangle$, where $x \in P$ has order p^a.

Now let $y \in Q$. Since P is normal in G, we have $yxy^{-1} \in P$. And yxy^{-1} is nontrivial, because x is nontrivial. Thus there exists $e(y) \in \{1, 2, \ldots, p^a - 1\}$ such that $yxy^{-1} = x^{e(y)}$. Furthermore, the map $y \mapsto e(y)$ is injective on Q, because this is true of $y \mapsto yxy^{-1}$ by Lemma 4.3.2. Letting y' be an element of Q as well, we observe

$$x^{e(yy')} = (yy')\,x\,(yy')^{-1} = yx^{e(y')}y^{-1} = \prod_{i=1}^{e(y')} yxy^{-1} = \prod_{i=1}^{e(y')} x^{e(y)} = x^{e(y)e(y')}.$$

Likewise $x^{e(y'y)} = x^{e(y)e(y')}$; hence $x^{e(yy')} = x^{e(y'y)}$. And we observe that if i and j are distinct elements of $\{1, 2, \ldots, p^a - 1\}$, then x^i and x^j are distinct; for otherwise, assuming $i < j$, we must conclude that x has order $\leq j - i$. Thus $e\,(yy') = e\,(y'y)$, and so $yy' = y'y$ because e is injective. It follows that Q is abelian, and in particular, Q is not a generalized quaternion group. (See the proof of 4.3.5.) Therefore Q is cyclic, in view of the result of Lemma 4.3.5. □

We now give arguments for **Theorem 4.1.3**, organized into two separate proofs. Our first deals with the structure of G, the second with Δ_{G^*}. We begin with assertions **a–c of 4.1.3**, regarding the group G.

Proof. First assume that $|\mathcal{S}_p(G)| = 1$. Then by Lemma 4.3.6, $|\mathcal{S}_q(G)| = p^a = |I_p(G)|$, and each distinct pair of Sylow q-subgroups of G has a trivial intersection. Furthermore, any element $Q \in \mathcal{S}_q(G)$ is a cyclic or generalized quaternion group, by Lemma 4.3.5.

Now assume that $|\mathcal{S}_p(G)| > 1$. It is well known that $I_p(G)$, itself a normal p-subgroup of G, contains every such subgroup of G. (See [3, p.149].) Assume that $|I_p(G)| = p^e$, where e is a nonnegative integer, and let us define $\overline{G} = G/I_p(G)$. Then $\overline{G}$ is a group of order $p^{a-e}q^b$ (cf. [4, p.42]), and we observe that $a > e$ because $|\mathcal{S}_p(G)| > 1$. Therefore $\overline{G}$ has order divisible by p and q. But we claim that $\overline{G}$ has no elements of mixed order. Suppose that $x \in G$ has order i, and note that i is a power of p or q, because $M(G) = \emptyset$. Since $x^i \in I_p(G)$, there exists a minimum positive integer j such that $x^j \in I_p(G)$. Let k be the order of x^j. Then obviously we have $i = jk$; hence j is a power of p or q. But j is also the order of the coset $x \cdot I_p(G) \in \overline{G}$. Thus we have the claim.

Suppose $p^{a-e} > q^b$. Then by Lemma 4.3.3, $\overline{G}$ has a nontrivial normal p-subgroup $\overline{N}$. Moreover, $\overline{N}$ clearly takes the form $N/I_p(G)$, where N is a normal subgroup of G that strictly contains $I_p(G)$. And we observe that N is itself a p-group, because $\overline{N}$ and $I_p(G)$ are as such, and $|N| = |I_p(G)| \cdot |\overline{N}|$. (Again refer to [4, p.42]). But this contradicts the maximality of $I_p(G)$, as specified above. Therefore $p^{a-e} < q^b$, since equality is impossible, and so $e > 0$ because $p^a > q^b$. Hence $I_p(G)$ is nontrivial.

Fix $Q \in \mathcal{S}_q(G)$, and define $H = I_p(G) \cdot Q$. Since $I_p(G)$ is a normal subgroup of G, H is a subgroup of G containing both $I_p(G)$ and Q. (See [3, p.94].) We observe that the subgroup $I_p(G) \cap Q$, of $I_p(G)$ and Q alike, is trivial by Lagrange's Theorem, because $|I_p(G)| = p^e$ and $|Q| = q^b$ are relatively prime. Therefore H has order $p^e q^b$, by equation (2.4.1). And we have $p^e > q^b$, by Lemma 4.3.2 with $R_1 = I_p(G)$ and $R_2 = Q$.

Now $H/I_p(G)$ is isomorphic to Q, by the diamond isomorphism theorem, because $I_p(G) \cap Q$ is trivial. (See [3, p.97].) In particular, $|H/I_p(G)| = |Q| = q^b$. Thus we see that $H/I_p(G)$ is a Sylow q-subgroup of $\overline{G}$, because $|\overline{G}| = p^{a-e}q^b$. But Q, and hence $H/I_p(G)$, is a cyclic or generalized quaternion group by Lemma 4.3.5. So furthermore by Lemma 4.3.7, with the roles of p and q reversed because $p^{a-e} < q^b$, $H/I_p(G)$ is cyclic and normal in $\overline{G}$; thus Q is cyclic. Moreover each Sylow p-subgroup of $\overline{G}$ is cyclic.

Since $H/I_p(G)$ is normal in $\overline{G}$, H is obviously a normal subgroup of G. Therefore since H contains Q, and all Sylow q-subgroups of G are conjugate (cf. [4, p.95]), H contains each Sylow q-subgroup of G. On the other hand we observe that $I_p(G)$ is a Sylow p-subgroup of H, because $H/I_p(G)$ is a q-group. Furthermore $I_p(G)$ is normal in H, since normal in G. Thus $\mathcal{S}_p(H) = \{I_p(G)\}$. Therefore by Lemma 4.3.6, the number of Sylow q-subgroups of H, and hence of G, is $p^e = |I_p(G)|$. Also, each distinct pair of elements of $\mathcal{S}_q(G)$ has a trivial intersection.

The fact that $|\mathcal{S}_q\left(\overline{G}\right)| = 1$ also implies $\left|\mathcal{S}_p\left(\overline{G}\right)\right| = q^b$, in view of Lemma 4.3.6 once again. Furthermore each distinct pair of Sylow p-subgroups of $\overline{G}$ has a trivial intersection. But obviously $\mathcal{S}_p\left(\overline{G}\right) = \{P/I_p(G) \,|\, P \in \mathcal{S}_p(G)\}$. Thus $|\mathcal{S}_p(G)| = q^b$ as well, but the intersection of each distinct pair of elements of $\mathcal{S}_p(G)$ is $I_p(G)$. In particular we point out that $|\mathcal{S}_p(G)| > 1$, so no member of $\mathcal{S}_p(G)$ is a cyclic or generalized quaternion group, by Lemma 4.3.7.

For a fixed $P \in \mathcal{S}_p(G)$, we observe that $P/I_p(G)$ is a cyclic group, because $P/I_p(G) \in \mathcal{S}_p\left(\overline{G}\right)$. We claim that $\varphi : x \cdot I_p(G) \mapsto x \cdot H$ is an isomorphism of $P/I_p(G)$ with G/H. Since $I_p(G)$ is a subgroup of H, φ is well defined. And φ is multiplicative, by the definition of coset multiplication in a quotient group. Suppose that $\varphi\left(x \cdot I_p(G)\right) = \varphi\left(x' \cdot I_p(G)\right)$ for some $x, x' \in P$. Then we have $\left(x'\right)^{-1} x \in H$, and of course $(x')^{-1}x \in P$. But $H \cap P = I_p(G)$, because $I_p(G)$ is a Sylow p-subgroup of H. Thus $x \cdot I_p(G) = x' \cdot I_p(G)$, so it follows that φ is injective. Therefore we have the claim, because $|P/I_p(G)| = |G/H| = p^{a-e}$. We conclude that G/H is a cyclic p-group. □

We finally give our argument for **Theorem 4.1.3, part d**, concerning Δ_{G^*}.

Proof. Suppose $\mathcal{S}_p(G) = \{P\}$. Then $\Delta_{U_p(G)} = \Delta_{P^*}$, which has diameter ≤ 2 because P has a nontrivial center by Lemma 3.2.3. In particular, given any pair of elements $x, x' \in P^*$, (x, z_P, x') is a commuting path in Δ_{P^*}. On the other hand for each $Q \in \mathcal{S}_q(G)$, Δ_{Q^*} is connected component of Δ_{G^*} by Lemma 4.3.5; hence Δ_{P^*} must be a connected component as well. Moreover each Q is a cyclic or generalized quaternion group, with the diameter of Δ_{Q^*} being 1 or 2 accordingly, unless $q^b = 2$, where we have diameter 0.

Now assume that $|\mathcal{S}_p(G)| > 1$. Then each $Q \in \mathcal{S}_q(G)$ is cyclic, as shown in the proof above; thus Δ_{Q^*}, which remains a connected component of Δ_{G^*}, has diameter 0 or 1. Regarding $\Delta_{U_p(G)}$, let P_1 and P_2 be distinct elements of $\mathcal{S}_p(G)$. For $i \in \{1, 2\}$, select $x_i \in P_i \setminus I_p(G)$, and suppose that there exists a p-element y commuting with each x_i. Then by 4.3.1, $C_G(y)$ is a p-group; hence there exists $P \in \mathcal{S}_p(G)$ containing $C_G(y)$. In particular, P contains x_1 and x_2. Thus $P \cap P_1 \nsubseteq I_p(G)$, and $P \cap P_2 \nsubseteq I_p(G)$. It follows that $P = P_1$ and $P = P_2$, since each distinct pair of Sylow p-subgroups of G has intersection $I_p(G)$, as established in the earlier proof. But this contradicts that $P_1 \neq P_2$. Therefore $d_{U_p(G)}(x_1, x_2) \geq 3$, and so the diameter of $\Delta_{U_p(G)}$ is ≥ 3.

For the reverse inequality, let N be a nontrivial abelian normal p-subgroup of G, as in Lemma 4.3.3. Also let x_1 and x_2 be arbitrary nontrivial p-elements of G, and let $P_1, P_2 \in \mathcal{S}_p(G)$ contain x_1 and x_2 respectively. Since N is normal in G, and any conjugate of a nontrivial element remains nontrivial, each P_i acts on N^* by conjugation. We point out that the index of any subgroup of P_i is a power of p, because P_i is a p-group. So likewise, the number of elements of any orbit under the action of P_i is a power of p. (See [4, p.89].) But $|N^*| = |N| - 1$ is not divisible by p, because N is a p-group. Hence the action of P_i yields a singleton orbit, say $\{z_i\}$. Therefore z_i commutes with each element of P_i, and in particular with x_i. We observe that z_1 and z_2 themselves commute, because N is abelian. Moreover z_1 and z_2, as members of N^*, are nontrivial p-elements. Thus (x_1, z_1, z_2, x_2) is a commuting path in $\Delta_{U_p(G)}$. We conclude that $\Delta_{U_p(G)}$ has diameter ≤ 3, and furthermore $\Delta_{U_p(G)}$ is a connected component of Δ_{G^*}, because each Δ_{Q^*} is as such. □

4.4 Examples

In this section we exhibit a pair of constructions, each yielding a group of order $p^a q^b$ with no elements of mixed order.

Example 4.4.1. Let p be an odd prime, let q be any prime divisor of $p-1$, and let n be an arbitrary element of $\{2, 3, \ldots, q\}$. Define $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements, and define

$$P = \{(a_{ij}) \in GL_n(\mathbb{F}_p) \mid a_{ij} = 0 \text{ for } i < j, \text{ and } a_{ii} = 1 \text{ for } 1 \leq i \leq n\}.$$

Then P is obviously a group, and we have $|P| = p^s$, where $s = 1 + 2 + \cdots + (n-1)$. Hence, P is a p-group.

By Cauchy's Theorem, the multiplicative group $F_p^{\#}$, of order $p-1$, has an element ζ of order q. Let

$$Q = \left\langle \text{diag}\left(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\right)\right\rangle \subseteq P.$$

We observe that Q acts on P by conjugation, and thus we may form the semidirect product $P \rtimes Q$. Let G denote this group, of order $p^s q$.

Suppose that G contains an element (C_1, D_1) of order divisible by p and q. Taking appropriate powers of (C_1, D_1), we obtain a commuting pair of elements (C_2, D_2) and (C_3, D_3) having respective orders p and q. Define

$$\tilde{P} = \{(A, \text{id}_n) \mid A \in P\}, \quad \tilde{Q} = \{(\text{id}_n, B) \mid B \in Q\}.$$

Obviously $\tilde{P}$ and $\tilde{Q}$ are subgroups of G, and in fact $\tilde{P} \in \mathcal{S}_p(G)$ and $\tilde{Q} \in \mathcal{S}_q(G)$, in view of their orders. Furthermore $\tilde{P}$ is normal in G, clearly; therefore $(C_2, D_2) \in \tilde{P}$. And since all Sylow q-subgroups of G are conjugate, we may take $(C_3, D_3) \in \tilde{Q}$. Assume that $(C_2, D_2) = (A, \text{id}_n)$ and $(C_3, D_3) = (\text{id}_n, B)$, where $A \in P$ and $B \in Q$. We note that A and B have orders p and q, respectively, so in particular these elements are nontrivial. We observe

$$\begin{aligned}(C_2, D_2) \cdot (C_3, D_3) &= (A, B),\\ (C_3, D_3) \cdot (C_2, D_2) &= (BAB^{-1}, B).\end{aligned}$$

Therefore $A = BAB^{-1}$, because (C_2, D_2) and (C_3, D_3) are commuting elements.

Since B is a nontrivial element of Q, we have $B = \operatorname{diag}(1, \zeta^e, \zeta^{2e}, \ldots, \zeta^{(n-1)e})$ for some $e \in \{1, 2, \ldots, q-1\}$. Thus

$$\left(BAB^{-1}\right)_{ij} = \zeta^{(i-1)e} \cdot a_{ij} \cdot \zeta^{-(j-1)e} = \zeta^{(i-j)e} \cdot a_{ij}.$$

Since A is nontrivial, there exist $i, j \in \{1, 2, \ldots, n\}$, $i > j$, such that $a_{ij} \neq 0$. Hence $\zeta^{(i-j)e} = 1$, because $A = BAB^{-1}$. It follows that q divides $(i-j)e$, since ζ has order q. Thus q divides $i - j$ or e, because q is a prime. But q does not divide e, clearly, and furthermore q does not divide $i - j$, because $1 \leq i - j < n \leq q$. Therefore we have a contradiction, and so G has no elements of mixed order. □

We remark that the above example generalizes to the case where q is replaced by q^b, provided that q^b is a divisor of $p - 1$ and q remains $> n$. However the existence of an element $\zeta \in \mathbb{F}_p^{\#}$ of order q^b is not implied by Cauchy's Theorem in this situation. We may instead cite the fact that $\mathbb{F}_p^{\#}$ is cyclic, as is well known.

Example 4.4.2. For a positive integer n, let Q denote the cyclic or generalized quaternion group of order 2^n. (If $n \in \{1, 2\}$, we take Q to be cyclic.) Referring to 3.2.3 and 3.2.4, let z_Q denote the unique element of Q of order 2, and note that

$z_Q \in Z(Q)$. Let p be an odd prime, and let R denote the group ring $\mathbb{F}_p[Q]$, of order p^{2^n}. Define

$$V = \left\{ s \in R \mid s + \left(1_{\mathbb{F}_p} \cdot z_Q\right) s = 0_R \right\}$$

We observe that $1_{\mathbb{F}_p} \cdot 1_Q + \left(-1_{\mathbb{F}_p}\right) \cdot z_Q \in V$, because z_Q has order 2. Moreover, V is obviously closed under addition; therefore V is a nontrivial additive p-group, say of order p^m. We also observe that $g \in Q$ and $s \in V$ implies $\left(1_{\mathbb{F}_p} \cdot g\right) s \in V$, because g commutes with z_Q. Thus Q acts on V.

Let G denote the semidirect product $V \rtimes Q$, of order $p^m 2^n$. Suppose G contains an element of mixed order, divisible by p and 2. Then arguing as in the previous example, we realize that there exists $s \in V$ of order p and $g \in Q$ of order 2 such that $(s, 1_Q)$ and $(0_V, g)$ are commuting elements of G. Furthermore we have $g = z_Q$, because of the uniqueness of z_Q. Hence, taking the product of the commuting elements in each possible order, we find that

$$(s, g) = \left(\left(1_{\mathbb{F}_p} \cdot z_Q\right) s, g\right).$$

Thus $s = \left(1_{\mathbb{F}_p} \cdot z_Q\right) s$. However $s = \left(\left(-1_{\mathbb{F}_p}\right) \cdot z_Q\right) s$, because $s \in V$. Therefore since s is nontrivial, we have $1_{\mathbb{F}_p} = -1_{\mathbb{F}_p}$. But this is a contradiction, because p is odd. Hence G has no elements of mixed order. □

4.5 A condition for connectivity of Δ_{G^*}

Here we formalize a brief argument for **Theorem 4.1.2**.

Proof. As we have noted more than once, G is a solvable group by Burnside's Theorem. (See [3, p.621].) Therefore if G has no cyclic or generalized quaternion Sylow subgroups, then Δ_{G^*} is connected of diameter ≤ 7 by Corollary 3.1.3. On the other hand if G contains a cyclic or generalized quaternion Sylow subgroup, and $M(G)$ is nonempty, then in fact Δ_{G^*} has diameter ≤ 6 by Proposition 4.2.1. But by Theorem 4.1.3, Δ_{G^*} is disconnected if $M(G)$ is empty. $\square$

We point out that in the proof we might have said "if G has no cyclic or generalized quaternion Sylow subgroups, and $M(G)$ is nonempty, then...". However this was logically unnecessary, because of 3.1.3. Thus, as we have mentioned previously, $M(G)$ is automatically nonempty if G has no cyclic or generalized quaternion Sylow subgroups.

Bibliography

[1] C. Bates et al., *Commuting involution graphs for symmetric groups*, J. Algebra **266** (2003), 133–153.

[2] D. Bundy, *The connectivity of commuting graphs*, J. Combinatorial Theory **113** (2006), 995–1007.

[3] D. Dummit and R. Foote, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.

[4] T. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer-Verlag, New York, NY, 1974.

[5] N. Jacobson, *Basic Algebra I, Second Edition*, W.H. Freeman and Company, New York, NY, 1985

[6] T. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics **131**, Springer-Verlag, New York, NY, 1991.

[7] A. Potapchik and A. Rapinchuk, *Normal subgroups of $SL_{1,D}$ and the classification of finite simple groups*, Proc. Indian Acad. Sci. **106** (1996), 329–368.

[8] A. Rapinchuk and Y. Segev, *Valuation-like maps and the congruence subgroup property*, Invent. math. **144** (2001), 571–607.

[9] A. Rapinchuk, Y. Segev, and G. Seitz, *Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable*, J. Amer. Math. Soc. **15** (2002), 929–978.

[10] D. Robinson, *A Course in the Theory of Groups, Second Edition*, Graduate Texts in Mathematics **80**, Springer-Verlag, New York, NY, 1996.

[11] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra*, Ann. of Math. **149** (1999), 219–251.

[12] Y. Segev and G. Seitz, *Anisotropic groups of type A_n and the commuting graph of finite simple groups*, Pacific J. Math. **202** (2002), 125–225.