Ádám's Conjecture and its Generalizations

Thesis

Presented to the Graduate Council of the University of North Texas in Partial Fulfillment of the Requirements for the Degree of Master of Arts

By

Edward T. Dobson, B.S.
Denton, Texas
August, 1990

This paper examines Ádám's conjecture and some of its generalizations. In terms of Ádám's conjecture, we prove Alspach and Parson's results for $Z_{pq}$ and $Z_{p^2}$. More generally, we prove Babai's characterization of the CI-property, Palfy's characterization of CI-groups, and Brand's result for $Z_{pr}$ for polynomial isomorphism's.

We also prove for the first time a characterization of the CI-property for $\Omega \leq S_G$, and prove that $Z_n$ is a CI-$P_n$-group where $P_n$ is the group of permutation polynomials on $Z_n$, and $n$ is square free.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>II. CHARACTERIZATION AND GENERAL RESULTS</td>
<td>8</td>
</tr>
<tr>
<td>III. PRODUCTS OF TWO PRIMES</td>
<td>37</td>
</tr>
<tr>
<td>IV. PRODUCTS OF PRIMES</td>
<td>46</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>65</td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

Let $Z_n$ be the cyclic group of order $n$. We define a digraph on $Z_n$ to be the ordered pair $(Z_n, Q)$, where $Q \subseteq Z_n \times Z_n$. We shall say a digraph is simply a graph if whenever $(i, j) \in Q$ then $(j, i) \in Q$. Further, two (di)graphs, $(Z_n, Q)$ and $(Z_n, Q')$ are isomorphic if and only if there exists a bijection $f: Z_n \rightarrow Z_n$ such that if $(x, y) \in Q$ then $((x)f, (y)f) \in Q'$. A bijective function $f: Z_n \rightarrow Z_n$ such that if $(x, y) \in Q$ then $((x)f, (y)f) \in Q$ will be called an automorphism. A (di)graph $(Z_n, Q)$ will be called cyclic with connection set $T \subseteq Z_n$ if and only if $Q = \{(i, j) : i - j \in T\}$. It is not difficult to see that the function $(x)t = x + 1$ (with all arithmetic is calculated modulo $n$) is an automorphism of an arbitrary cyclic (di)graph. Henceforth, we shall denote the cyclic (di)graph $(Z_n, Q)$ with connection set $T$ by $\Gamma(n, T)$.

Let $\Gamma(n, T)$ be a cyclic graph. If $\Gamma(n, T')$ is another graph such that $\Gamma(n, T)$ is isomorphic to $\Gamma(n, T')$, we simply write $\Gamma(n, T) \cong \Gamma(n, T')$. Then one can easily see that $\Gamma(n, T) \cong \Gamma(n, kT)$, where $k$ is relatively prime to $n$. In 1967 Ádám [1] conjectured the converse, i.e., if two cyclic graphs $\Gamma(n, T)$ and $\Gamma(n, T')$ are isomorphic, then there exists $k$ relatively prime to $n$ so that $T = kT'$. If $T = kT'$ for any isomorphic (di)graph $\Gamma(n, T')$ we say that $\Gamma(n, T)$ has the
Cayley isomorphism property. In Chapter IV we shall see that the conjecture is false.

Following Babai [2], Pálfy [3,4] and Brand [5] let $G$ be a finite set and $S$ be a subset of $V \cup 2^V \cup 2^2V \cup \ldots$, where $2^V$ represents the subsets of $V$ and $2^2V$ is the subsets of the subsets of $V$, etc. The pair $B = (G,S)$ is called a combinatorial object (Babai's and Pálfy's relational structure). An isomorphism between two combinatorial objects $(G,S)$ and $(G,S')$ is a bijective function $f:G \rightarrow G$ such that $S$ and $S'$ correspond under the bijection. $\text{Aut}(B)$, the automorphism group of $B$, is the group of all automorphisms from $B$ to $B$. By a Cayley object $X$ of a group $G$ we mean a combinatorial object with underlying set $G$ such that the right translations $G_R = \{g_R: G \rightarrow G \text{ where } (x)g_R = xg\}$ are contained in $\text{aut}(X)$ (Brand's cyclic combinatorial object). Thus if we have a cyclic (di)graph $\Gamma(n,T) = (Z_n,Q)$, then $Q \subseteq V \cup 2^V$ as an ordered pair $(x,y) = \{x,\{x,y\}\}$. Thus a cyclic (di)graph (as well as a non-cyclic (di)graph) is a combinatorial object. Hence graphs satisfy our definition of a combinatorial object.

Let $X$ be a Cayley object defined on some group $G$ in some class $\mathcal{K}$ of combinatorial objects. Let $S_G$ denote the symmetric group on $G$ ($S_n$ if $G = Z_n$) and $G_R \leq \Omega \leq S_G$. We shall say that $G$ is a $\mathcal{K}$-CI-$\Omega$-group (CI stands for Cayley-isomorphism property) if whenever two Cayley objects
X and Y are isomorphic by some $\alpha \in \Omega$, then X and Y are isomorphic by some element of $\text{aut}(G)$. If G is a $\mathcal{K}$-CI-$\Omega$-group for every class of combinatorial objects $\mathcal{K}$, then we simply refer to G as a CI-$\Omega$-group. If $\Omega = S_G$, and G is a $\mathcal{K}$-CI-$\Omega$-group, we refer to G as simply a $\mathcal{K}$-CI-group. If G is a $\mathcal{K}$-CI-group for any class $\mathcal{K}$, then we will say G is a CI-group. Babai and Pálfy generalized Ádám’s conjecture and asked: If G is a finite group and $\mathcal{K}$ is a class of combinatorial objects, are any two isomorphic Cayley objects in $\mathcal{K}$ isomorphic by an automorphism of the group G? The first positive result was obtained for the case of designs on $\mathbb{Z}_p$ by Bays [6] and Lombossy [7], and in the case of graphs on $\mathbb{Z}_p$ (p a prime) by Elspas and Turner [8], Djoković [9], and Alspach and Parsons [10]. For any class of combinatorial object, Babai [2] proved:

**Theorem 2.5:** $\mathbb{Z}_p$ is a CI-group, where $p$ is prime.

More generally, Pálfy [4] characterized CI-groups:

**Theorem 2.10:** G is a CI-group if and only if $G \cong \mathbb{Z}_n$ and $(n,(n)\varphi) = 1$ or $n = 4$, where $(n)\varphi$ is Euler’s phi function.

According to the Pálfy’s Theorem 2.10, there exist infinitely many natural numbers n that are the product of distinct prime numbers so that $\mathbb{Z}_n$ is not a CI-group. It can be trivially shown with a result proven in Chapter 2 (Corollary 2.3) that for each n, a product of distinct
primes, $Z_n$ is a CI-$G_R$-group. It would seem natural to ask if there are larger subgroups $\Omega$ of $S_n$ for which $Z_n$ is a CI-$\Omega$-group. We were able to prove:

**Theorem 2.7:** If $n = p_1 \ldots p_m$ where each $p_i$ is prime and $n$ is square free, then $Z_n$ is a CI-$P_n$-group, where $P_n$ is the group of permutation polynomials on $Z_n$.

Pálfy's theorem tells us that if $n \neq 4$ and $(n,(n)\varphi) \neq 1$ then there exists a class of combinatorial objects $\mathcal{X}$ such that $Z_n$ is not a $\mathcal{X}$-CI-group. It does not tell us which class, however, so in terms of Ádám's conjecture for $n$ a product of distinct primes, it does not tell us anything. In general, if $n$ is square free Ádám's conjecture is still unanswered. In the case of $n = pq$, $p$ and $q$ prime, however, Godsil [9], Klin and Pöschel [10], and Alspach and Parsons [8] have proven:

**Theorem 3.1.** $Z_{pq}$ is a $\mathcal{A}(\mathcal{G})$-CI-group where $\mathcal{A}(\mathcal{G})$ is the class of cyclic (di)graphs.

By Pálfy's theorem we know that if $q \mid (p - 1)$, then there exists some class of combinatorial object $\mathcal{Y}$ for which $Z_{pq}$ is not a $\mathcal{Y}$-CI-group. Phelps [11] has found examples of designs for which $Z_{pq}$ is not a CI-group with respect to the class of designs, although we will not prove that result.

Most of the theorems are proven from a purely group theoretic point of view. The characterization was first developed by Bays [6] and Lombossy [7] for designs, and was
later proven independently for any class of combinatorial objects by Babai [2]. Alspach and Parsons [8] also arrived at the characterization but only for the case of (di)graphs.

As mentioned before, Ádám's conjecture is not true. The first counter examples for the conjecture were found by Elspas and Turner [6] for a cyclic graph of 8 vertices and a digraph with 16 vertices. Both examples are powers of 2. Alspach and Parsons [8] went on to characterize when a (di)graph defined on $\mathbb{Z}_p^2$ has the Cayley isomorphism property, and if a (di)graph does not have the Cayley isomorphism property, necessary and sufficient conditions on which (di)graphs it can be isomorphic with.

In general, no one has proven any results with the generality of Pálfy's theorem for $\mathbb{Z}_{pr}$, where $p$ is prime, but Brand [5] has proven for $\mathbb{Z}_{pr}$, with $p$ a prime, that under certain technical conditions, two isomorphic Cayley objects $X$ and $Y$ are isomorphic by a polynomial of degree $n + 1$ if certain polynomials of degree $n$ are in $\text{aut}(X)$. Brand also found examples of hypergraphs which satisfy the conditions of the theorem.

The group theoretic characterization of the Cayley isomorphism property, and Theorems 2.7 and 2.10 will be proven in Chapter II. The result for $\mathbb{Z}_{pq}$ will be proven in Chapter III, and the results for $\mathbb{Z}_p^r$ will be proven in Chapter IV.
CHAPTER I BIBLIOGRAPHY


5. N. Brand, Polynomial Isomorphisms of Combinatorial Objects, Preprint.


267–270.


CHAPTER II

CHARACTERIZATION AND GENERAL RESULTS

As mentioned in the introduction, several authors independently characterized CI-groups from a purely group theoretic point of view. The result we prove will be based on the proof by Babai in [2], but in a slightly more general fashion.

Let $\mathcal{X}$ be a class of combinatorial objects, $X$ a Cayley object of the group $G$ in $\mathcal{X}$, and $\alpha \in \text{aut}(G)$. Then

Lemma 2.1: $(X)\alpha$ is a Cayley object of $\mathcal{X}$.

Proof: Obviously the underlying set of $(X)\alpha$ is still $G$, so it only remains to be shown that $G_R \trianglelefteq \text{aut}((X)\alpha)$. Since $(x)\alpha^{-1}G_R \alpha = ((x)\alpha^{-1}g)\alpha = (x)\alpha^{-1}(g)\alpha = x(g)\alpha$, $\alpha^{-1}G_R \alpha = ((g)\alpha)^{-1}$. Thus $\text{aut}((X)\alpha) = \alpha^{-1}(\text{aut}(X)) \trianglelefteq \alpha^{-1}G_R \alpha = G_R$. □

Lemma 2.2: For a Cayley object $X$ of $G$ in $\mathcal{X}$ and $G_R \trianglelefteq \Omega \trianglelefteq S_G$, the following are equivalent:

(i) $X$ is a $\mathcal{X}$-CI-$\Omega$-object;

(ii) given a permutation $\varphi \in \Omega$ such that $\varphi G_R \varphi^{-1} \trianglelefteq \text{aut}(X)$, $G_R$ and $\varphi G \varphi^{-1}$ are conjugate in $\text{aut}(X)$.

Proof: (ii) implies (i). Let $Y$ be another Cayley object of $G$ in $\mathcal{X}$ such that $X$ and $Y$ are isomorphic by some $\varphi \in \Omega$. Now,

$$\text{aut}(X) = \varphi(\text{aut}(y))\varphi^{-1} \triangleright \varphi G_R \varphi^{-1},$$

so by (ii), there exists $\beta \in \text{aut}(X)$ such that $\varphi G_R \varphi^{-1} = \beta^{-1}G_R \beta$.
Let $\beta \varphi = \tau$, and hence $\tau^{-1}G_R \tau = G_R$. If $(1)^{-1} = g$, let $\delta = g_R \tau$. Thus $(1)^{-1}$ and $\delta^{-1}G_R \delta = G_R$. Hence $\delta$ induces an automorphism $\alpha$ on $G_R$. Thus $\delta^{-1}g_R \delta = (\alpha)_{R} = \alpha^{-1}g_R \alpha$ for some $\alpha \in \text{aut}(G)$. As $\delta \alpha^{-1}g_R = g_R \delta \alpha^{-1}$, $\delta \alpha^{-1}$ belongs to the centralizer of $G_R$. As is well known, this centralizer is $G_L = \{g_L: g_L(x) = gx\}$, the left translations of $G$. Now, $(x)1_R \delta \alpha^{-1} = (1x) \delta \alpha^{-1} = \alpha^{-1}(\delta(x) \delta) \alpha^{-1}$ as $(1)^{-1} = 1$. Thus, $\alpha^{-1}(\delta(x) \delta) \alpha^{-1} = (1)^{-1}(\delta(x) \delta) \alpha^{-1} = (1x) \delta \alpha^{-1} = \delta \alpha^{-1}$. Since $\delta \alpha^{-1}$ fixes $1$ and $\delta \alpha^{-1} \in G_L$, $\delta \alpha^{-1} = 1_R$. Recall that $g_R \tau = \delta = \alpha$ so $\tau = g_R^{-1} \alpha$. As $\beta \varphi = \tau$, $\varphi = \beta^{-1} \tau = \beta^{-1} g_R^{-1} \alpha$. Thus $Y = (X) \varphi = (X) \beta^{-1} g_R^{-1} \alpha = (X) \alpha$ as $\beta \varphi = \tau$, $g_R \alpha \in \text{aut}(X)$. This proves that $X$ is a $\mathcal{K}$-CI-$\Omega$-object.

(i) implies (ii). Suppose $\varphi \in \Omega$ and $\varphi G_R \varphi^{-1} \not\in \text{aut}(X)$. Let $Y = (X) \varphi$. $Y$ is a Cayley object of $G$ in $\mathcal{K}$ as $\text{aut}(Y) = \varphi^{-1}(\text{aut}(X)) \varphi \geq G_R$. If $X$ is a CI-object we have $Y = (X) \alpha$ for some $\alpha \in \text{aut}(G)$. Hence $(X) \alpha = (X) \varphi$, so $(X) \varphi \alpha^{-1} = X$. Thus $\beta = \varphi \alpha^{-1} \in \text{aut}(X)$. Then

$$\varphi G_R \varphi^{-1} = \beta \alpha G_R \alpha^{-1} \beta = \beta G_R \beta^{-1},$$

and so concludes the proof. \(\square\)

**Corollary 2.3:** For a group $G$ and $G_R \leq \Omega \leq S_G$ the following are equivalent:

(i) $G$ is a CI-$\Omega$-group.

(ii) Given any permutation $\varphi \in \Omega$, $G_R$ and $\varphi G_R \varphi^{-1}$ are conjugate in the subgroup $\langle G_R, \varphi G_R \varphi^{-1} \rangle$ of $\Omega$.

**Proof:** (ii) implies (i). Let $\varphi \in \Omega$. Then $G_R$ and
\( \phi_{G_R} \psi^{-1} \) are conjugate in the subgroup \( \langle G_R, \phi_{G_R} \psi^{-1} \rangle \leq \Omega \). Hence if \( \phi_{G_R} \psi^{-1} \leq \text{aut}(X) \) then by Lemma 2.2 (ii), \( G \) is a \( \mathcal{K}-\text{CI}-\Omega \)-group for any class \( K \).

(i) implies (ii). Let \( \varphi \in \Omega \), \( n = |G| \), and let \( \{g_i\}_{i=1}^n \) be an enumeration of \( G \). Let \( R = \{(a_1, \ldots, a_n) : (g_1, \ldots, g_n) \delta = (a_1, \ldots, a_n) \text{ for some } \delta \in \langle G_R, \phi_{G_R} \psi^{-1} \rangle \} \). Notice that \( C = (G, R) \) is a combinatorial object by the definition of an \( n \)-tuple.

Let \( \delta \in \langle G_R, \phi_{G_R} \psi^{-1} \rangle \) and \( (a_1, \ldots, a_n) \in R \). Thus there exists \( \tau \in \langle G_R, \phi_{G_R} \psi^{-1} \rangle \) such that \( (g_1, \ldots, g_n) \tau = (a_1, \ldots, a_n) \). Hence \( \tau \delta^{-1} \in \langle G_R, \phi_{G_R} \psi^{-1} \rangle \) and thus \( ((a_1) \delta^{-1}, \ldots, (a_n) \delta^{-1}) \in R \). It follows that \( ((a_1) \delta^{-1}, \ldots, (a_n) \delta^{-1}) \delta = (a_1, \ldots, a_n) \). Therefore \( G_R \leq \langle G_R, \phi_{G_R} \psi^{-1} \rangle \leq \text{aut}(C) \) so \( C \) is a Cayley object in the class \( \mathcal{R}_n \) of \( n \)-ary combinatorial objects.

Let \( \delta \in \text{aut}(C) \). Then \( (g_1, \ldots, g_n) \delta \in R \) and hence \( \delta \in \langle G_R, \phi_{G_R} \psi^{-1} \rangle \). Thus \( \text{aut}(C) = \langle G_R, \phi_{G_R} \psi^{-1} \rangle \).

Hence as \( G \) is a \( \mathcal{K}-\text{CI}-\Omega \)-group, \( G \) is a \( \mathcal{R}_n-\text{CI}-\Omega \)-group. Thus \( G_R \) and \( \phi_{G_R} \psi^{-1} \) are conjugate in \( \langle G_R, \phi_{G_R} \psi^{-1} \rangle \). Let \( X \) be a Cayley object of \( G \) in \( K \). Let \( \varphi \in \Omega \) such that \( \phi_{G_R} \psi^{-1} \leq \text{aut}(X) \). Then \( \langle G_R, \phi_{G_R} \psi^{-1} \rangle \leq \text{aut}(X) \) and so \( G_R \) and \( \phi_{G_R} \psi^{-1} \) are conjugate in \( \text{aut}(X) \). Thus by Lemma 2.2 (i), \( G \) is a \( \mathcal{K}-\text{CI}-\Omega \)-group for any arbitrary class of combinatorial objects. \( \square \)

If \( \Omega = S_G \), we have

**Corollary 2.4:** For a group \( G \) the following are equivalent:
(i) $G$ is a CI-group.

(ii) Given any permutation $\varphi \in S_G$, $G_R$ and $\varphi G_R \varphi^{-1}$ are conjugate in the subgroup $\langle G_R, \varphi G_R \varphi^{-1} \rangle$ of $S_G$.

Now a simple application of the Sylow theorems gives us [2]:

**Theorem 2.5:** $Z_p$ is a CI-group, where $p$ is prime.

**Proof:** Observe that $G_R$ and $\varphi G_R \varphi^{-1}$ are both Sylow $p$-subgroups of $\langle G_R, \varphi G_R \varphi^{-1} \rangle$, so the result follows from Corollary 2.4 by an application of the Sylow theorems. □

Recall that $P_n$ is the set of all permutation polynomials on $Z_n$. We now prove a lemma describing the structure of $P_n$, where $n$ is square free.

**Lemma 2.6:** If $n = p_1 \ldots p_m$ and $n$ is square free, then

$$P_n = \bigoplus_{i=1}^{m} S_{p_i}.$$  

**Note:** We say $P_n = \bigoplus_{i=1}^{m} S_{p_i}$, but in fact $P_n \cong \bigoplus_{i=1}^{m} S_{p_i}$. Hence in this context we mean that the two groups are equal upto isomorphism. As two isomorphic groups have the same group theoretic properties, this abuse of notation is somewhat justified, and will be employed in the remainder of the text.

**Proof:** Let $f \in P_n$, and let $f_i: Z_{p_i} \rightarrow Z_{p_i}$ by $(x)f_i = (x)f$ (mod $p_i$). Each $f_i$ is well defined, as we know from elementary number theory that if $a \equiv b$ (mod $p_i$) then $(a)f \equiv (b)f$ (mod $p_i$). We wish to show that the function $g:P_n \rightarrow$
12

\[ \prod_{i=1}^{m} S_{p_i} \text{ given by } (f)g = \prod_{i=1}^{m} f_i \text{ is an isomorphism. To show each } f_i \in S_{p_i}, \text{ it is sufficient to show that each } f_i \text{ is surjective. As } f \text{ is a permutation, given } y \in Z_{p_i}, \text{ there is a } w \in Z_n \text{ such that } (w)f = y. \text{ Let } x \equiv w \pmod{p_i}. \text{ Then } (x)f = y. \text{ Hence } f_i \in S_{p_i}. \text{ Thus } g \text{ is well defined.} \]

Let \( f_1, f_2 \in P_n \) such that \( f_1 \neq f_2 \). Thus there exists \( x \in Z_n \) such that \( (x)f_1 \neq (x)f_2 \). Hence there is an \( i \) such that \( (x)f_i \) is not congruent to \( (x)f_2 \pmod{p_i} \). Let \( y \in Z_n \) such that \( y \equiv x \pmod{p_i} \) and \( y < p_i \). Thus \( (y)f_i \neq (y)f_2 \). Hence \( (f_i)g \neq (f_2)g \), proving that \( g \) is injective.

As each permutation in \( Z_{p_i} \) is a polynomial and \( g \) is injective, to show \( g \) is surjective, we need only show that the domain of \( g^{-1} \) is \( \prod_{i=1}^{m} S_{p_i} \). It follows easily from the Chinese Remainder Theorem that each \( f = \prod_{i=1}^{m} f_i \) is in fact a permutation in \( Z_n \). Thus we need only establish that \( f \) is indeed a polynomial. As each \( f_i \) is a polynomial on \( Z_{p_i} \) we may apply Fermat's Little Theorem and write \( (x)f_i = \prod_{j=0}^{p_i-1} \sum_{j_i=0}^{a_{j_i}} x_j \). Then, if \( x = \sum_{j=1}^{m} a_{j_i} x_j \), we have

\[ \prod_{i=1}^{m} ((x)f_i) = (x) \left[ \prod_{i=1}^{m} f_i \right] = \prod_{i=1}^{m} \left[ \prod_{j_i=0}^{p_i-1} \sum_{j_i=0}^{a_{j_i}} x_j \right] \]
\[ p_{m-1} = \sum_{j=0}^{m} \left[ \sum_{i=1}^{m} a_{j,i} \right] x^j \]

which is certainly a polynomial on \( Z_n \). Thus \( g \) is a bijection.

Let \( f_1, f_2 \in P_n \). Then \( (f_1 f_2)g = \bigoplus_{i=1}^{m} (f_1 f_2)_i \)

\[ = \bigoplus_{i=1}^{m} (f_1)_i (f_2)_i \]

\[ = (f_1)g(f_2)g \]

This completes the proof. \( \square \)

Let \( G_{R_i} \) be the set of right translations on \( Z_{p_i} \), and note that \( G_R = \bigoplus_{i=1}^{m} G_{R_i} \), where \( G_R \) is the set of right translations on \( Z_n \). We are now able to prove:

**Theorem 2.7.** If \( n = p_1 \ldots p_m \) where \( p_1, \ldots, p_m \) are distinct primes, then \( Z_n \) is a CI-P-group.

**Proof:** As \( G_R \leq P_n \), by Corollary 2.3 we only need to establish that given \( \varphi \in P_n \), \( G_R \) and \( \varphi G_R \varphi^{-1} \) are conjugate in the subgroup \( \langle G_{R_i}, \varphi G_R \varphi^{-1} \rangle \) of \( P_n \). Now, \( G_R = \bigoplus_{i=1}^{m} G_{R_i} \) so \( \varphi G_R \varphi^{-1} = \bigoplus_{i=1}^{m} (\varphi_i G_{R_i} \varphi_i^{-1}) \) where \( \varphi = \bigoplus_{i=1}^{m} \varphi_i \). Further, \( \langle G_{R_i}, \varphi G_R \varphi^{-1} \rangle = \bigoplus_{i=1}^{m} <G_{R_i}, \varphi G_{R_i} \varphi_i^{-1}> \). By Theorem 2.5, \( Z_{p_i} \) is a CI-group, so for each \( i \), \( G_{R_i} \) and \( \varphi G_{R_i} \varphi_i^{-1} \) are conjugate in the subgroup \( <G_{R_i}, \varphi G_{R_i} \varphi_i^{-1}> \) of \( S_{p_i} \). Thus there is \( \beta_i \in <G_{R_i}, \varphi G_{R_i} \varphi_i^{-1}> \) so that
\[ \beta^{-1}G_{\beta} \beta = \varphi G_{\beta} \varphi^{-1}. \] Let \( \beta = \bigoplus_{i=1}^{m} \beta_i. \) Then \( \beta \in \langle G_{\beta}, \varphi G_{\beta} \varphi^{-1} \rangle \) and
\[ \beta^{-1}G_{\beta} \beta = \varphi G_{\beta} \varphi^{-1}. \] This completes the proof. \( \Box \)

Let \( G \) be a group and \( \Omega \subseteq S_G. \) We shall say \( \Omega \) is \textit{transitive} if given any \( x, y \in G, \) there exists \( \beta \in \Omega \) such that \((x)\beta = y.\) If \( \Omega \) is not transitive, we say \( \Omega \) is \textit{intransitive}. Let \((x_1, x_2)\) and \((y_1, y_2)\) be arbitrary ordered pairs of elements of \( G. \) If there exists \( \beta \in \Omega \) such that \((x_i)\beta = y_i, \) where \( i = 1, 2, \) then we say that \( \Omega \) is \textit{doubly transitive}.

Let \( H \subseteq G. \) We call \( H \) a \textit{block} of \( \Omega \) if \((H)\beta = H \) or \((H)\beta \) has no point in common with \( H \) for every \( \beta \in \Omega. \) Obviously, \( G, \) the empty set, and sets consisting of only one point of \( G \) are blocks of every \( \Omega \subseteq G. \) We call these blocks \textit{trivial blocks}.

A transitive group \( \Omega \subseteq S_G \) is \textit{imprimitive} if there is at least one nontrivial block \( H. \) If a group \( \Omega \subseteq S_G \) is not imprimitive, we say that \( \Omega \) is \textit{primitive}. Let \( H \) be a block of \( \Omega. \) Then for each \( \beta \in \Omega \) \((H)\beta \) is also a block of \( \Omega. \) \( H \) and \((H)\beta \) are called \textit{conjugate blocks}. Note that two conjugate blocks are either disjoint or equal. All blocks conjugate to \( H \) form a \textit{complete block system}. Hence each block in a complete block system contains the same number of elements, and the cardinality of any block divides the degree of \( \Omega. \)

By a \textit{Burnside group} we mean a finite group \( H \) with the property that every primitive group containing the right translations of \( H \) as a transitive subgroup is doubly transitive. We state without proof a result by Wielandt.
[14, pg. 65]:

**Theorem 2.8:** Every cyclic group of composite order is a Burnside group.

By the *socle* of $\Omega \leq S_\nu$, we mean the product of the minimal normal subgroups of $\Omega$. We state without proof a result of O'Nan and Scott [15]:

**Theorem 2.9:** Let $G$ be a group and $\Omega \leq S_G$ be a primitive permutation group, with degree $n$ and socle $N$. Then one of the following occurs:

(i) $N$ is elementary abelian of order $p^d$ and regular, $n = p^d$, where $p$ is prime and $d \geq 1$.

(ii) $N = T_1 \times \ldots \times T_m$, where $T_1, \ldots, T_m$ are all isomorphic to a fixed simple group $T$.

We now have the necessary definitions to prove the result by Palfy [4]:

**Theorem 2.10:** $G$ is a CI-group if and only if $G \cong Z_n$ and $(\varphi(n), n) = 1$, or $n = 4$, where $\varphi$ is Euler's phi function.

**Proof:** The proof will be divided into several parts.

We will first show that $Z_4$ and $Z_2 \oplus Z_2$ are CI-groups.

**Lemma 2.11:** $Z_4$ is a CI-group.

**Proof:** We need to show that if $\varphi \in S_4$ then $G = (Z_4)_R$ and $\varphi G \varphi^{-1}$ are conjugate in $W = \langle G, \varphi G \varphi^{-1} \rangle$. Let $\varphi \in S_4$. If $|W| = 4$, then we are trivially done, so assume that $|W| > 4$.

Suppose there exists $\varphi$ such that $\varphi g R \varphi^{-1} = h R$, where $g \neq 0 \neq h$. Then $h = 2$ as $1_R$ and $3_R$ both generate $G$. Further,
\( \varphi_0 \varphi^{-1} = 0_\mathcal{R} \) and both \( \varphi_1 \varphi^{-1} \) and \( \varphi_3 \varphi^{-1} \) are four cycles. Thus \( g = 2 \). Hence,

\[
(x) \varphi_{2-R} = (x) \varphi + 2 = (x + 2) \varphi = (x) 2 \varphi,
\]

and so \( \varphi = 2_\mathcal{R} \). But then \( \varphi G \varphi^{-1} = G \). Thus \( |G \cap \varphi G \varphi^{-1}| = 1 \).

Now,

\( G \varphi G^{-1} \subseteq <G, \varphi G \varphi^{-1}> \) where \( G \varphi G^{-1} = \{hk : h \in G, k \in \varphi G \varphi^{-1}\} \).

By [16, pg 39],

\[
|G \varphi G^{-1}| = \frac{|G||\varphi G \varphi^{-1}|}{|G \cap \varphi G \varphi^{-1}|} = 16.
\]

Thus \( |<G, \varphi G^{-1}>| = 24 \) and \( <G, \varphi G^{-1}> = S_4 \).

Also,

**Lemma 2.12:** \( G = Z_2 \oplus Z_2 \) is a CI-group.

**Proof:** Let \( \varphi \in S_G \). Again, let \( W = <G_{\mathcal{R}}, \varphi G_{\mathcal{R}} \varphi^{-1}> \). If \( |W| = 4 \) or \( 24 \), then we are trivially finished. Hence \( |W| = 8 \) or \( 12 \). If \( |W| = 12 \), then \( G_{\mathcal{R}} \) and \( \varphi G_{\mathcal{R}} \varphi^{-1} \) are Sylow 2-subgroups of \( W \) and hence are conjugate in \( W \). Notice that \( a_{\mathcal{R}} \) is a product of two disjoint two cycles, for any \( a \neq 0 \). Hence \( \varphi a_{\mathcal{R}} \varphi^{-1} \) is even, so \( W \leq A_G \). But \( A_G \) has no subgroups of order 8. Hence \( |W| \neq 8 \).

We now show that if \( G \cong Z_n \) and \( ((n) \varphi, n) = 1 \), then \( G \) is a CI-group. We proceed by induction on the number of prime divisors of \( n \). If \( n \) is prime, then the theorem follows from Theorem 2.5. So assume \( n \) is composite. By the hypothesis we know that \( ((n) \varphi, n) = 1 \), so we know that \( n \) is odd,
square-free, and for all divisors \( n_1, n_2 \) of \( n \), \( ((n_1)\varphi, n_2) = 1 \). By induction we know that for all proper divisors \( m \) of \( n \), \( Z_m \) is a CI–group.

Let \( G_n \) be the set of all right translations in \( Z_n \). What we wish to show is given any permutation \( \beta \in S_n \), \( G_n \) and \( \beta G_n \beta^{-1} \) are conjugate in the subgroup \( \langle G_n, \beta G_n \beta^{-1} \rangle \) of \( S_n \). Equivalently, if \( x \) is the \( n \)–cycle \((1 \, 2 \, \ldots \, n)\), given any other \( n \)–cycle \( y \), the cyclic subgroups \( \langle x \rangle \) and \( \langle y \rangle \) are conjugate in the subgroup \( \langle x, y \rangle \) of \( S_n \). Now, \( \langle x, y \rangle \) is of composite order and it contains an \( n \)–cycle. As \( Z_n \) is cyclic and of composite order, by Theorem 2.8, \( \langle x, y \rangle \) is either imprimitive or doubly transitive. As \( n \) is odd, we know \( \langle x, y \rangle \not\subseteq A_n \), the alternating group on \( Z_n \). We will consider the following three cases:

1. \( \langle x, y \rangle \) is imprimitive;
2. \( \langle x, y \rangle \) is doubly transitive, \( \langle x, y \rangle \neq A_n \);
3. \( \langle x, y \rangle = A_n \).

**Case 1:** \( \langle x, y \rangle \) is imprimitive.

This proof is similar to the proof of Theorem 1 in [3], with slight modifications to Lemma 1.3 in [4] (our Lemma 2.14). Lemma 1.1 was proven in [4] (our Lemma 2.13).

Let \( x \) be defined as above and let \( y \) be an arbitrary \( n \)–cycle in \( S_n \) such that \( \langle x, y \rangle \) is imprimitive. Thus there exists \( H \subset Z_n \) such that \( H \) is a block of \( \langle x, y \rangle \). Hence the complete block system contains \( m \) blocks each of size \( k = |H| \).
(where \(mk = n\)). Let \(z_i = (i \; i+m \ldots i+(k-1)m)\) where \(i = 1,2,\ldots,m\), and \(P = \langle z_i : 1 \leq i \leq m \rangle\). Hence \(x^m = z_1z_2\ldots z_m\) and \(x^{-1}z_ix = z_{i+1}\).

**Lemma 2.13:** If \(\langle x,y \rangle\) admits a complete block system of \(m\) blocks of size \(k\) and \(Z_k\) is a CI–group then there exists a \(y' \in S_n\) such that \(y'\) is conjugate to \(y\) in \(\langle x,y \rangle\) and \(y'^m \in P\).

**Proof:** The only such complete block system for \(\langle x \rangle\) is formed by the orbits of \(\langle x^m \rangle\), and the same is true for \(\langle y \rangle\). Hence if \(y^m = w_1w_2\ldots w_m\), where each \(w_i\) is a \(k\)–cycle containing \(i\), then \(w_i\) and \(z_i\) permute the same \(k\) elements. Since we are assuming that \(Z_k\) is a CI–group, there is an element \(t = \langle x^m,y^m \rangle\) such that \(t^{-1}w_it = z_i^{a_i}\) for some \(a_i\), where \((a_i,k) = 1\). Similarly, there is an element \(t_2 \in \langle x^m,y^m \rangle\) such that \(t_2^{-1}w_2t_2 = z_2^{a_2}\) for some \(a_2\), where \((a_2,k) = 1\). Further, \(t_2^{-1}(t_1w_2t_1)t_2 = t_2^{-1}z_1^{a_1}t_2 = z_1^{a_1}\) as \(z_1\) is centralized by \(\langle x^m,y^m \rangle\). Continuing analogously there are elements \(t_3,\ldots,t_m\) so that if \(t = t_1\ldots t_m\), then for each \(i\), \(t^{-1}w_i^m = z_i^{a_i}\). Hence if \(y' = \langle y^m \rangle\) then \(y'^m = t^{-1}yt = t^{-1}w_1^m\ldots w_m^mt = z_1^{a_1}\ldots z_m^{a_m} \in P\). \(\square\)

**Lemma 2.14.** If \(Z_m\) is a CI–group and \(y^m \in P\) then there exists a \(y' \in S_n\) such that \(\langle y' \rangle\) is conjugate to \(\langle y \rangle\) in \(\langle x,y \rangle\), \(y'^{-1}z_1^m \langle y' \rangle = \langle z_1^m \rangle\) and \(y'^m \in P\).

**Proof:** As \(x\) and \(y\) are \(n\)–cycles and \(x^m,y^m \in P\), the
effect of conjugation by \( x \) and \( y \) on the set of subgroups \( Z = \{<z_i>: 1 \leq i \leq m\} \) are \( m \)-cycles. Denote the \( m \)-cycles derived by conjugation on \( Z \) by \( x \) and \( y \) by \([x]\) and \([y]\) respectively. Further, if \( q \in <x,y> \) then \( q \) can also be viewed as a permutation on \( Z \), which we will call \([q]\). Conversely, if \([q] \in <[x],[y]>\), then \([q] = [x]^{e_1}[y]^{e_2}...[x]^{e_{r-1}}[y]^{e_r}\) for some \( r \) and where each \( 0 \leq e_i \leq m-1 \). Hence \([q]\) is the permutation on \( Z_m \) derived by conjugating \( Z \) by \( x \) \( e_1 \) times, by \( y \) \( e_2 \) times, etc. Hence \([q] = [x^{e_1}y^{e_2}...x^{e_{r-1}}y^{e_r}]\). Note that \([q]\) has a unique representation in the form \([x^{e_1}y^{e_2}...x^{e_{r-1}}y^{e_r}]\) where each \( e_i \leq m - 1 \).

As \( x^{-1}z_i x = z_i^{+1} \), \([x]<z_i> = <z_i^{+1}>\). Thus the \( m \)-cycle \([x]\) translates by \( 1 \). Hence \([x]\) and \([y]\) are conjugate in \(<[x],[y]>\), as \( Z_m \) is a CI-group. Thus there is a \([y^*]\) \( \in \) \(<[x],[y]>\) so that \([y^*]^{-1}[y][y^*] = [x]\). Let \( r, e_1, \ldots, e_r \) be integers such that \([y^*] = [x^{e_1}y^{e_2}...x^{e_{r-1}}y^{e_r}]\). Thus \( y^* = x^{e_1}y^{e_2}...x^{e_{r-1}}y^{e_r} \in <x,y>\). Set \( y' = y^*-yy^* \). Then \( y' \in <x,y>, y^*<y'>y^{*-1} = <y>, y'^{-1}<z_i>y' = <z_i^{+1}>, \) and \( y'^m \in P \).

**Lemma 2.15:** If \( m \) is prime to both \( k \) and \( (k)\varphi \), \( y^m = z_1^{a_1}z_2^{a_2}...z_m^{a_1} \) with \( (a_i,k) = 1 \) and \( y^{-1}z_iy = z_i^{b_i} \) with \( (b_i,k) = 1 \) then there exists a \( y' \in S_n \) such that \(<y'>\) is conjugate to \(<y>\) in \(<x,y>\), \( y'^m = x^m \) and \( y'^{-1}z_i y' = z_i^{+1} \).

**Proof:** As \( m \) is prime to \( (k)\varphi \) we may choose a number \( r \) so that \( mr \equiv -1 \pmod{(x)\varphi} \). Let

\[
u = \Pi_{j=1}^{m} [(yx^{-1})^{rm-rj} x].\]
Then

\[ u^{-1}z_i u = \left[ \prod_{j=1}^{m} (yx^{-1})^{\frac{m-r_j}{x-j}} \right]^{-1} z_i \left[ \prod_{j=1}^{m} (yx^{-1})^{\frac{m-r_j}{x-j}} x \right] \]

\[ = \prod_{j=1}^{m} x^{-1} (xy^{-1})^{\frac{r_j}{x-j}} z_i \prod_{j=1}^{m} (yx^{-1})^{\frac{m-r_j}{x-j}} x \]

\[ = \prod_{j=2}^{m} x^{-1} (xy^{-1})^{\frac{r_j}{x-j}} z_{i+1} \prod_{j=2}^{m} (yx^{-1})^{\frac{m-r_j}{x-j}} x \]

Continuing inductively, we find that

\[ u^{-1}z_i u = z_i \]

In order to simplify notation, let \( c_i = \prod_{j=1}^{m} b_{i+j-1} \). Hence

\[ u^{-1}z_i u = \overline{c_i} \]

As \( y = y^{-1} y = \prod_{i=1}^{m} a_i b_i \), \( a_{i+1} \equiv a_i b_i \) (mod \( k \)). Further,

\[ b_i c_i \equiv b_i c_i \left[ \prod_{q=1}^{m} b_i \right]^{r} = b_i \prod_{j=1}^{m} b_{i+j-1} = b_i \prod_{j=1}^{m} c_i \equiv c_i \equiv (mod \ k) \]

as \( y^{-m} z_i y^m = z_i = \prod_{q=1}^{m} b_q \equiv 1 \) (mod \( k \)). Thus there exists an \( s \) so that \( c_i \equiv s a_i \) (mod \( k \)) and we can also assume that \( s \equiv 1 \) (mod \( m \)) as \( m \) is prime to \( k \). Hence \( u^{-1}z_i u = z_i^{sa_i} \).

Let \( y' = uy u^{-1} \). Then

\[ y'^m = uy^m u^{-1} = \prod_{i=1}^{m} u z_i^{sa_i} u^{-1} = \prod_{i=1}^{m} u z_i^{c_i} u^{-1} = \prod_{i=1}^{m} z_i = x^m. \]

Further,
Lemma 2.16: If \((m,k) = 1\), \(y^m = x^m\) and \(y^{-1} z_i y = z_{i+1}\) then \(y\) is conjugate to \(x\) in \(\langle x, y \rangle\).

Proof: As \((m,k) = 1\), we may choose \(t\) so that \(mt \equiv -1 \pmod{k}\). Let

\[ w = \prod_{j=1}^{m} ((yx^{-1})^{tm-tj}x). \]

We show that \(y = w^{t}xw\).

By the definition of \(x\), \((r)x = r + 1\), so

\[(r + m)y = (r)x^m y = (r)y^{m+1} = (r)y^m = (r)y + m\]

and

\[(r)yz_{m+1} = (r)z_{m}y = (r + m)y = (r)y + m.\]

Hence \((r)y \equiv r + 1 \pmod{m}\). Thus \((r)y - r - 1\) depends only on the residue class \(r \pmod{m}\). Hence \((r)y = r + 1 + md_r\) for some \(d_r\). Note that

\[ r + m = (r)x^m = (r)y^m = 1 + m + m \sum_{j=1}^{m} d_j, \]

so \(m \sum_{j=1}^{m} d_j \equiv 0 \pmod{n}\).

Now,

\[ (r)w = (r) \prod_{j=1}^{m} ((yx^{-1})^{tm-tj}x) \]

\[ = (r + 1 + t(m-1) + md_r) \prod_{j=1}^{m} ((yx^{-1})^{tm-tj}x). \]

Continuing inductively, we find that
\[(r)w = r + m + mt \sum_{j=1}^{m} (m - j)d_{r+j-1}.
\]

Hence,
\[
(r)wy = \left[ r + m + mt \sum_{j=1}^{m} (m - j)d_{r+j-1} \right] y
\]
\[
= r + m + 1 + md_{1} + mt \sum_{j=1}^{m} (m - j + 1)d_{r+j-1}
\]
\[
= r + 1 + m + mt \sum_{i=1}^{m} (m - i)d_{r+i} + md_{r}(r + mt)
\]
\[
= (r + 1)w = (r)xw.
\]

Thus \(wy = xw\) and so \(y = w^{-1}xw\). \(\Box\)

As \(<x, y>\) is imprimitive, by Lemma 2.13, there exists \(y_{1} \in <x, y>\) such that there exists \(\beta_{1} \in <x, y>\) with \(\beta_{1}^{-1}y\beta_{1} = y\) and \(y_{1}^{m} \in P\). Hence by Lemma 2.14, there exists \(y_{2} \in <x, y_{1}> \leq <x, y>\) such that there exists \(\beta_{2} \in <x, y_{1}>\) where \(\beta_{2}^{-1}y_{2}\beta_{2} = y_{1}\), \(y_{2}^{-1}z_{i}y_{2} = <z_{i+1}>\), and \(y_{2}^{m} \in P\). As \(y_{2}^{m} \in P\), \(y_{2}^{m} = z_{1}^{a_{1}} \cdots z_{m}^{a_{m}}\)

for \(0 \leq a_{i} < m\). By the proof of Lemma 2.13, \(y_{1}^{m} = z_{1}^{e_{1}} \cdots z_{m}^{e_{m}}\)

where \((e_{i}, k) = 1\). As \(\beta_{2}y_{2}\beta_{2}^{-1} = y_{1}\), \(\beta_{2}^{-1}y_{2}\beta_{2} = y_{1}\) where \((r, k) = 1\). Hence \(\beta_{2}^{-1}y_{2}\beta_{2}^{-1}z_{i}^{e_{1}} \cdots z_{m}^{e_{m}}\beta_{2}^{-1}\) and \((re_{i}, k) = 1\).

Thus \(re_{i} \equiv a_{i} \pmod{m}\) and so \((a_{i}, k) = 1\). Further, as \(y_{2}^{-1}z_{i}y_{2} = <z_{i+1}>\), \(y_{2}^{-1}z_{i}y_{2} = z_{i}^{b_{i}}\) where \((b_{i}, k) = 1\). Thus by Lemma 2.15 there exists \(y_{3} \in <x, y_{2}> \leq <x, y>\) such that there exists \(\beta_{3} \in <x, y_{2}>\) where \(\beta_{3}^{-1}y_{3}\beta_{3} = y_{2}\), \(y_{3}^{m} = x^{m}\), and \(y_{3}^{-1}z_{i}y_{3} = z_{i+1}\). Finally, by Lemma 2.16, there exists \(\beta_{4} \in <x, y_{3}>\) such that \(\beta_{4}^{-1}y_{3}\beta_{4} = <x>\). Let \(\beta = \beta_{3}\beta_{3}\beta_{4}\). Then \(\beta \in <x, y>\) and \(\beta^{-1}y\beta = <x>\). Hence by Corollary 2.4, \(Z_{n}\) is a CI-group. \(\Box\)
Case 2: \(<x,y>\) is doubly transitive but \(G \not\cong A_n\).

Case 2 will be reduced to Case 1 by proving a result that ultimately depends upon the recent classification of the finite simple groups.

**Lemma 2.17.** Let \(G \leq S_n\) be a doubly transitive group, \(G \not\cong A_n, S_n\). If \(n\) is square free then there exists a prime divisor \(p\) of \(n\) such that the Sylow \(p\)-subgroups of \(G\) have order \(p\).

**Proof.** Note that if \(n\) is prime then the result is true even without excluding \(A_n\) or \(S_n\). Now, if the socle of \(G\) is abelian then by Theorem 2.9, \(n\) is a power of \(p\), and as \(n\) is square free, \(n = p\). We now restrict ourselves to groups \(G\) with nonabelian socle. These groups have been classified \[18\] and are listed in Table 1.

The groups reference by \(\dagger\) in Table 1 all have a prime divisor \(p\) of \(n\) such that the Sylow \(p\)-subgroups have order \(p\). For \(A_7\), note that \(|A_7| = 7\cdot 6\cdot 5\cdot 4\cdot 3\), so 5 divides the degree 15 and the Sylow 5-subgroups of \(A_7\) have order 5. The group \(M_{22}\) is a subgroup of \(M_{24}\), one of only two non-trivial 5-fold transitive groups known, which was discovered by Mathieu. The order of \(M_{22}\) is \(2^7\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23\) \[18\]. Hence the order of \(M_{22}\) is divisible by 11, and so the Sylow 11-subgroups of \(M_{22}\) have order 11.

Thus we now need to deal only with the groups
Table 1

Doubly transitive groups with nonabelian socle.

<table>
<thead>
<tr>
<th>degree</th>
<th>socle</th>
<th>remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>$n \geq 5$</td>
<td>$A_n$</td>
</tr>
<tr>
<td>$(q^d - 1)$</td>
<td>$d \geq 3$ or $d = 2, q \geq 5$</td>
<td>$\text{PSL}_d(q)$</td>
</tr>
<tr>
<td>$(q - 1)$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$q^3 + 1$</td>
<td>$q \geq 3$</td>
<td>$\text{PSU}_d(q)$</td>
</tr>
<tr>
<td>$q^2 + 1$</td>
<td>$q = 2^{2n+1}, n \geq 3$</td>
<td>$2B_2(q)$</td>
</tr>
<tr>
<td>$q^3 + 1$</td>
<td>$q = 3^{2n+1}, n \geq 3$</td>
<td>$3G_2(q)$</td>
</tr>
<tr>
<td>$2^{d-1}(2^d - 1)$</td>
<td>$d \geq 3$</td>
<td>$\text{Sp}_{2d}(2)$</td>
</tr>
<tr>
<td>$2^{d-1}(2^d + 1)$</td>
<td>$d \geq 3$</td>
<td>$\text{Sp}_{2d}(2)$</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>$\text{PSL}_2(11)$</td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>$M_{11}$</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>$M_{11}$</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>$M_{12}$</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>$A_7$</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td>$M_{22}$</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td>$M_{23}$</td>
</tr>
<tr>
<td>24</td>
<td></td>
<td>$M_{24}$</td>
</tr>
<tr>
<td>28</td>
<td></td>
<td>$\text{PSL}_2(8)$</td>
</tr>
<tr>
<td>176</td>
<td></td>
<td>$\text{HS}$</td>
</tr>
<tr>
<td>276</td>
<td></td>
<td>$\text{Co}_3$</td>
</tr>
</tbody>
</table>

($q = q_0^f$, with $q_0$ prime)
Table 2

| socle     | $G | \text{divides} | e | q_0^e - 1 |
|-----------|-----------------|---|-------------|
| $\text{PSL}_d(q)$ | $\prod_{i=0}^{d-1} (q^d - q^i - 1)f q^{d(d-1)/2}$ | df | n(q-1) |
| $\text{PSU}_d(q)$ | $(q^3 + 1)q^3(q^2 - 1)f$ | 6f | n(q^3 - 1) |
| $^2B_2(q)$ | $(q^2 + 1)q^2(q - 1)f$ | 4f | n(q^2 - 1) |

referenced by * in Table 1. In these cases we define $e$ as shown in Table 2.

By a theorem of Zsigmondy [19] (see also [20, p. 508]), with several exceptions there is a prime $p$ such that the multiplicative order of $q_0 \pmod{p}$ is $e$ and $p$ does not divide $e$. The exceptional cases are $e = 2$, $q_0 + 1$ is a power of 2 and $e = 6$, $q_0 = 2$. If $e$ and $q_0$ are not exceptional then the same power of $p$ divides $n$ and $q_0^e - 1$. As $n$ is square free, that power is 1. Further, from the formulas for $|G|$, it is apparent that only the first power of $p$, as chosen, divides $|G|$.

In the exceptional cases, first let $e = 2$, and $q_0 + 1$ be a power of 2. Then by the choice of $e$, the socle of $G$ is $\text{PSL}_2(q_0)$ and $n = q_0 + 1$, which is not square free. Finally, if $e = 6$ and $q_0 = 2$, then the socle of $G$ is $\text{PSL}_4(2)$, $\text{PSL}_3(4)$, or $\text{PSL}_2(8)$. $\text{PSL}_6(2)$ has degree 63 which is not square free.
SL_2(4) has degree 9 which is not square free. Finally, PSL_3(4) has degree 21, and the choice of p = 7 will satisfy the lemma. □

Hence if \langle x, y \rangle is doubly transitive but not A_n, by Lemma 2.17 there exists a prime divisor p of n such that the Sylow p-subgroups of \langle x, y \rangle have order p. Thus if n = mp, both \langle x^m \rangle and \langle y^m \rangle are Sylow p-subgroups in \langle x, y \rangle and so they are conjugate in \langle x, y \rangle. Thus there exists \beta \in \langle x, y \rangle such that \beta^{-1}x^m\beta = \langle x^m \rangle. Hence there exists k < p such that \beta^{-1}y^m\beta = x^m. Let y' = \beta^{-1}y^k\beta. Thus \langle y' \rangle is conjugate to \langle y \rangle and y'^m = x^m. Then \langle x, y' \rangle is imprimitive with respect to the orbits of \langle y^m \rangle and \langle x^m \rangle. Hence by Case 1 there exists \alpha \in \langle x, y' \rangle such that \alpha^{-1}x^{-1}y\alpha = \langle x \rangle and so \alpha^{-1}y^{-1}\beta\alpha = \langle x \rangle. □

Case 3. \langle x, y \rangle = A_n

Lemma 2.18: If n = 2k + 1, with k ≥ 2, then there are two or one conjugacy classes of regular cyclic subgroups of A_n, where there are two if n does not contain any even powers.

Proof: As any two n-cycles in S_n are conjugate, any two regular cyclic subgroups of S_n are conjugate, and thus there is only one conjugacy class of regular cyclic subgroups of S_n. Hence the number of conjugacy class of regular cyclic subgroups of A_n is one or two, and it is two if the normalizer of a regular cyclic subgroup is contained in A_n. The normalizer is the set N = \{\beta \in S_n: (x)\beta = ax + b, \}
Let \( a \in Z_n, b \in Z_n \). Let \( n = \prod_{i=1}^{m} p_i^{e_i} \), and choose numbers \( g_i \) such that the multiplicative order of \( g_i \mod (p_i^{e_i}) \) is \( p_i - 1 \) and \( g_i \equiv 1 \mod (p_j) \) for all \( j \neq i \). Since \( n \) is odd, it is sufficient to show that the permutation \( x \rightarrow g_i x \) is an odd permutation if \( e_i \) is odd. This permutation fixes the elements divisible by \( p_i^{e_i} \) and permutes the elements not divisible by \( p_i^{e_i} \) in cycles of length \( p_i - 1 \). As there are \( n(1 - 1/p_i^{e_i}) \) elements in \( Z_n \) not divisible by \( p_i^{e_i} \), the permutation will be a product of \( n(1 - 1/p_i^{e_i})/(p_i - 1) \) \( p_i - 1 \) cycles. Hence the permutation will be odd if \( n(1 - 1/p_i^{e_i})/(p_i - 1) \) is odd. Now, \( n(1 - 1/p_i^{e_i})/(p_i - 1) = n/p_i^{e_i}[(p_i^{e_i} - 1)/(p_i - 1)] \). Hence the permutation will be odd if \( (p_i^{e_i} - 1)/(p_i - 1) \) is odd. Thus the permutation is odd if \( e_i \) is odd.

As, by the hypothesis, we assume \( n \) is square free, there is only one conjugacy class of regular cyclic subgroups of \( A_n \). Hence, as \( <x> \) and \( <y> \) are regular cyclic subgroups of \( A_n = <x,y> \), they are conjugate in \( A_n \).

We have just established that if \( n = 4 \) or \( ((n) \varphi, n) = 1 \), then \( G \cong Z_n \) is a CI-group. We now prove the converse, and the proof is somewhat like Theorem B in [4], but also borrows heavily from several theorems in [3]. We first prove that:

**Lemma 2.19:** If \( G \) is non-commutative then \( G \) is not a CI-group. (c.f. [3] Lemma 2.1)
Proof: Define a function \( f: G \to G \) by \((g)f = g^{-1}\) for all \( g \in G \). Hence \( f \in S_G \). Then for any \( h \in G \),
\[
(g)(h)f^{-1} = (g^{-1}h)f^{-1} = h^{-1}g = (g)h^{-1}.
\]
Hence \( f \) is a left translation on \( G \). As well known, \( G_L \) centralizes \( G_R \) and hence \( G_R \) is normal in \( \langle G_R, fG_Rf^{-1} \rangle \). However, the non-commutativity of \( G \) implies \( G_R \neq G_L \). As \( G_R \) is normal in \( \langle G_R, fG_Rf^{-1} \rangle \), \( G_R \) and \( G_L \) cannot be conjugate, and hence \( G \) is not a CI-group.

By Lemma 2.19 we may henceforth only deal with the case when \( G \) is abelian. The remainder of the proof will be based on the following two lemmas.

**Lemma 2.20:** Let \( H \) be a subgroup of a group \( G \). Then if \( G \) is a CI-group, then \( H \) is also a CI-group.

**Proof:** Let \( G = \cup H_t \) be the right coset decomposition of \( G \) by \( H \). So each \( g \in G \) has a unique representation of the form \( g = h(g)t(g) \), where \( h(g) \in H \) and \( t(g) \in T \). Let \( f \in S_H \). Define \( f' \in S_G \) by \((g)f' = h(g)ft(g)_R \), for each \( g \in G \).

Since \( G \) is a CI-group there exists \( \beta \in \langle f^{-1}G_Rf', G_R \rangle \) such that \( f^{-1}G_Rf' = \beta^{-1}G_R\beta \). Let \( d' = [(1)\beta^{-1}]_R \beta \in \langle f^{-1}G_Rf', G_R \rangle \). Hence \( d'^{-1}G_Rd' = \beta^{-1}G_R\beta = f'^{-1}G_Rf' \) and \((1)d' = (1)(1)\beta^{-1}\beta = 1 \).

Now, the right cosets of \( G \) formed by \( H \) are a complete block system for \( G_R \) and \( f' \), and hence for \( d' \) also. Further, \((1)d' = 1\) and so \((H)d' = H \). Let \( d \) denote the restriction of
d' to H. Then the subgroup of \( d'^{-1}G_R d' = f'^{-1}G_R f' \) that fixes H is \( d'^{-1}H_R d' = f'^{-1}H_R f' \). If we restrict this equation to H, we obtain

\[
d'^{-1}H_R d = f'^{-1}G_R f.
\]

As \( d' \in <f'^{-1}G_R f', G_R> \),

\[
d' = g_{k_1R}^{e_1} [f'^{-1} g_{k_2R}^{e_2} f'] \ldots g_{k_sR}^{e_s}
\]

for some integers \( e_i \) and \( s \). Hence

\[
d = h(g_{k_1R}^{e_1}) [f'^{-1} h(g_{k_2R}^{e_2} f') \ldots h(g_{k_sR}^{e_s})
\]

and so \( d \in <f'^{-1}H_R f', H_R> \). □

**Lemma 2.21:** Let \( Q = \{(a,b,c,d) \in G^4 : ab^{-1}cd^{-1} = 1\} \). Then \( C = (G,Q) \) is a combinatorial object and \( \text{aut}(C) = \{\beta : (x) \beta = (x)\alpha h \text{ where } h \in G \text{ and } \alpha \in \text{aut}(G)\} = \text{Hol}_H \).

**Proof.** As \( Q \subseteq G^4 \), by the definition of a 4-tuple, \( C \) is a combinatorial object. Let \( (a,b,c,d) \in Q \), \( h \in G \), and \( \alpha \in \text{aut}(G) \). Then

\[
(a,b,c,d)\alpha h = ((a)\alpha h, (b)\alpha h, (c)\alpha h, (d)\alpha h)
\]

Further,

\[
(a)\alpha h [(b)\alpha h]^{-1} (c)\alpha h [(d)\alpha h]^{-1}
\]

\[
= (a)\alpha hh^{-1}(b^{-1})\alpha(c)\alpha hh^{-1}(d^{-1})\alpha
\]

\[
= (a)\alpha(b^{-1})\alpha(c)\alpha(d^{-1})\alpha
\]

\[
= (ab^{-1}cd^{-1})\alpha = (1)\alpha = 1.
\]

Thus \( \text{Hol}_G \subseteq \text{aut}(C) \).

Let \( \beta \in \text{aut}(C) \) and let \( h = (1)\beta \). Let \( \beta' = \beta h^{-1} \). Then
\( \beta' \in \text{aut}(C) \) and \((1)\beta' = 1\). Thus we may assume without loss of generality that \((1)\beta = 1\). Now, \((a,ba,b,1) \in G\) for every \(a,b \in G\). Hence

\[(a)\beta(ba)\beta^{-1}(b)\beta = 1 \text{ so } (a)\beta = (b)\beta^{-1}(ba)\beta, \text{ and hence }\]

\((b)\beta(a)\beta = (ba)\beta\). Thus \(\beta \in \text{Hol} G\). Thus \(\text{Hol} G = \text{aut}(C)\).

Note that in the above proof we did not assume that \(G\) was abelian.

Note that for a group \(G\), if \(\beta \in \text{Hol} G\), then

\[(w)\beta^{-1}g_R \beta = h^{-1}(w)\beta^{-1}g_R \beta h = h^{-1}((w)\beta^{-1}g)\beta h =\]

\[h^{-1}w(g)\beta h = (g)\beta w = (w)[(g)\beta]_R\]

Hence \(G_R\) is normal in \(\text{Hol} G\). Thus if \(G\) is not isomorphic to \(Z_n\) where \(((n)\varphi,n) = 1\), we may show \(G\) is not a CI–group by finding a subgroup \(B \leq \text{Hol} G\) such that \(B \ncong G \ncong G_R\) and \(B \ncong G_R\). Now, if \(G = A \oplus B\) and \(A' \leq \text{Hol} A\) and \(A' \ncong A \ncong A_R\), then \(A' \oplus B_R \ncong G \ncong G_R\). Hence we consider the following cases where \(G\) is isomorphic to:

1) \(Z_p^k\), \(p \geq 2\), \(k \geq 2\).

2) \(Z_p \oplus Z_p = <a,b>\), \(p\) a prime.

3) \(Z_2 \oplus Z_2 \oplus Z_2 = <a,b,c>\).

4) \(Z_4 \oplus Z_2 = <a,b>\).

5) \(Z_4 \oplus Z_4 = <a> \oplus <b>\).

6) \(Z_n\), \(n\) is square free but \(((n)\varphi,n) > 1\).

7) \(Z_4 \oplus Z_m\), \(m\) is odd and square free.

8) \(Z_2 \oplus Z_2 \oplus Z_m\), \(m\) is odd and square free.
Case 1:

Lemma 2.22. $Z_{p^2}$ is not a CI-group (c.f. [3] Lemma 2.4).

Proof. Let $G = \langle a : a^{p^2} = 1 \rangle \cong Z_{p^2}$ and define a function $b$ by $(a^k dw = a^{k^p + k + 1}$. Hence $b \in Z_{p^2}$. If $(1)b^m = 1$ then

$$m-1 \sum (p+1)^j \quad a^0 = (a^0)b^m = a^j=0,$$

hence,

$$0 \equiv \sum_{j=0}^{m-1} (p+1)^j \equiv \sum_{j=0}^{m-1} (jp+1) \equiv \frac{m(m-1)p}{2} + m \pmod{p^2}.$$Thus $m \equiv 0 \pmod{p}$, and since $p$ is odd, $\frac{m(m-1)p}{2}p \equiv 0 \pmod{p^2}$. This implies that $m \equiv 0 \pmod{p^2}$. Hence $b$ is a $p^2$-cycle.

Further, $(a^{kp^k + 1})b^{-1}a_R b = (a^k)a_R b = (a^{k+1})b = a^{kp^k + k + 1} = a^{kp^k + p + 1}$. Thus $b^{-1}a_R b = a_R^{p + 1}$, so $<a_R>$ is a normal subgroup of $<a_R,b>$. Hence $<a_R>$ and $<b>$ are not conjugate in $<a_R,b>$, and obviously $<a_R> \neq <b>$. \Box

If $k \geq 2$, then by the Sylow Theorems $Z_{p^k}$ contains a subgroup of order $p^2$. Hence by the contrapositive of Lemma 2.21, $Z_{p^k}$ is not a CI-group.

In cases 2–5 we define permutations $f,g,h$ in the following ways:

(2) $(a^x b^y)f = a^{x+y}b^y$, $(a^x b^y)g = a^{x+y}b^{y+1}$

(3) $(a^x b^y c^z)f = a^{x+y}b^y c^z$, $(a^x b^y c^z)g = a^{x+y}b^{y+1}c^z$, and

$(a^x b^y c^z)h = a^{x+y}b^yc^{y+1}$. 
(4) and (5) \((a^x b^y)f = a^{x^r}b^y\), \((a^x b^y)g = a^{x^{2r^2}y^r}b^{y^r}\).

We wish to show that the subgroups \(<f,g>\), and \(<f,g,h>\) are each contained in \(\text{Hol } G\), that the above groups are isomorphic to their respective groups \(G\), and that the are different from \(GR\).

Case 2:

We know \(f \in \text{Hol } G\) as \(f = a^R\). Now, if \(a^x b^y\) and \(a^q b^r\) then

if \((a^x b^y)\beta = a^{x\gamma} b^y\), then \((a^x b^y a^q b^r)\beta = (a^{x\gamma} b^y a^q b^r)\beta = a^{x^{\gamma\gamma} b^{\gamma\gamma}} a^{q\gamma b^{r\gamma}} = (a^x b^y)\beta(a^q b^r)\beta\). Hence \(\beta\) is a group homomorphism from \(G\) to \(G\). Let \(a^x b^y \in G\). Let \(z = x - y\). Then \((a^z b^y)\beta = a^x b^y\). Hence \(\beta\) is onto and as \(|G|\) is finite, \(\beta\) is an automorphism. As \(g = \beta b^R, g \in \text{Hol } G\).

It is not difficult to see that \(GR = <a^R,b^R>\) and that both \(GR\) and \(<f,g>\) are commutative. Define \(\alpha:GR \rightarrow <f,g>\) by \((a^x b^y)^R\alpha = \beta a^x b^y\). We assert that \(\alpha\) is onto, as \((a^x b^y)\beta = a^{x^{\gamma\gamma} b^{\gamma\gamma}} = (a^x b^y)^R\alpha (a^{r\gamma} b^{r\gamma})\), and \(\alpha\) is easily seen to be a homomorphism, and thus is an isomorphism. As \(GR\) is isomorphic to \(G\), \(<f,g>\) is isomorphic to \(G\), and \(<f,g>\) is obviously not \(GR\). \(Q\)

Note that cases 3–5 have similar proofs so will not be given here.

Case 6:

We know from elementary number theory that if \(n = p_1 \ldots p_m\) where each \(p_i\) is a prime, then

\((n)\varphi = (p_1 - 1) \ldots (p_m - 1)\).
Hence there exist primes $p_j$ and $p_k$ such that $p_j \mid (p_k - 1)$,
as $(n,n)\varphi > 1$. We show:

**Lemma 2.23:** If $n = pq$, $p$ and $q$ prime and $q \mid (p - 1)$,
then $Z_n$ is not a CI-group (c. f. [3] Lemma 2.3).

**Proof:** Let $G = \langle a, b : a^p = a^q = 1, ab = ba \rangle$. Since $q \mid \n - 1$, we can choose an $r$ such that $r$ is not congruent to 1
(mod $n$) but $r^q \equiv 1 \pmod{p}$. Define $f : Z_n \to Z_n$ by $(a^kb^j)f =
a^{kr^j}b^j$. Hence $f \in S_G$. Now,

$$(a^kb^j)f^{-1}a_R = (a^{kr^j}b^j)a_R = (a^{kr^{q^j}b^j})f = a^{kr^j}b^j$$

and similarly $(a^kb^j)f^{-1}b_R = a^{kr^jb^j}$. Straightforward
calculations will show that

$$(f^{-1}a_R)^{-1}a_R f^{-1}a_R = a_R$$

and

$$(f^{-1}b_R f)^{-1}a_R(f^{-1}b_R) = a_R^r.$$ 

Hence $\langle a_R \rangle$ is normal in $\langle G_R, f^{-1}G_R \rangle$, but $\langle a_R \rangle \neq f^{-1}\langle a_R \rangle$ are
Sylow $p$-subgroups of $G_R$ and $f^{-1}G_R f$, respectively. This
implies that $Z_n$ is not a CI-group. $\square$

As $Z_{pq}$ is not a CI-group, where $q \mid p - 1$, if

$((n)\varphi,n) > 1$, then $Z_n$ is not a CI-group by the
contrapositive of Lemma 2.20. $\square$

In the remaining cases we will examine another group $H$
such that $H \cap H$ contains isomorphic copies of $G$ that are not
conjugate.

(7) $G = Z_4 \oplus Z_m$, $m$ is odd, square free, and $m > 1$. Let
$H = \langle a, b : a^m = 1, b^4 = 1, b^{-1}ab = a^{-1} \rangle$ and $c = a$. 
(8) $G = \mathbb{Z}_2 \ast \mathbb{Z}_2 \ast \mathbb{Z}_m$, $m$ is odd and square free, $m > 1$.

Let $H = \langle a, b : a^{2m} = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$ and $c = a^2$.

In both cases let $G_1 = \langle a_R, b_L \rangle$, $G_2 = \langle a_L, b_R \rangle$. Now, $a_R$ and $b_R$ are obviously in $\text{Hol } H$. Now, each element of $H$ may be expressed in the form $a^x b^y$ as $ab = ba^{-1}$. Define $\beta : H \rightarrow H$ by $(a^x b^y)\beta = a^{-x} b^y$. Then $\beta$ is a group automorphism. Now, for each $a^x b^y$, $b(a^x b^y) = a^{-x} b^{y+1}$ as $ba = a^{-1}b$. Thus $b_L = \beta b_R$. Thus $b_L \in \text{Hol } H$. A similar argument will show that $a_L \in \text{Hol } H$. Thus both $G_1$ and $G_2$ are subgroups of $\text{Hol } H$.

We wish to consider $(a^x b^y)a_R b_L$, and will examine the cases when $y$ is even and $y$ is odd separately. If $y$ is odd then $(a^x b^y)a_R b_L = (a^x b^y)a b_L = (a^{-x} b^y)b \beta b_R = a^{-x} b^{y+1} = ab^{-x} b^y = aba^x b^y = ba^{-x} b^y = (a^x b^y)b_L = (a^x b^y)b_L = b_L a_R$. If $y$ is even, then $(a^x b^y)a_R b_L = (a^x b^y)a \beta b_R = (a^{x+1} b^y)\beta b_R = a^{-x-1} b^{y+1} = ba^{-x-1} b^y = ba^{-x} b^y = (a^x b^y)b_L a_R$. Hence every element of $G_1$ is expressible as $a^x b^y a_R b_L$, and $G_1$ is abelian. This implies that $|G_1| = |G|$. Define $\alpha : G_1 \rightarrow G$ by $(a^x b^y a_R b_L) = d^x e^y$ where $G = <d, e : |d| = |a|$ and $|b| = |e|>$. Then $(a^x b^y a_R b_L)\alpha = (b_L a_R^{-1})\alpha = d^x e^{y+1} = d^x e^y d^x e^y = (b_L a_R^{-1})\alpha (b_L a_R^{-1})\alpha = (a_R b_L)^x (a_R b_L)^y \alpha$. Thus $\alpha$ is a homomorphism and thus an isomorphism. A similar argument will show that $G_2 \cong G$.

Now $<c_R>$ is the unique subgroup of order $m$ both in $G_1$ and $H_R$. $H_R$ is normal in $\text{Hol } H$, hence $<c_R>$ is also normal in $\text{Hol } H$. Similarly $<c_L>$ is the unique subgroup of order $m$ in
$G_2$ and $\langle c_L \rangle$ is also normal in $\text{Hol } H$. But $\langle c_L \rangle \neq \langle c_R \rangle$, and so $G_1$ and $G_2$ cannot be conjugate in $\text{Hol } H$. $\Box$
CHAPTER II REFERENCES


CHAPTER III

PRODUCTS OF TWO PRIMES

In this section we prove that \( Z_{pq} \), where \( p \) and \( q \) are distinct primes, is a CI-group with respect to graphs and digraphs. As mentioned in the introduction, several authors have published this result. The proof we show is by Alspach and Parsons [10].

Let \( \mathcal{C} \) be the class of cyclic graphs and \( \mathcal{C} \mathcal{D} \) the class of cyclic digraphs. Then;

**Theorem 3.1:** \( Z_{pq} \) is a \( (\mathcal{C} \mathcal{D}) \)-CI-group where \( p \) and \( q \) are distinct primes.

**Proof:** Let \( X = \Gamma(n,T) \), where \( n = pq \), \( p \) and \( q \) both prime with \( q < p \), be a cyclic (di)graph. As in Chapter 2, let \( x = (1 \ 2 \ \ldots \ \ n) \), \( z_i = (i \ i+q \ \ldots \ i+(p-1)q) \) where \( 1 \leq i \leq q \). As before, \( z_i \) is a \( p \)-cycle and \( x^q = z_1 \ldots z_q \).

Let \( P \) be any Sylow \( p \)-subgroup of \( \text{aut}(X) \). Note that \( |<x^q>| = p \) and so \( x^q \in P_0 \), where \( P_0 \) is some Sylow \( p \)-subgroup of \( \text{aut}(X) \). Hence by the Sylow theorems there is a \( \beta \in \text{aut}(X) \) such that \( \beta^{-1}P_0\beta = P \). Then \( \beta^{-1}z_1 \ldots z_p\beta \in P \). Let \( \alpha_i = \beta^{-1}z_i\beta \). Then \( \alpha = \alpha_1 \ldots \alpha_q \in P \). Hence every Sylow \( p \)-subgroup of \( \text{aut}(X) \) contains an element that is the product of \( q \) disjoint \( p \)-cycles.

Let \( P \) be any Sylow \( p \)-subgroup of \( \text{aut}(X) \). Consider the action of \( P \) on \( Z_n \). As \( P \leq S_n \), \( p \leq |P| \leq p^q \). Then the orbit
of any \( i \in \mathbb{Z}_n \) under the action of \( P \) has cardinality \( p^r \) where \( p \leq p^r \leq n < p^2 \). Then \( r = 1 \) and the cardinality of the orbit of \( i \) is \( p \). Further, \( P \) contains some \( \alpha = \alpha_1 \ldots \alpha_q \) and hence the orbit of \( i \) is exactly the set \( A_i \), where \( A_i = \{ j : (j) \alpha_i \neq j \} \).

Let \( W = \langle \alpha_i : 1 \leq i \leq q \rangle \). Then

**Lemma 3.2:** \( P \leq W \), \( P \) is abelian and if \( \tau \in W \) so that \( \tau \in \text{aut}(X) \) then \( \tau \in P \).

**Proof:** If \( \beta \in P \), the restriction of \( \beta \) to \( A_i \), \( \beta | A_i \), is a permutation of the elements of \( A_i \). Then the mapping \( \beta \rightarrow \beta | A_i \) is a homomorphism of \( P \) onto a nontrivial \( p \)-subgroup of the symmetric group \( S_p(A_i) \) on \( A_i \). Since the nontrivial \( p \)-subgroups of \( S_p(A_i) \) are Sylow and cyclic of order \( p \), the image of \( P \) is \( \langle \alpha_i \rangle \). Thus the elements of \( P \) are of the form \( \alpha_1^{e_1} \ldots \alpha_q^{e_q} \) for some integers \( e_1, \ldots, e_q \) where \( e_j \leq p \). Hence \( P \leq W \) and \( P \) is abelian. Further, suppose \( \tau \in \text{aut}(X) \cap W \) but \( \tau \notin P \). Then the subgroup of \( \text{aut}(X) \) generated by \( P \) and \( \tau \) has cardinality greater than \( |P| \). But \( P \) is a Sylow \( p \)-subgroup of \( \text{aut}(X) \), a contradiction. \( \square \)

Let \( M(P) = \{ \theta : \theta \alpha_i \theta^{-1}, \theta \alpha_2 \theta^{-1}, \ldots, \theta \alpha_q \theta^{-1} \text{ is some permutation of } \alpha_i, \ldots, \alpha_q \} \). Then

**Lemma 3.3:** \( M(P)/P \) is a factor group and can be viewed as a permutation group on the set \( \{ \alpha_1, \ldots, \alpha_q \} \).

**Proof:** Clearly, \( P \) is normal in \( M(P) \) and so \( M(P)/P \) is a factor group. If \( \theta \in P \), then \( \theta \alpha_i \theta^{-1} = \alpha_i \) for each \( i \leq q \).
Conversely, if $\theta \in \mathcal{M}(P)$ and $\theta \alpha_i \theta^{-1} = \alpha_i$ for each $i \leq q$, then for each $i$, $\theta$ maps the elements of the cycle $\alpha_i$ cyclicly onto themselves. Thus $\theta = a_i^{e_i} \cdots a_q^{e_q}$ for suitable choices of the $e_i$'s. Then by Lemma 3.2, $\theta \in \mathcal{W}$ and hence $\theta \in P$. Then the factor group $\mathcal{M}(P)/P$ acts faithfully on the set \{a_1, \ldots, a_q\}, and thus $\mathcal{M}(P)/P$ may be regarded as a permutation group on \{a_1, \ldots, a_q\}. \Box

Note that up until now, the above comments and proofs have not used the fact that $q$ is prime, and hence are also true when $q$ is not prime.

We now split the proof into two cases. Case 1 will consider when the Sylow $p$-subgroups of $\text{aut}(X)$ have order $p$, and Case 2 will consider when the Sylow $p$-subgroups of $\text{aut}(X)$ have order $p^r > p$.

Case 1. The Sylow $p$-subgroups of $\text{aut}(X)$ have order $p$.

Let $y$ be an $n$-cycle contained in $\text{aut}(X)$. Then $y^q = a_1 \cdots a_q$, for some disjoint $p$-cycles $\alpha_i$, where $1 \leq i \leq q$. Then $P = \langle y^q \rangle$ is a Sylow $p$-subgroup of $\text{aut}(X)$ as is $\langle x^q \rangle$.

Thus by the Sylow theorems there is a $\rho \in \text{aut}(X)$ such that $\rho^{-1} \langle x^q \rangle \rho = \langle y^q \rangle$. Then there is an integer $r$ so that $\rho^{-1} (x^q)^r \rho = y^q$. Hence $r$ or $r + p$ is an integer $k$ so that $k$ is relatively prime to $n$ and $\rho^{-1} (x^q)^k \rho = y^q$. Thus $\rho^{-1} x^k \rho = \lambda$ is an $n$-cycle in $\text{aut}(X)$ and $\lambda^q = y^q = a_1 \cdots a_q$. In fact, $\lambda$ and $\tau$ are actually in $\mathcal{M}(P)$.

As shown in Lemma 3.2, $\mathcal{M}(P)/P$ can be regarded as a
permutation group on the set \( \{\alpha_1, \ldots, \alpha_q\} \). Thus the corresponding permutations \([\tau]\) and \([\lambda]\) are \(q\)-cycles in \(M(P)/P\) as \(\lambda^q = \alpha = \alpha_1 \ldots \alpha_q\). Then the corresponding subgroups \(<[\tau]>\) and \(<[\lambda]>\) are Sylow \(q\)-subgroups of \(M(P)/P\), so they are conjugate. Let \([\theta] \in M(P)/P\) such that \([\theta]^{-1}[\lambda][\theta] = [\tau]\). Then there is an integer \(s < q\) with \([\theta]^{-1}[\lambda]^s[\theta] = [\tau]\), and so in \(M(P), \theta^{-1}\lambda^s\theta^{-1} \in <\alpha> = P\). Hence there is an integer \(r\) with \(r \in Z\) such that \(\theta^{-1}\lambda^s\theta^{-1} = (\tau^q)^r\) and so \(\theta^{-1}\lambda^s\theta = \tau^{qr+1}\). Since \(1 < s < q < p\), \(\lambda^s\) is an \(n\)-cycle in \(\text{aut}(X)\) and so \(\tau^{qr+1}\) is also an \(n\)-cycle. Hence \(<\tau^{qr+1}> = <\tau>\) and so \(<x>\) and \(<\tau>\) are conjugate in \(\text{aut}(X)\). Hence by Corollary 2.4, \(Z_n\) is a \((D)\) \(\mathcal{G}\)-CI–group.

Case 2. The Sylow \(p\)-subgroups of \(\text{aut}(X)\) of order \(p^e > p\).

As before, let \(y\) be an \(n\)-cycle in \(\text{aut}(X)\). Let \(P\) be a Sylow \(p\)-subgroup of \(\text{aut}(G)\) that contains \(y^q = \alpha = \alpha_1 \ldots \alpha_q\), where the \(\alpha_i\)'s are disjoint \(p\)-cycles with underlying set \(A_i = \{j: (j)\alpha_i \neq j\}\). Again, consider the action of \(P\) on \(Z_n\). As the orbits under \(P\) are the sets \(A_i\) and \(|A_i| = p\), if \(G_i = \{\beta: (i)\beta = i\}\) is the stabilizer of \(i\), then \(|G_i| = p^{e-1} > p\). We define an equivalence relation on \(Z_n\) by \(i \equiv j\) if and only if \(G_i = G_j\). Let \(C_i\) denote the equivalence class that contains \(i\).

**Lemma 3.4:** \(C_i = A_i\).

**Proof:** Recall from Lemma 3.2 that if \(\beta \in P\), then \(\beta = \alpha_1^{e_1} \ldots \alpha_q^{e_q}\) for suitable choices of the \(e_i\)'s. Suppose that \(i, j \in A_k\). Then \(\beta \in G_i\) if and only if \(e^k = 0\) if and only if
\( \beta \in G_j \), and thus \( i \equiv j \). Hence \( |C_i| \geq p \). As each \( C_i \) is nontrivial, there are \( i,j \) such that \( i \equiv j \). Thus \( |C_i| < n \).

Let \( i,j \in Z_n \), where \( i \neq j \). Then there exists an integer \( r \in Z_n \) so that \( (i)y^r = j \). Since \( y^r \in M(P) \), \( y^rPy^r = P \). Let \( \beta \in G_i \). Then \( (j)y^r\beta y^r = (i)\beta y^r = (i)y^r = j \), and hence \( y^rG_iy^r \leq G_j \), with equality holding as \( |G_i| = |G_j| \). If \( k \equiv j \), then \( (k)y^r\gamma y^r = (k)\gamma y^r = (k)y^r \). Hence \( G_j = G_k \) for every \( k \equiv j \). Hence \( C_iy^r \leq C_j \) and so \( |(C_i)y^r| \leq |C_j| \), with equality holding by symmetry. Hence each equivalence class \( C_k \) has the same cardinality, \( s \), where \( q < p \leq s < pq \) and \( s \) must divide \( pq \). Hence \( s = p \). Thus \( C_i = A_i \).

Lemma 3.5: \( P = W \).

Proof: Let \( 1 \leq r,s \leq q \), where \( r \neq s \), and suppose that \( i \in A_r \) and \( j \in A_s \). Then by Lemma 3.4 there exists \( \beta \in P \) such that \( (i)\beta = i \) and \( (j)\beta \neq j \). By Lemma 3.2, \( \beta = \alpha_1^{e_1}\ldots\alpha_q^{e_q} \), so \( e_r = 0 \) and \( 0 < e_s < p \). Therefore, as \( \langle \alpha_s^{e_s} \rangle = \langle \alpha_s \rangle \), if \( i - j \in T \), then \( (i)\beta - (j)\beta = i - (j)\beta \in T \), and hence \( (i,a) \in T \) where \( a \in A_s \). As \( X \) is a (di)graph, we have all possible edges from \( i \) to any vertex in \( A_s \). If \( X \) is a graph, we have all possible edges between the vertices of \( A_r \) and the vertices of \( A_s \). If \( X \) is a digraph, we have all possible edges from \( A_r \) to \( A_s \), or all possible edges from \( A_s \) to \( A_r \), or all possible edges between \( A_r \) and \( A_s \), or no edges between \( A_r \) and \( A_s \). Now \( y^q \in \text{aut}(X) \), and \( (i)y^q = (i)\alpha_j \) for every \( i \in A_j \). Thus if \( i,k \in A_j \), with \( i \neq k \), then \( i - k \in T \) if and only if
(i) \(a_j \sim (k) a_j \in T\).

Now suppose that \(i \in A_j\) and \(k \in A_s\) with \(r \neq s\). If \(X\) is a graph then \(i - k \in T\) if and only if there is an edge between each vertex of \(A_r\) and each vertex of \(A_s\). Hence \(i - k \in T\) if and only if there is an edge between \((i)a_j\) and \((k)a_j = k\), i.e. if \((i)a_j - k \in T\). Finally note that if \(i \neq k\) and \(i, k \notin A_j\), then \((i)a_j = j\) and \((k)a_j = k\). Analogous remarks hold for \(X\) a digraph. Hence \(a_j \in \text{aut}(X)\) for each \(j\), and by Lemma 3.2, \(P = W. \square\)

Let \(Y = \Gamma(n,T')\) be a cyclic (di)graph isomorphic to \(X\). Let \(E_j = \{i: (i)z_j \neq i\}, U = \{i: i \in T\) and \(i\) is not congruent to \(0 \mod q\}\), \(V = \{i \in \mathbb{Z}_q: qj + i \in T\) where \(j \in \mathbb{Z}_p\}\), and define \(U'\) and \(V'\) similarly. Then

Lemma 3.6: There exist a unit \(r \in \mathbb{Z}_q\) such that \(U = rU'\).

Proof: As \(X \cong Y\) there exists a bijection \(\pi: \mathbb{Z}_n \to \mathbb{Z}_n\) such that \(\pi\) is an isomorphism from \(Y\) to \(X\). As \(x \in \text{aut}(Y)\), \(\pi^{-1}x\pi \in \text{aut}(X)\) and \(\pi^{-1}x\pi\) is an \(n\)-cycle. As \(y\) was originally taken to be an arbitrary \(n\)-cycle, we may assume without loss of generality that \(y = \pi^{-1}x\pi\). Let \(P_0\) be the Sylow \(p\)-subgroup of \(\text{aut}(X)\) containing \(x^q\). As \(P\) and \(P_0\) are Sylow \(p\)-subgroups of \(\text{aut}(X)\), there exists \(\rho \in \text{aut}(X)\) such that \(\rho^{-1}P\rho = P_0\). Then \(\pi\rho\) is another isomorphism from \(Y\) to \(X\) and \(\rho^{-1}y^q\rho \in P_0\). Hence we may assume without loss of generality the \(P = P_0\) and hence the \(E_j\)'s are a permutation of the \(C_i\)'s. This
assumption forces \( \rho \) to be the identity.

Now, \( x, y \in M(P_0) \) and by Lemma 3.3, the factor group \( M(P_0)/P \) may may be regarded as a permutation group on the set \( \{z_i : 1 \leq i \leq q\} \). Hence the permutations \( [x] \) and \( [y] \) are q–cycles and \( A_j = E_j[y] \). As \(|\{z_i : 1 \leq i \leq q\}| = q\), \( [x] \) and \( [y] \) are Sylow q–subgroups of \( M(P_0)/P \) and hence there exists \( \theta \in M(P_0) \) such that \( [\theta]^{-1}[y][\theta] = [x] \). Thus for some integer \( r \) with \( (r, q) = 1 \), \( [\theta^{-1}y\theta] = [x^r] = z_r \). Hence \( \pi\theta \) is another isomorphism from \( Y \) to \( X \). Let \( y' = (\pi\theta)^{-1}x\pi\theta \).

Hence \( y' \) is an n–cycle and \( y' = \theta^{-1}y\theta \), as above we assumed \( y = \pi^{-1}x\pi \). Thus \( y' \in M(P_0) \) and hence \( [y'] = [\theta^{-1}y\theta] = [x^r] \).

Hence \( [y'] \) permutes the p–cycles \( z_i \) as \( (z_r, z_{2r}, \ldots, z_{qr}) \) and thus \( y' \) may be viewed as permuting the sets \( E_i \) cyclicly as \( (E_r, E_{2r}, \ldots, E_{qr}) \). Note that if \( (0)\pi\theta \in E_{rk} \) then \( (E_q)\pi\theta = E_{rk} \), \( (E_i)\pi\theta = E_{rk+k} \), and so \( (E_j)\pi\theta = E_{rk+j} \).

Now, if \( i \in V \), then for some \( j \), \( qj + i \in T \), and so there is an edge \( (0, qj + i) \) in \( X \). Hence every vertex in \( E_0 \) is adjacent to every vertex of \( E_i \), by an argument presented in Lemma 3.5. Hence \( U = \bigcup_{i \in Y} E_i \). A similar result holds for digraphs.

Similarly, if \( i \in V' \), then for some \( j \), \( qj + i \in T' \), and so there is an edge \( (0, qj + i) \) in \( Y \). Henceforth we will only discuss graphs, but note that the arguments are valid for digraphs as well. Now \( 0 \in E_q \) and \( qj + i \in E_i \) so \( (0)\pi\theta \in E_{rk} \), and \( (qj + i)\pi\theta \in E_{rk+rqj+rj} = E_{rk+rj} \). Further, \((qj + 1)\pi\theta - \ldots
(0) \( \pi \theta \in T \). Thus every vertex of \( E_{rk} \) is adjacent in \( X \) to every vertex of \( E_{rk+rj} \). As \( (\pi \theta)^{-1} \) is an isomorphism from \( X \) to \( Y \), every vertex of \( E_q \) is adjacent in \( Y \) to every vertex in \( E_i \). Hence \( U' = \bigcup_{i \in Y} E_i \). Now, \( i \in Y' \) if and only if \( ri \in Y \). As \( 1 \leq r \leq q \), \( r \) is a unit in \( \mathbb{Z}_q \) and \( E_{ri} = rE_i \). Hence \( U = \bigcup_{i \in Y} E_{ri} = rU \bigcup_{i \in Y} E_i = rU' \). □

By the above proof, \( (E_q)\pi \theta = E_{rk} = E_t \) where \( t \in \mathbb{Z}_q \) and \( rk \equiv t \mod q \). Let \( Z = \{ i \in \mathbb{Z}_p : qi \in T \} \) and define \( Z' \) similarly. Let \( X' = \Omega(p,Z) \) and \( Y' = \Omega'(p,Z') \) be two cyclic graphs of order \( p \). Let \( \beta : \mathbb{Z}_p \to \mathbb{Z}_p \) be defined by \( (i)\beta = j \) if and only if \( (qi)\pi \theta = qj + t \). Then

**Lemma 3.7**: \( \beta \) is an isomorphism from \( Y' \) to \( X' \).

**Proof**: Let \( i,j \in \mathbb{Z}_p \) such that \( i - j \in Z' \). Then \( q(i - j) \in T \) and so there is an edge \( (qi,qj) \) in the graph \( Y \).

Hence \( (qi)\pi \theta - (qj)\pi \theta \in T \) and so \( [q(i)\beta + t] - [q(j)\beta + t] = q[(i)\beta - (j)\beta] \in T \). This implies that \( (i)\beta - (j)\beta \in Z \). □

By Theorem 2.5, \( \mathbb{Z}_p \) is a CI–group and hence there exists a unit \( s \in \mathbb{Z}_p \) such that \( Z = sZ' \). Hence, by the Chinese Remainder Theorem, there exists a unit \( u \in \mathbb{Z}_{pq} \) such that \( u \equiv r \mod q \) and \( u \equiv s \mod p \). Thus \( uE_i = E_{ui} = E_{ri} = rE_i \) and hence \( uU' = rU' = U \). Similarly, \( uZ' = sZ' = Z \mod p \) and so \( u(qZ') = quZ' = qsZ' = qZ \). Therefore, \( T = qZ \cup U = u(qZ') \cup (uU') = u(qZ' \cup U') = T' \). □
CHAPTER IV.

PRODUCTS OF PRIMES

As mentioned earlier, Ádám's conjecture is not true for digraphs or graphs. The first counter examples found were by Elspas and Turner [6]. We consider the digraph first.

Let \( \Gamma(8, T) \) and \( \Gamma(8, T') \) be cyclic digraphs where \( T = \{1, 2, 5\} \) and \( T' = \{1, 5, 6\} \). The units in the field \( \mathbb{Z}_8 \) are 1, 3, 5, and 7. It is easy to check that \( T \neq kT' \) where \( k = 1, 3, 5, \) or 7. However, \( \Gamma(8, T) \not\cong \Gamma(8, T') \) by the mapping \( t(i) = 4 \left\lfloor \frac{i+1}{2} \right\rfloor + 1, \) \( i \in \mathbb{Z}_8 \),

where \( \lfloor j \rfloor \) is the greatest integer less that or equal to \( j \).

For the case of graphs, let \( \Gamma(16, T) \) and \( \Gamma(16, T') \) be cyclic graphs where \( T = \{1, 2, 7, 9, 14, 15\} \) and \( T' = \{2, 3, 5, 11, 13, 14\} \). The units in the field \( \mathbb{Z}_8 \) are the odd integers less that 16. As both are graphs, \( 1 \in T, T' \) must be mapped to an odd integer, we only need to consider \( k = 3 \) or 5. If \( k = 3 \), then 2 is mapped to 6 \( \not\in T' \). If \( k = 5 \), then 2 is mapped to 10 \( \not\in T' \). However \( \Gamma(16, T) \not\cong \Gamma'(16, T') \) by the mapping \( i \rightarrow i \) (if \( i \) is even), \( i \rightarrow i + 1 \) (if \( i \) is odd).

A much more general result showing that Adam's conjecture is false was proven by Alspach and Parsons [8]. They were able to characterize when a cyclic (di)graph defined on \( \mathbb{Z}_p \) has the Cayley isomorphism property, and the
proof is similar to the proof of Theorem 3.1. More specifically, let \( (\mathcal{D}) \) be the class of (di)graphs. Let \( G = \Gamma(p^2, T) \) be a cyclic (di)graph with connection set \( T \). Let \( V = \{ i \in T : i \equiv 0 \pmod{p} \} \) and \( U = T - V \). Hence \( U \cup V = T \).

For \( J \subseteq Z_{p^2} \), let \( I(J) = \{ i \in Z_{p^2}^*: iJ = J \} \) where \( Z_{p^2}^* \) is the group of units in the ring \( Z_{p^2} \), and denote by \( I(J) \cdot I(K) \) the subgroup of \( Z_{p^2}^* \) generated by \( I(J) \cup I(K) \). As before, let \( x = (1 \ 2 \ \ldots \ p^2) \), and \( z_i = (i \ p + i \ \ldots \ p(p - 1) + i) \). Then:

**Theorem 4.1:** If \( U \) is not empty and \( U \) is not a union of cosets of the form \( <p> + j, j \notin <p> \), then \( G \) has the Cayley isomorphism property. Otherwise, \( G \) has the Cayley isomorphism property if and only if \( I(U) \cdot I(V) = Z_{p^2}^* \). If \( G \) does not have the Cayley isomorphism property then \( G \cong G' = \Gamma'(p^2, T') \) if and only if there exist \( r, s \in Z_{p^2}^* \) such that \( U = rU' \) and \( V = sV' \), where \( U' \) and \( V' \) are defined analogously to \( U \) and \( V \).

**Proof:** If the Sylow \( p \)-subgroups of \( \text{aut}(G) \) have order \( n = p^2 \), then for any \( n \)-cycle \( y \in \text{aut}(G) \), \( <x> \) and \( <y> \) are Sylow \( p \)-subgroups of \( <x, y> \) and so are conjugate. Thus we may assume that the Sylow \( p \)-subgroups of \( \text{aut}(G) \) have order \( p^e > p^2 \). Further, \( p^e \) divides \( p^2! \), so \( 2 < e \leq p + 1 \). Let \( P_0 \) be the Sylow \( p \)-subgroup containing \( x \). Then

**Lemma 4.2:** \( P_0 = <x, z_i : 1 < i < p> \).

**Proof:** Consider the action of \( P_0 \) on \( Z_n \). The orbit under \( P_0 \) of any \( i \in Z_n \) has cardinality \( n \), and as the size of
the orbit equals the index of the stabilizer $G_i$ in $P_0$, $|G_i| = p^{e-2} > p$. Define an equivalence relation on $Z_n$ by $i \equiv j$ if and only if $G_i = G_j$, and let $C_i$ denote the equivalence class that contains $i$. As $G_i$ is nontrivial there exists $j \in Z_n$ such that $i$ is not congruent to $j$. Thus $|G_i| < p^2$ for each $i \in Z_n$.

Now, if $i, j \in Z_n$, there exists $r \in Z_n$ such that $(i)x^r = j$. Since $x \in P_0$, $x^{-1}P_0x^r = P_0$. Hence $x^{-1}G_ix^r = G_j$ and so $(C_i)x^r = C_j$. Hence all equivalence classes have the same cardinality $m < p^2$, and since the sets $C_k$ form a partition of $Z_{p^2}$, $m$ divides $p^2$ and so $m = p$, or $m = 1$. If $G_i$ acts on $Z_n$ then there are $m$ orbits of cardinality one and the remaining orbits have cardinality $p$. Hence $p$ divides $p^2 - m$ and thus $m = p$. Now $(C_i)x^k = C_{i+k}$ where $i + k$ is computed modulo $n$, we may let $<x>$ act on the set of equivalence class $\{C_i : 1 \leq i \leq p^2\}$. This action is transitive, and as each equivalence class contain $p$ elements, has one orbit or cardinality $p$. Thus the stabilizer of each $C_i$ under the action of $<x>$ has cardinality $p$ and is thus the order $p$ subgroup $<x^p>$. Hence $C_i = \{j : (j)z_i \neq j\}$. Thus $C_j$ is the coset $C_0 + j$ of the subgroup $C_0 = <p>$.

Now, if $i$ is not congruent to $j$, then there exists $\beta \in G_i$ such that $\beta \in G_j$. Hence if $G$ is a graph, there is an edge between each element of $C_i$ and each element of $C_j$ or there are no edges between any element of $C_i$ and any element of
If $G$ is a digraph, then there is an edge from each element of $C_i$ to each element of $C_j$, or there is an edge from each element of $C_j$ to each element of $C_i$, or all possible edges between $C_i$ and $C_j$, or no edges at all between $C_i$ and $C_j$. Hence each $z_i \in \text{aut}(G)$. Notice that $<z_i:1 \leq i \leq p>$ is a subgroup of $\text{aut}(G)$ and has cardinality $p^p$. As $x \notin <z_i:1 \leq i \leq p>$, $<x,z_i:1 \leq i \leq p>$ is an order $p^{p+1}$ subgroup of $\text{aut}(G)$ and is hence a Sylow $p$-subgroup. As $P_0$ was any Sylow $p$-subgroup of $\text{aut}(G)$, we may assume that $P_0 = <x,z_i:1 \leq i \leq p>$. □

**Lemma 4.3:** The Sylow $p$-subgroups of $\text{aut}(G)$ have cardinality $p^{p+1}$ if and only if $U$ is the union of cosets of the form $<p> + j, j \notin <p>$. 

**Proof:** We first show that if the Sylow $p$-subgroups of $\text{aut}(G)$ have cardinality $p^{p+1}$, then $U$ is the union of cosets of the form $<p> + j, j \notin <p>$. 

By the above Lemma 4.2, we know that if the Sylow $p$-subgroups have order $p^{p+1}$, then $P_0$ is a Sylow $p$-subgroup. We consider the case of graphs only but note that the proof is analogous for digraphs.

Now, the sets $C_i$ and $C_j$ are connected by all possible edges or no edges at all. If they are connected then $(kp + i,tp + i)$ is an edge for all $k,t \in \mathbb{Z}_p$. Hence $(k - t)p + (i - j) \notin T$. Now $(k - t)p + (i - j) \in U$ if and only if $i \neq j$. Hence $<p> + (i - j) \notin U$. Further, suppose
If \( k,j \in \mathbb{Z}_p \) with \( j \neq 0 \) where \( kp + j \in U \). Now, \( z_j \in \text{aut}(G) \) so \( z_j^i \in \text{aut}(G) \) for \( i \in \mathbb{Z}_p \). This implies that \( ip + j \in U \) for every \( i \in \mathbb{Z}_p \).

Conversely, suppose \( U = \bigcup_{j \in Y<p>} j \), with \( Y \subseteq \mathbb{Z}_p^* \). Again we only consider graphs but note that the case for digraphs is analogous. Then the sets \( C_i \) and \( C_j \) are joined by no edges of \( G \) if \( j - i \notin Y \) or by all \( p^2 \) edges if \( j \in Y \). This implies that \( z_i \in \text{aut}(G) \) for every \( i \), by a previous argument, and consequently, the Sylow \( p \)-subgroups of \( \text{aut}(G) \) have order \( p^e \geq p^d > p^2 \). Hence by a previous argument, the order of the Sylow \( p \)-subgroups if \( p^{p+1} \). □

**Corollary 4.4:** If \( U \) is not the union of cosets of the form \( \langle p \rangle + j, j \notin \langle p \rangle \), then \( G \) has the Cayley isomorphism property.

**Proof:** By Lemma 4.3, the Sylow \( p \)-subgroups of \( \text{aut}(G) \) do not have order \( p^{p+1} \), and hence by a previous argument must have order \( p^2 \). □

As in Chapter III, let \( M(P_0) \) be the subgroup of \( \text{aut}(G) \) consisting of all \( \theta \in \text{aut}(G) \) such that \( \theta^{-1}z_i^0, \theta^{-1}z_2^0, \ldots, \theta^{-1}z_p^0 \) is some permutation of \( z_1, z_2, \ldots, z_p \). Now, \( x \in M(P_0) \) and it is apparent that \( \theta^{-1}z_i^0 = z_i \), for all \( i \), if and only if there exist integers \( e_1, e_2, \ldots, e_p \) such that \( \theta = z_1^{e_1} \ldots z_p^{e_p} \).

Hence \( \theta^{-1}z_i^0 = z_i \), for all \( i \), if and only if \( \theta \in K_0 = \langle z_i : 1 \leq i \leq p \rangle \). Thus the factor group \( M(P_0) \) may be regarded as a permutation group on the set \( \{z_1, z_2, \ldots, z_p\} \).
Let $G' = \Gamma(n,T')$ be a cyclic (di)graph such that $G' \subseteq G$. Then there exists a bijection $\pi: Z_n \rightarrow Z_n$ such that $\pi$ is an isomorphism from $G'$ to $G$. Let $U' = \{i \in T' : i \equiv 0 \pmod{p}\}$, and $V' = T' - U'$. Then:

**Lemma 4.5**: There exist $r, s \in Z_n^*$ such that $U = rU'$ and $V = sV'$.

**Proof**: Let $y = \pi^{-1}x\pi \in \text{aut}(G)$. Now, $y$ is in some Sylow $p$-subgroup of $\text{aut}(G)$ and by using conjugation if necessary we may assume without loss of generality that $y \in P_0$. As $y \in P_0$, $y \in M(P_0)$ and hence $x$ and $y$ determine $p$-cycles $[x]$ and $[y]$ respectively on the set $Q = \{z_1, z_2, \ldots, z_p\}$. As $M(P_0)/K_0$ is a subgroup of the symmetric group on $Q$, the subgroups $<[x]>$ and $<[y]>$ are Sylow $p$-subgroups and hence are conjugate in $M(P_0)/K_0$. Thus there exists $\theta \in M(P_0)$ such that $[\theta]^{-1}<[y]>[\theta] =<[x]>$. Hence there exists $r \in Z_p^*$ such that $[\theta^{-1}y\theta] = [x^r]$. Hence $\theta^{-1}y\theta$ permutes the sets $C_i$ cyclicly as $(C_1, C_{2r}, \ldots, C_{pr})$. Thus there exists $k \in Z_p$ such that for all $j \in Z_p$, $(C_j)y = C_{rk+j}$.

Let $X = \{i \in Z_p : ip \equiv 0 \pmod{p^2}\}$, $Y = \{i \in Z_p^* : pj + t \in T$ for some $j \in Z_p\}$ and define $X'$ and $Y'$ similarly. As in Lemma 3.6, there exists $r \in Z_p$ such that $U = rU'$ and there exists $s \in Z_p$ such that $X = sX'$ and hence $pX = spX'$ and so $V = sV'$. □

Let $r, s \in Z_n^*$ and $U', V' \subseteq Z_n$ such that $U' = r^{-1}U$ and $V' = s^{-1}V$. Let $T' = U' \cup V'$. Then $i \in T'$ if and only if $-i \in T'$. 
(in the case of graphs). Hence $G' = \Gamma(n,T')$ is a cyclic (di)graph. We now show the converse of Lemma 4.4.

**Lemma 4.5:** $G \cong G'$.

**Proof:** Define $\pi: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $(i + pj)\pi = ri + spj$, where $i, j \in \mathbb{Z}_p$. As each element of $\mathbb{Z}_n$ may be uniquely expressed in the form $i + pj$, $\pi$ is well defined. Suppose $(i + pj)\pi = (k + pt)$. Then $ri + spj \equiv rk + spt \pmod{p^2}$, so that $ri \equiv rk \pmod{p}$, as $r$ is relatively prime to $p$. Since $i, k \in \mathbb{Z}_p$, $i \equiv k \pmod{p}$. Further $spj \equiv spt \pmod{p^2}$ and thus $sj \equiv st \pmod{p}$. Again we find that $j \equiv t \pmod{p}$. Thus $i + pj = k + pt$. Hence $\pi$ is injective and thus bijective.

Let $i, j, k, t \in \mathbb{Z}_p$. Then $(i + pj, k + pt)$ is an edge in $G'$ if and only if $(i - k) + (j - t)p \in T'$. The latter holds if and only if either $i \neq k$ and $(i - k) + (j - t)p \in U'$ or $i = k$ and $p(j - t) \in V'$. The former is true if and only if $r(i - k) + sp(j - t) \in U$ if and only if $(ri + spj) - (rk + spt) \in U$. The latter holds if and only if $ri = rk$ and $sp(j - t) \in V$ if and only if $(ri + spi) - (rk + spt) \in V$. Hence $(i + pj, k + pt)$ is an edge in $G'$ if and only if $((i + pj)\pi, (k + pt)\pi)$ is an edge in $G$. Thus $\pi$ is an isomorphism of $G'$ onto $G$. □

**Lemma 4.6:** If $U$ is the union of cosets of the form $<p> + j$, $j \notin <p>$, then $G$ has the Cayley isomorphism property if and only if $I(U) \cdot I(V) = \mathbb{Z}_n^*$. 
Proof: Suppose that $I(U) \cdot I(V) \neq Z_n^*$, and let $s = 1$, and $r \in Z_n - I(U) \cdot I(V)$. Let $U' = r^{-1}U$ and $V' = V$ and $T' = U' \cup V'$. Then $G \cong G' = \Gamma(n, T')$. Let $u \in Z_n^*$ and suppose that $S = uS' = uU' \cup uV' = r^{-1}uU' \cup uV$. Since $u < p > = < p >$, and for $j \notin < p >$, $u(< p > + j) \cap < p >$ is empty. Hence $U = ur^{-1}U$ and $V = uV$. Then $ur^{-1} \in I(U)$ and $u \in I(V)$ and thus $r^{-1} \in I(U) \cdot I(V)$. But $r \notin I(U) \cdot I(V)$. Hence if $I(U) \cdot I(V) \neq Z_n^*$, then $G$ does not have the Cayley isomorphism property.

Conversely, suppose that $I(U) \cdot I(V) = Z_n^*$. If $G \cong G' = \Gamma(n, T')$, then there exist $r, s \in Z_n^*$ such that $U = rU'$ and $V = sV'$, where $U'$ and $V'$ are defined as before and $U' \cup V' = T'$. Now, $rs^{-1} \in I(U) \cdot I(V)$ and so $rs^{-1} = uv$ for some $u \in I(U)$ and $v \in I(V)$. Thus $u^{-1}r = vs = w \in Z_n^*$. Further,

$$wS' = wU' \cup wV' = wr^{-1}U \cup ws^{-1}V = u^{-1}U \cup vV = U \cup V = T'.$$

Hence $G$ has the Cayley isomorphism property. \(\diamondsuit\)

We know from Chapter II that $Z_{pr}$ is not a CI-group, but Brand [5] was able to prove a result with some generality for the case $Z_{pr}$. More specifically, for an arbitrary combinatorial object on $Z_{pr}$, where $p$ is prime, $p \neq 2$, fix $n < p$ and $m \geq \lceil \frac{r}{2} \rceil$, the ceiling function of $\frac{r}{2}$. For convenience, let $v = p^r$. Let $Q^n = \{f : Z_v \to Z_v : (x)f = \sum_{i=0}^{n} a_i x_i \}$, $a_i \in Z_v$ for each $i$, $p$ is relatively prime to $a_i$ and $p^m$ divides $a_i$ for $i = 2, \ldots, n$, and $Q^n_1 = \{f \in Q^n : (x)f = \sum_{i=0}^{n} a_i x_i \text{ with } a_i \equiv 1 \pmod{p^m} \}$. Then
Theorem 4.7: Let $B$ and $B'$ be combinatorial objects such that $Q^n_1 \subseteq \text{aut}(B)$, $p^r(n+1)-mn+1$ does not divide $|\text{aut}(B)|$, and $n < p - 1$ with $p \neq 2$ a prime. Then $B$ and $B'$ are isomorphic if and only if they are isomorphic by a map in $Q^{n+1}$.

Proof: We first prove the following lemmas:

**Lemma 4.8:** The set $Q^n$, and $Q^n_1$ are subgroups of $S_v$.

**Proof:** Let $f, g \in Q^n$ where $(x)f = \sum_{i=1}^{n} a_ix^i$ and $(x)g = \sum_{i=0}^{n} b_ix^i$. Then

\[(x)gf = \sum_{i=0}^{n} a_i \left[ \sum_{j=0}^{n} b_j x^j \right]^i = a_0 + a_i \sum_{i=0}^{n} b_i x^i + \sum_{i=2}^{n} a_i [c_0 + c_1 x]^i \]

as in the expansion of $\sum_{i=2}^{n} a_i \left[ \sum_{j=0}^{n} b_j x^j \right]^i$, if $j \geq 2$, $p^n$ divides $c_j$, where $m \geq \lceil \frac{r}{2} \rceil$, $c_j$ is raised to at least the power 2.

Now, let $(x)gf = \sum_{i=1}^{n} c_i x^i$. $p^n$ certainly divides $c_i$, where $i \geq 2$, as $p^n$ divides both $b_i$ and $a_i$. Further,

\[c_1 = a_1 b_1 + \sum_{i=2}^{n} i a_i b_1^{i-1} b_i\]

\[= a_1 b_1 + p^n \left[ \sum_{i=2}^{n} i d_i b_1^{i-1} b_i \right] \text{ where } a_i = d_i p^n.\]

Since $p$ does not divide $a_i b_1$, $p$ cannot divide $c_i$. Thus $gf \in Q^n$. Also, if $f, g \in Q^n_1$, then it is apparent that $c_1 \equiv 1 \pmod{p^n}$. Hence if $f, g \in Q^n_1$, then $gf \in Q^n_1$. 

We now only need to show that $f^{-1} \in Q^n$ (and $f^{-1} \in Q^n_1$ if $f \in Q^n_1$). Let $(x)h = \frac{n}{j=1} q_j \left( \sum_{i=0}^{n} a_i x^i - a_0 \right)^j$ where $q_j = a_i^j$ and for $i > 1$, $q_i = -a_i a_i^{i-1}$. $h$ is obviously well defined as $a_i$ is a unit in $\mathbb{Z}_v$. Also note that $h \in Q^n$ by an argument analogous to the argument above and if $f \in Q^n_1$, then $h \in Q^n_1$. Now,

$$(x)fh = \left( \sum_{j=1}^{n} q_j \left( \sum_{i=0}^{n} a_i x^i - a_0 \right) \right)^j$$

$$= \left( \sum_{j=1}^{n} q_j \left( \sum_{i=1}^{n} a_i x^i \right)^j \right)$$

$$= q_i \sum_{i=0}^{n} a_i x^i + \sum_{j=2}^{n} b_j a_i^j x^j$$

$$= \sum_{i=1}^{n} a_i^{i-1} a_i x^i + \sum_{i=2}^{n} -a_i a_i^{i-1} a_i x^i$$

$$= x + \sum_{i=2}^{n} a_i^{i-1} a_i x^i + \sum_{i=1}^{n} a_i^{i-1} a_i x^i$$

$$= x.$$  

A similar argument will show that $(x)fh = x$. Thus $Q^n$ and $Q^n_1$ are subgroups of $S_v$. □

Let $G \leq S_v$ be a subgroup containing $G_R$. Let $H(G) = \{ h \in S_v : h^{-1}th \in G, \text{ where } (x)t = x+1 \}$.

**Lemma 4.9:** Let $B$ and $B'$ be cyclic combinatorial objects. Let $P$ be any Sylow $p$-subgroup of $\text{Aut}(B)$. Then $B$ and $B'$ are isomorphic if and only if they are isomorphic by a map in $H(P)$.  

Proof: Let $f \in S_v$ be an isomorphism from $B$ to $B'$. Let $P'$ be a Sylow $p$-subgroup of $\text{aut}(B')$ which contains $T$. Since $B$ and $B'$ are isomorphic, their automorphism groups are also isomorphic. Hence $fPf^{-1} = P'$ is a Sylow $p$-subgroup of $\text{aut}(B')$. By the Sylow theorems, there is a $g \in \text{aut}(B')$ such that $gP'g^{-1} = P''$. Let $h = g^{-1}f$. Then $h$ is an isomorphism from $B$ to $B'$ and $h^{-1}h' = f^{-1}gP'g^{-1}f = f^{-1}P''f = P$.

Lemma 4.10: The map $h$ sending $(a_0, a_1, \ldots, a_n) \in [Z_v]^{n+1}$ to $f \in S_v$ given by $(x)f = \sum_{i=0}^{n} a_i x^i$ is injective if $n < p$.

Proof: If $h$ is not injective then there exist $(a_0, a_1, \ldots, a_n), (b_0, b_1, \ldots, b_n) \in [Z_v]$ such that

\[ \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} b_i x^i, \text{ and there exists some } j \text{ such that } a_j \neq b_j. \]

Thus, $\sum_{i=0}^{n} (a_i - b_i)x^i = 0$, but $a_j - b_j \neq 0$. Thus the matrix

\[
M = \begin{bmatrix}
1 & 0 & 0 & \ldots & 0 \\
1 & 2 & 3 & \ldots & n \\
1^2 & 2^2 & 3^2 & \ldots & n^2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1^n & 2^n & 3^n & \ldots & n^n
\end{bmatrix}
\]

cannot be invertible. Hence the determinant $D$ of $M$ cannot be a unit. However, $D$ is the well know Vandermonde determinant and $D = 1^{n2}2^{n-1}3^{n-2}\ldots n^1$. As $n < p$, $D$ is clearly a unit. Hence $g$ is injective. □
Lemma 4.11: If \( n < p \) then \( Q^n_i \) has exactly \( p^{r(n+1)} - mn \) elements.

Proof: Let \( f \in Q^n_i \) where \( (x)f = \sum_{i=0}^{n} a_i x^i \). The constant term \( a_0 \) can be any one of \( v = p^r \) different values. Each \( a_i \), where \( i = 1, 2, \ldots, n \) can be any one of \( p^r \) different values. By Lemma 4.10 each is unique and hence the order of \( Q^n_i \) is
\[
p^r(p^{r-m})^r = p^{r(n+1)} - mn.
\]

Lemma 4.12: \( Q^{n+1}_i \subseteq H(Q^n_i) \).

Proof: Let \( f \in Q^{n+1}_i \) where \( (x)f = \sum_{i=0}^{n+1} a_i x^i \). Recall from Lemma 4.8 that \( (x)f^{-1} = \sum_{i=0}^{n+1} b_i (x - a_0)^i \) where \( b_i = -a_i a_i^{-1} \) for \( i > 1 \). Now,
\[
(x)ftf^{-1} = ((x)f + 1)f^{-1}
\]
\[
= \left[ \sum_{i=0}^{n+1} a_i x^i + 1 \right] f^{-1}
\]
\[
= \sum_{i=1}^{n+1} b_i \left[ \sum_{j=0}^{n+1} a_j x^j + 1 - a_0 \right]^i
\]
\[
= b_i \left[ \sum_{j=1}^{n+1} a_j x^j + 1 \right] + \sum_{i=2}^{n+1} b_i (a_i x + 1)^i
\]
Hence \( ftf^{-1} \) is a polynomial of degree at most \( n + 1 \). In fact, the coefficient of \( x^{n+1} \) is \( b_i a_{n+1} - b_{n+1} a_i^{n+1} = a_i a_{n+1} - a_{n+1} a_i^1 = 0 \). Also, for \( i \geq 2 \) the coefficient of \( x^i \) is divisible by \( p^m \) as each \( a_j \) and \( b_j \) are divisible by \( p^m \), for \( j \geq 2 \). Further, the coefficient of \( x \) is
\[ b_i a_i + \sum_{i=2}^{n+1} i b_i a_i = b_i a_i + p^n \left[ \sum_{i=2}^{n+1} i d_i a_i \right] \equiv 1 \pmod{p^n} \]

where \( b_i = d_i p^n \). Thus \( f \in H(Q^n) \).

**Lemma 4.13**: If \( f \in Q^n \) has order \( v = p^r \) then \((x)f = \sum_{i=0}^{n} a_i x^i \) with \( a_0 \) relatively prime to \( p \). Further, an element \( f \in Q^n \) has order \( v \) if and only if \((x)f = cx + d\) for some \( d \) relatively prime to \( p \).

**Proof**: Let \( f \in Q^n \) and suppose that \( p \) divides \( a_0 \). Then the orbit of 0 under the action of \( <f> \) contains only elements divisible by \( p \). Hence \( f \in S_\nu \) does not generate a full \( v \) cycle. Thus \( f \) does not have order \( v \).

Let \((x)f = cx + d\). Then \((x)f^j = c^j x + d(1 + c + c^2 + \ldots + c^{j-1})\). As \( c \equiv 1 \pmod{p^n} \) let \( c = 1 + kp^n \). Hence \( c^i = 1 + ikp^n \). Also,

\[
(x)f^j = c^j x + d \left[ 1 + (1 + kp^n) + \ldots + (1 + (j-1)kp^n) \right]
\]

\[
= c^j x + d \left[ j + kp^n \frac{j(j-1)}{2} \right]
\]

If \( d \) is relatively prime to \( p \) then

\[
d \left[ p^{r-1} + \frac{p^{r-1}(p^{r-1}-1)}{2} \right] \neq 0,
\]

and thus the order of \( f \) is at least \( p^r \). Further, it is apparent from the above formulas that \((x)f^{p^r} = x\). Hence the order of \( f \) is \( p^r \).

**Lemma 4.14**: Let \( p - 1 > n \geq 1 \) and \( g \in Q^n \) have order \( p^r = v \). Then there is an \( f \in Q^{n+1} \) such that \( fgf^{-1} = t \).
Proof: We proceed by induction on \( n \). If \( n = 1 \), let \((x)g = cx + d\). As \( g \) has order \( v \), we know from Lemma 3.6 that \( d \) and 2 are relatively prime to \( p \) and \( c \equiv 1 \pmod{v} \), we can let \( f \in Q^2 \) be given by \((x)f = \frac{c^{-1} dx^2}{c+1} + \frac{2d x}{c+1}\). Then,

\[
(x)f^{-1} = \frac{1}{2}(1-c)\left[\frac{1 + c}{2d}\right]x^2 + \frac{1 + c}{2d}.
\]

We will show that \( ftf^{-1} = g \). Now,

\[
ftf^{-1} = \left[\frac{c^{-1}d(x+1)^2}{c+1} + \frac{2d(x+1)}{c+1}\right]f^{-1} = \frac{1-c}{8}\left[(c-1)d(x+1)^2 + 2d(x+1)\right]^2 + \frac{1+c}{2d}\left[\frac{c^{-1}d(x+1)^2}{c+1} + \frac{2d(x+1)}{c+1}\right]
\]

\[
= \frac{1-c}{8}\left[(c-1)(x+1)^2 + 2(x+1)\right]^2 + \frac{c-1}{2}(x+1)^2 + (x+1)
\]

\[
= \frac{-kp^n}{8}\left[kp^n(x+1)^2 + 2(x+1)\right]^2 + \frac{kp^n}{2}(x+1)^2 + (x+1)
\]

where \( c = 1 + kp^n \),

\[
= \frac{-kp^n}{8}\left[4kp^n(x+1)^3 + 4(x+1)\right] + \frac{kp^n}{2}(x+1)^2 + (x+1)
\]

\[
= \frac{-kp^n}{2}(x+1)^2 + \frac{kp^n}{2}(x+1)^2 + (x+1) = x+1 = (x)t.
\]

Let \( g \in Q^k_1 \) with order \( v \) where \( k > 2 \). It is sufficient to show that there exists \( f \in Q^{k+1} \) such that \( fgf^{-1} \in Q^{k+1}_1 \), as if we conjugate a permutation of degree \( q \), the conjugate still has degree \( q \). Let \((x)g = \sum_{i=0}^{k} b_ix^i\). Then by Lemma 4.13
b_0 is prime to p. Further, as k < p - 1, k + 1 is a unit in 
\(Z_v\). Thus we define \(a_1\) and \(a_{k+1}\) by:

\[
a_1 = b_1^{-1}
\]
\[
a_{k+1} = b_k b_1^{-2k-1} \left[ (k + 1) c_0 \right]^{-1}
\]

Now, if \((x)f = a_{k+1} x^{k+1} + a_i x\), then \(f \in Q^{n+1}\). Further,

\[
(x)fgf^{-1} = \left[ \sum_{i=0}^{k} b_i (a_{k+1} x^i + a_i x)^i \right] f^{-1}
\]
\[
= \left[ b_0 + a_i a_{k+1} x^i c_i a_i x + \sum_{i=2}^{k} b_i (a_i x)^i \right] f^{-1}
\]
\[
= -a_1^{-k-1} a_{k+2} \left[ b_0 + b_i a_i x \right]^{k+1} + a_1^{-1} \left[ b_0 + b_i a_{k+1} x^{k+1} + b_i a_i x \right.
\]
\[
\left. + \sum_{i=2}^{k} c_i (a_i x)^i \right]
\]

By a similar argument used in Lemma 4.8, the coefficient of 
\(x^j\) is 0 for \(j > k\). The coefficient of \(x^k\) is:

\[-a_1^{-k-2} a_{k+1} (k + 1) b_0 b_k a_k + a_1^{-1} b_k a_1^k\]
\[
= -b_1^{k+2} b_k b_1^{-2k-1} \left[ (k + 1) b_0 \right]^{-1} (k + 1) b_0 + b_k b_1^{-k+1}\]
\[
= -b_1 b_k + b_1 b_k^{-k+2} b_k\]
\[
= 0
\]

Thus \(fgf^{-1}\) has at most degree \(k - 1\). Further, the 
coefficient of \(x\) is:

\[-a_1^{-k-2} a_{k+1} b_k b_1 a_1 + b_1\]

As \(a_{k+1} \equiv 0 \pmod{p^n}\) and \(b_1 \equiv 1 \pmod{p^n}\), \(fgf^{-1} \in Q_{k-1}^{n+1}\). \(\Box\)
Lemma 4.16: If \( p - 1 \geq n > 2 \) then \( H(Q_n) = Q^{n+1} \).

Proof: In view of Lemma 3.6, we only need to show that \( H(Q_n) \subseteq Q^{n+1} \). Let \( h \in H(Q_n) \) and \( g = hth^{-1} \). By Lemma 3.5, there is an \( f \in Q^{n+1} \) such that \( fgf^{-1} = t \). Now, \( g = f^{-1}tf = hth^{-1} \), so \( t = hf^{-1}tfh^{-1} \). The only elements of \( S_v \) that commute with \( t \), a full \( v \) cycle, are the powers of \( t \). Thus \( hf^{-1} = t^j \) for some \( j \). Since \( Q^{n+1} \) is a subgroup of \( S_v \), \( h = t^j f \in Q^{n+1} \). □

We now have the necessary lemmas to prove Theorem 3.7.

As by assumption \( p^{mn+mn+1} \) does not divide \( |\text{aut}(B)| \), by Lemma 4.11, \( Q_n \) is a Sylow \( p \)-subgroup \( \text{aut}(B) \). Then by Lemma 4.16, \( H(Q_n) = Q^{n+1} \). Then by Lemma 4.9, \( B \) and \( B' \) are isomorphic if and only if they are isomorphic by a map in \( H(Q_n) = Q^{n+1} \). □

Let \( X \) be a finite set and \( \mathcal{S} = \{ E_i : i \in I \} \) be a family of subsets of \( X \). The ordered pair \((X, \mathcal{S})\) is said to be a hypergraph on \( X \) if for each \( i \in I \), \( E_i \) is nonempty and \( \bigcup_{i \in I} E_i = X \). \( \mathcal{S} \subseteq 2^X \) and hence a hypergraph \( H = (X, \mathcal{S}) \) is a combinatorial object. The elements of \( X \) are the vertices of \( H \) and the elements of \( E \) are called edges. The multiplicity of an edge \( E_i \) is defined to be \( |\{ j : E_j = E_i \}| \).

Let \( H = (X, \mathcal{S}) \) and \( G = (Y, \mathcal{F}) \) be two hypergraphs where \( \mathcal{S} = \{ E_i : 1 \leq i \leq m \} \) and \( \mathcal{F} = \{ F_i : 1 \leq i \leq n \} \). We will say that \( H \) and \( G \) are isomorphic if \( m = n \) and there exists a bijection \( \varphi : X \to Y \) so that \( (\mathcal{S})\varphi = \mathcal{F} \).
We will now construct examples of hypergraphs which satisfy the hypothesis of Theorem 4.7 and prove that such examples must have at least \( n + 2 \) vertices.

**Lemma 4.17:** Let \( G \) be a hypergraph with each edge having at most \( n + 1 \) vertices with \( n \geq 0 \). If the vertex set of \( G \) is \( Z_v \) and \( Q^n_1 \) is a subgroup of \( \text{aut}(G) \), then \( Q^k_1 \) is a subgroup of \( \text{aut}(G) \) for every \( k \).

**Proof:** Let \( e = \{x_1, x_2, \ldots, x_m\} \) be an edge of \( G \) with multiplicity \( d \). Let \( f \in Q^k_1 \). We shall show by induction of the degree of \( f \) that there exists \( q \in Q^n_1 \) with \((e)q = (e)f\).

If \( k < n \), then by the definition of \( Q^n_1 \), \( Q^k_1 \subset Q^n_1 \). So assume \( k > n \). Let \((x)g = (x - x_1)(x - x_2)\ldots(x - x_m)\),

\[(x)f = \sum_{i=0}^{k} a_ix^i, \text{ and } (x)f' = (x)f - a_kx^{k\cdot m}(x)g. \]

Hence

\[\deg(f') \leq \deg(f)\]

and if \((x)f' = \sum_{i=0}^{k} a'_ix^i\) then \(a'_i \equiv a_i \pmod{p^n}\) as \(a_k \equiv 0 \pmod{p^n}\). Hence \(f' \in Q^k_1\) and

\[(e)f' = \{(x_1)f - a_kx^{n\cdot m}(x_1)g, \ldots, (x_m)f - a_kx^{n\cdot m}(x_m)g\}
= (e)f.\]

As \(f' \in \text{aut}(G)\), \((e)f'\) also has multiplicity \(d\) as an edge in \(G\).

Let \( n < m < p - 1 \). We define the hypergraph \( G \) to have vertex set \( Z_v \), with the edge set being the orbit of \( 0,1,\ldots,m \) under the action of \( Q^n_1 \).

**Lemma 4.18:** \( \text{Aut}(G) = Q^n_1 \).

**Proof:** \( \text{Aut}(G) \) acts transitively on the edge set of \( G \).
as $Q^n_1$ acts transitively on the edge set of $G$ and there exists an obvious bijective function from $Q^n_1$ to the edges of $G$, $[\text{aut}(G):G_e] = |Q^n_1|$. It thus only remains to be shown that $|G_e| = 1$. Let $f \in G_e$. We will show by induction on $x$ that $(x)f = x$ for all $x \in Z_v$. Since $Q^n_1$ is a $p$-subgroup and $e$ has only $m + 1 < p$ elements, if an element fixes $e$ then it must fix each point of $e$ as the elements of $e$ cannot be contained in a $p$-cycle and avoid at least one of them being moved outside of $e$. Thus $(x)f = x$ for each $0 \leq x \leq m$, and we inductively assume that for each $m < x$ and $w < x$, $(w)f = w$. As $f$ is an automorphism of $G$ and $\{x - m, x - m - 1, \ldots , x - 1, x\}$ is an edge of $G$, $e' = \{x - m, x - m - 1, \ldots , x - 1, (x)f\}$ is an edge of $G$. Hence $(e)q = e'$ for some $q \in Q^n_1$.

Let $(x)q = \sum_{i=0}^{n} a_i x^i$. Then $(z)q \equiv z + a_0 \pmod {p^m}$ for all $z \in Z_v$. Hence $(i)q = x - m + i$ for $i < m$ or else $(0)q = (x)f$ and $(i)q = x - m + i - 1$ for $i \leq m$. Then either $(i)q = x - m + i$ for each $i \in Z_v$ or $(i)q = x - m + i - 1$ for each $i \in Z_v$, by Lemma 4.9. If the second case were true then $(0)q = x - m - 1$, but $(0)q = (x)f \neq x - m - 1$. Hence $(x)f = x - m - 1$. But $(x - m - 1)f = x - m - 1$ as $x - m - 1 < x$. Hence $(x)f = x$. \(\square\)
CHAPTER IV REFERENCES


REFERENCES

5. N. Brand, Polynomial Isomorphisms of Combinatorial Objects, Preprint.
9. D. Z. Djoković, Isomorphism Problem for a Special Class of