The Cayley Isomorphism Problem

Ted Dobson

Mississippi State University
and
The University of Primorska
dobson@math.msstate.edu

August 20, 2016

Basic Definitions and Background

Definition 1

Let G be a group and $S \subseteq G$.

Basic Definitions and Background

Definition 1

Let G be a group and $S \subseteq G$. Define a **Cayley digraph of** G*, denoted* $\mathrm{Cay}(G,S)$*, to be the digraph with* $V(\mathrm{Cay}(G,S)) = G$ *and*

Basic Definitions and Background

Definition 1

Let G be a group and $S \subseteq G$. Define a **Cayley digraph of** G*, denoted* $\mathrm{Cay}(G, S)$*, to be the digraph with* $V(\mathrm{Cay}(G, S)) = G$ *and* $E(\mathrm{Cay}(G, S)) = \{(g, gs) : g \in G, s \in S\}$.

Basic Definitions and Background

Definition 1

Let G be a group and $S \subseteq G$. Define a **Cayley digraph of** G*, denoted* $\mathrm{Cay}(G, S)$*, to be the digraph with* $V(\mathrm{Cay}(G, S)) = G$ *and* $E(\mathrm{Cay}(G, S)) = \{(g, gs) : g \in G, s \in S\}$*. We call* S *the* **connection set of** $\mathrm{Cay}(G, S)$*.*

Basic Definitions and Background

Definition 1

Let G be a group and $S \subseteq G$. Define a **Cayley digraph of** G*, denoted* $\mathrm{Cay}(G,S)$*, to be the digraph with* $V(\mathrm{Cay}(G,S)) = G$ *and* $E(\mathrm{Cay}(G,S)) = \{(g,gs) : g \in G, s \in S\}$*. We call S the* **connection set of** $\mathrm{Cay}(G,S)$.

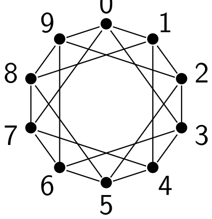


Figure: The Cayley graph $\mathrm{Cay}(\mathbb{Z}_{10}, \{1,3,7,9\})$.

Notice that

$$(x, y) \in E(\mathrm{Cay}(G, S))$$

Notice that

$$(x, y) \in E(\mathrm{Cay}(G, S)) \quad \text{if and only if} \quad \begin{array}{l}(x, y) = (g, gs) \text{ for} \\ \text{some } g \in G \text{ and } s \in S\end{array}$$

Notice that

$$
\begin{aligned}
(x, y) \in E(\mathrm{Cay}(G, S)) \quad & \text{if and only if} \quad (x, y) = (g, gs) \text{ for} \\
& \qquad\qquad\qquad\quad \text{some } g \in G \text{ and } s \in S \\
& \text{if and only if} \quad g^{-1}gs \in S
\end{aligned}
$$

Notice that

$$
\begin{aligned}
(x, y) \in E(\mathrm{Cay}(G, S)) \quad & \text{if and only if} \quad (x, y) = (g, gs) \text{ for} \\
& \qquad\qquad\qquad\quad \text{some } g \in G \text{ and } s \in S \\
& \text{if and only if} \quad g^{-1}gs \in S \\
& \text{if and only if} \quad x^{-1}y \in S.
\end{aligned}
$$

Notice that

$$
\begin{aligned}
(x, y) \in E(\mathrm{Cay}(G, S)) \quad &\text{if and only if} \quad (x, y) = (g, gs) \text{ for} \\
&\qquad\qquad\qquad\quad \text{some } g \in G \text{ and } s \in S \\
&\text{if and only if} \quad g^{-1}gs \in S \\
&\text{if and only if} \quad x^{-1}y \in S.
\end{aligned}
$$

So $(x, y) \in E(\mathrm{Cay}(G, S))$ if and only if $x^{-1}y \in S$.

Notice that

$$\begin{aligned}(x,y)\in E(\mathrm{Cay}(G,S)) \quad &\text{if and only if} \quad (x,y)=(g,gs) \text{ for}\\ &\qquad\qquad\qquad\quad \text{some } g\in G \text{ and } s\in S\\ &\text{if and only if} \quad g^{-1}gs\in S\\ &\text{if and only if} \quad x^{-1}y\in S.\end{aligned}$$

So $(x,y)\in E(\mathrm{Cay}(G,S))$ if and only if $x^{-1}y\in S$. This is sometimes used to define Cayley digraphs.

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G, S)$ is a graph,

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G, S)$ is a graph, then the condition that $S^{-1} = \{s^{-1} : s \in S\} = S$ must be satisfied as

$$(g, gs), (gs, g) \in E(\mathrm{Cay}(G, S))$$

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G, S)$ is a graph, then the condition that $S^{-1} = \{s^{-1} : s \in S\} = S$ must be satisfied as

$$(g, gs), (gs, g) \in E(\mathrm{Cay}(G, S)) \quad \text{if and only if} \quad g^{-1}gs, (gs)^{-1}g \in S$$

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G, S)$ is a graph, then the condition that $S^{-1} = \{s^{-1} : s \in S\} = S$ must be satisfied as

$$\begin{aligned}(g, gs), (gs, g) \in E(\mathrm{Cay}(G, S)) \quad &\text{if and only if} \quad g^{-1}gs, (gs)^{-1}g \in S \\ &\text{if and only if} \quad s, s^{-1}g^{-1}g \in S\end{aligned}$$

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G, S)$ is a graph, then the condition that $S^{-1} = \{s^{-1} : s \in S\} = S$ must be satisfied as

$$\begin{aligned}(g, gs), (gs, g) \in E(\mathrm{Cay}(G, S)) \quad &\text{if and only if} \quad g^{-1}gs, (gs)^{-1}g \in S \\ &\text{if and only if} \quad s, s^{-1}g^{-1}g \in S \\ &\text{if and only if} \quad s, s^{-1} \in S.\end{aligned}$$

If one wishes to specify that the Cayley digraph $\mathrm{Cay}(G,S)$ is a graph, then the condition that $S^{-1} = \{s^{-1} : s \in S\} = S$ must be satisfied as

$$\begin{aligned}(g,gs),(gs,g) \in E(\mathrm{Cay}(G,S)) \quad & \text{if and only if} \quad g^{-1}gs, (gs)^{-1}g \in S \\ & \text{if and only if} \quad s, s^{-1}g^{-1}g \in S \\ & \text{if and only if} \quad s, s^{-1} \in S.\end{aligned}$$

Also, in order for $\mathrm{Cay}(G,S)$ to be loopless, it must be that $1 \notin S$.

Definition 2

A Cayley digraph of the cyclic group $\mathbb{Z}_n$ *is a* **circulant digraph of order** n.

Definition 2

A Cayley digraph of the cyclic group $\mathbb{Z}_n$ is a **circulant digraph of order** *n.*

Ádám made the following conjecture in 1967 [1]:

Definition 2

A Cayley digraph of the cyclic group $\mathbb{Z}_n$ *is a* **circulant digraph of order** n.

Ádám made the following conjecture in 1967 [1]:

Conjecture 3

Two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, T)$ *are isomorphic if and only if* $mS = \{ms : s \in S\} = T$ *for some* $m \in \mathbb{Z}_n^*$.

Definition 2

A Cayley digraph of the cyclic group $\mathbb{Z}_n$ is a **circulant digraph of order** *n.*

Ádám made the following conjecture in 1967 [1]:

Conjecture 3

Two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if $mS = \{ms : s \in S\} = T$ for some $m \in \mathbb{Z}_n^*$.

The integer m is called a **multiplier**, and Ádám's conjecture is often stated as "two circulant graphs are isomorphic by a multiplier".

Why might someone make this conjecture?

Why might someone make this conjecture?

The first problem in Oystein Ore's book "Theory of Graphs" [31] published in 1962 (the first graph theory book written in English) is:

Why might someone make this conjecture?

The first problem in Oystein Ore's book "Theory of Graphs" [31] published in 1962 (the first graph theory book written in English) is: Show the following graphs are isomorphic.

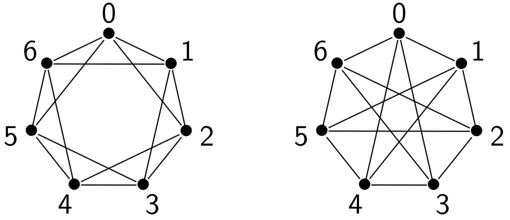


Figure: The Cayley graphs $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2, 5, 6\})$ and $\mathrm{Cay}(\mathbb{Z}_7, \{1, 3, 4, 6\})$

Why might someone make this conjecture?

The first problem in Oystein Ore's book "Theory of Graphs" [31] published in 1962 (the first graph theory book written in English) is: Show the following graphs are isomorphic.

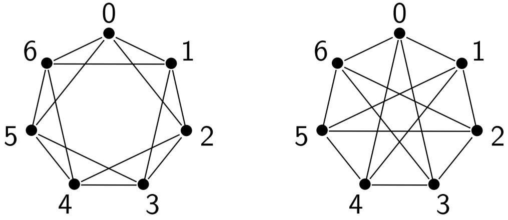


Figure: The Cayley graphs $\mathrm{Cay}(\mathbb{Z}_7, \{1, 2, 5, 6\})$ and $\mathrm{Cay}(\mathbb{Z}_7, \{1, 3, 4, 6\})$

Note that $3 \cdot \{1, 2, 5, 6\} = \{1, 3, 4, 6\}$.

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$.

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G, S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$.

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G,S))$.

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G, S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G, S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G, S))$. Then

$$\alpha(g, gs) =$$

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G,S))$. Then

$$\alpha(g, gs) = (\alpha(g), \alpha(gs)) =$$

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G,S))$. Then

$$\alpha(g, gs) = (\alpha(g), \alpha(gs)) = (\alpha(g), \alpha(g)\alpha(s)) =$$

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G, S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G, S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G, S))$. Then

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

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G,S))$. Then

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

where $g' = \alpha(g)$ and $s' = \alpha(s) \in \alpha(S)$. $\square$

Lemma 4

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G,S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof.

Clearly $\alpha : G \mapsto G$ is a bijection and $V(\alpha(\mathrm{Cay}(G,S))) = G$. Let $(g, gs) \in E(\mathrm{Cay}(G,S))$. Then

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

where $g' = \alpha(g)$ and $s' = \alpha(s) \in \alpha(S)$. □

This means that in checking whether or not two Cayley digraphs of G are isomorphic, one must always check the groups automorphisms of G.

As $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto mx : m \in \mathbb{Z}_n^*\}$, we see that $mS = \{ms : s \in S\}$ is the image of S under a group automorphism of $\mathbb{Z}_n$.

As $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto mx : m \in \mathbb{Z}_n^*\}$, we see that $mS = \{ms : s \in S\}$ is the image of S under a group automorphism of $\mathbb{Z}_n$. So Ádám's conjecture is equivalent to

As $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto mx : m \in \mathbb{Z}_n^*\}$, we see that $mS = \{ms : s \in S\}$ is the image of S under a group automorphism of $\mathbb{Z}_n$. So Ádám's conjecture is equivalent to

Conjecture 5

Two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if $\alpha(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, T)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.

As $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto mx : m \in \mathbb{Z}_n^*\}$, we see that $mS = \{ms : s \in S\}$ is the image of S under a group automorphism of $\mathbb{Z}_n$. So Ádám's conjecture is equivalent to

Conjecture 5

Two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if $\alpha(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, T)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.

Thus Ádám conjectured that the necessary isomorphisms that one must check, the group automorphisms, are sufficient to test for isomorphism. This form is also easy to generalize:

As $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto mx : m \in \mathbb{Z}_n^*\}$, we see that $mS = \{ms : s \in S\}$ is the image of S under a group automorphism of $\mathbb{Z}_n$. So Ádám's conjecture is equivalent to

Conjecture 5

Two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if $\alpha(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, T)$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$.

Thus Ádám conjectured that the necessary isomorphisms that one must check, the group automorphisms, are sufficient to test for isomorphism. This form is also easy to generalize:

Problem 6

Determine the groups G for which any two isomorphic Cayley (di)graphs of G are isomorphic by a group automorphism of G.

Definition 7

A group G for which any two isomorphic Cayley (di)graphs of G are isomorphic by a group automorphism of G is called a **CI-group with respect to (di)graphs**.

Definition 7

A group G for which any two isomorphic Cayley (di)graphs of G are isomorphic by a group automorphism of G is called a **CI-group with respect to (di)graphs**.

Definition 8

Let G be a group and $\mathrm{Cay}(G, S)$ a Cayley (di)graph of G.

Definition 7

A group G for which any two isomorphic Cayley (di)graphs of G are isomorphic by a group automorphism of G is called a **CI-group with respect to (di)graphs**.

Definition 8

Let G be a group and $\mathrm{Cay}(G, S)$ a Cayley (di)graph of G. We say $\mathrm{Cay}(G, S)$ is a **CI-(di)graph of** *G if and only if whenever $\mathrm{Cay}(G, T)$ is another Cayley (di)graph of G then $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, T)$ are isomorphic if and only they are isomorphic by a group automorphism of G.*

Definition 7

A group G for which any two isomorphic Cayley (di)graphs of G are isomorphic by a group automorphism of G is called a **CI-group with respect to (di)graphs**.

Definition 8

Let G be a group and $\mathrm{Cay}(G,S)$ a Cayley (di)graph of G. We say $\mathrm{Cay}(G,S)$ is a **CI-(di)graph of** *G if and only if whenever $\mathrm{Cay}(G,T)$ is another Cayley (di)graph of G then $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G,T)$ are isomorphic if and only they are isomorphic by a group automorphism of G.*

So G is a CI-group with respect to (di)graphs if every Cayley (di)graph of G is a CI-(di)graph.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$.*

Definition 9

A group $H \leq S_n$ *is* **transitive** *if whenever* $x, y \in \mathbb{Z}_n$ *(we assume here that* S_n *permutes the set* $\mathbb{Z}_n$*) then there exists* $h \in H$ *with* $h(x) = y$*. The* **stabilizer of** x **in** H*, denoted* $\mathrm{Stab}_H(x)$ *(many people denote this group* H_x*), is the set of all* $h \in H$ *with* $h(x) = x$*.*

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of x in** *H, denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$.*

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of** x **in** H*, denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of** x **in** H, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of x in H**, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of x in H**, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Let G be a group and $g \in G$.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of** x **in** H, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Let G be a group and $g \in G$. Define $g_L : G \mapsto G$ by $g_L(x) = gx$.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of x in H**, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Let G be a group and $g \in G$. Define $g_L : G \mapsto G$ by $g_L(x) = gx$. If $g_L(x) = g_L(y)$ then $gx = gy$ and $x = y$ so g_L is injective.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of x in H**, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Let G be a group and $g \in G$. Define $g_L : G \mapsto G$ by $g_L(x) = gx$. If $g_L(x) = g_L(y)$ then $gx = gy$ and $x = y$ so g_L is injective. Also, if $h \in G$ then $g_L(g^{-1}h) = gg^{-1}h = h$, so g_L is a bijection.

Definition 9

A group $H \leq S_n$ is **transitive** *if whenever $x, y \in \mathbb{Z}_n$ (we assume here that S_n permutes the set $\mathbb{Z}_n$) then there exists $h \in H$ with $h(x) = y$. The* **stabilizer of** x **in** H, *denoted $\mathrm{Stab}_H(x)$ (many people denote this group H_x), is the set of all $h \in H$ with $h(x) = x$. So $\mathrm{Stab}_H(x) = \{h \in H : h(x) = x\}$. We say H is* **regular** *if $\mathrm{Stab}_H(x) = 1$.*

Definition 10

For a digraph Γ, we denote it's automorphism group by $\mathrm{Aut}(\Gamma)$, where an automorphism of Γ is an isomorphism of the digraph with itself. A digraph is **vertex-transitive** *if $\mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$.*

Let G be a group and $g \in G$. Define $g_L : G \mapsto G$ by $g_L(x) = gx$. If $g_L(x) = g_L(y)$ then $gx = gy$ and $x = y$ so g_L is injective. Also, if $h \in G$ then $g_L(g^{-1}h) = gg^{-1}h = h$, so g_L is a bijection. If $(h, hs) \in E(\mathrm{Cay}(G, S))$ then $g_L(h, hs) = (gh, ghs) \in E(\mathrm{Cay}(G, S))$ and so $g_L \in \mathrm{Aut}(Cay(G, S))$.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** *G.*

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G,S)$ is vertex-transitive.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G, S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$ for every $S \subseteq G$. Additionally, as for $g,h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G,S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G, S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.

The following result of Sabidussi [35] characterizes Cayley digraphs.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G, S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.
The following result of Sabidussi [35] characterizes Cayley digraphs.

Theorem 12

A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup isomorphic to G.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G,S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.

The following result of Sabidussi [35] characterizes Cayley digraphs.

Theorem 12

A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup isomorphic to G.

To prove this, choose a vertex of Γ and label it with 1.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G, S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.

The following result of Sabidussi [35] characterizes Cayley digraphs.

Theorem 12

A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup isomorphic to G.

To prove this, choose a vertex of Γ and label it with 1. Then for every other vertex $v \in V(\Gamma)$, there exists a unique element $g_v \in G$ with $g_v(1) = v$.

Definition 11

For a group G, let $G_L = \{g_L : g \in G\}$. G_L is the **left regular representation of** G.

So $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$ for every $S \subseteq G$. Additionally, as for $g, h \in G$, $(hg^{-1})_L(g) = h$ we see that G_L is transitive and so $\mathrm{Cay}(G,S)$ is vertex-transitive. Finally, if $g_L(x) = gx = x$, then $g = 1$. Thus G_L is regular.

The following result of Sabidussi [35] characterizes Cayley digraphs.

Theorem 12

A digraph Γ is isomorphic to a Cayley digraph of a group G if and only if $\mathrm{Aut}(\Gamma)$ contains a regular subgroup isomorphic to G.

To prove this, choose a vertex of Γ and label it with 1. Then for every other vertex $v \in V(\Gamma)$, there exists a unique element $g_v \in G$ with $g_v(1) = v$. Label vertex v with g_v.

Definition 13

For a set V, define 2^V to be the set of all subsets of V.

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$.*

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$. An* **isomorphism** *between two Cayley objects (V, E) and (V', E') is a bijection $\delta : V \mapsto V'$ such that $\delta(E) = \{\delta(e) : e \in E\} = E'$.*

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$. An* **isomorphism** *between two Cayley objects (V, E) and (V', E') is a bijection $\delta : V \mapsto V'$ such that $\delta(E) = \{\delta(e) : e \in E\} = E'$. As* **automorphism** *of X is an isomorphism of X with itself.*

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$. An* **isomorphism** *between two Cayley objects (V, E) and (V', E') is a bijection $\delta : V \mapsto V'$ such that $\delta(E) = \{\delta(e) : e \in E\} = E'$. As* **automorphism** *of X is an isomorphism of X with itself.*

Graphs, digraphs, designs, codes, matroids, etc. are all combinatorial objects.

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$. An* **isomorphism** *between two Cayley objects (V, E) and (V', E') is a bijection $\delta : V \mapsto V'$ such that $\delta(E) = \{\delta(e) : e \in E\} = E'$. As* **automorphism** *of X is an isomorphism of X with itself.*

Graphs, digraphs, designs, codes, matroids, etc. are all combinatorial objects.

Sabidussi's Theorem shows us a way of defining when a combintorial object is a Cayley object of a group G:

Definition 13

For a set V, define 2^V to be the set of all subsets of V. A **combinatorial object** *X is an ordered pair (V, E), where V is a set and $E \subseteq 2^V \cup 2^{2^V} \cup \ldots$. An* **isomorphism** *between two Cayley objects (V, E) and (V', E') is a bijection $\delta : V \mapsto V'$ such that $\delta(E) = \{\delta(e) : e \in E\} = E'$. As* **automorphism** *of X is an isomorphism of X with itself.*

Graphs, digraphs, designs, codes, matroids, etc. are all combinatorial objects.
Sabidussi's Theorem shows us a way of defining when a combintorial object is a Cayley object of a group G:

Definition 14

A Cayley object X of G in some class $\mathcal{K}$ of combinatorial objects is a combinatorial object with $V(X) = G$ and $G_L \leq \mathrm{Aut}(X)$.

Definition 15

Let $\mathcal{K}$ be a class of combinatorial objects. A group G for which any two isomorphic Cayley objects of G in $\mathcal{K}$ are isomorphic by a group automorphism of G is called a **CI-group with respect to** $\mathcal{K}$.

Definition 15

Let $\mathcal{K}$ be a class of combinatorial objects. A group G for which any two isomorphic Cayley objects of G in $\mathcal{K}$ are isomorphic by a group automorphism of G is called a **CI-group with respect to** $\mathcal{K}$.

Definition 16

Let $\mathcal{K}$ be a class of combinatorial objects. Let G be a group and X a Cayley object of G in $\mathcal{K}$.

Definition 15

Let $\mathcal{K}$ be a class of combinatorial objects. A group G for which any two isomorphic Cayley objects of G in $\mathcal{K}$ are isomorphic by a group automorphism of G is called a **CI-group with respect to** $\mathcal{K}$.

Definition 16

Let $\mathcal{K}$ be a class of combinatorial objects. Let G be a group and X a Cayley object of G in $\mathcal{K}$. We say X is a **CI-object of** *G in $\mathcal{K}$ if and only if whenever Y is another Cayley of G in $\mathcal{K}$ then X and Y are isomorphic if and only they are isomorphic by a group automorphism of G.*

Definition 15

Let $\mathcal{K}$ be a class of combinatorial objects. A group G for which any two isomorphic Cayley objects of G in $\mathcal{K}$ are isomorphic by a group automorphism of G is called a **CI-group with respect to** $\mathcal{K}$.

Definition 16

Let $\mathcal{K}$ be a class of combinatorial objects. Let G be a group and X a Cayley object of G in $\mathcal{K}$. We say X is a **CI-object of** *G in $\mathcal{K}$ if and only if whenever Y is another Cayley of G in $\mathcal{K}$ then X and Y are isomorphic if and only they are isomorphic by a group automorphism of G.*

So G is a CI-group with respect to $\mathcal{K}$ if every Cayley object of G in $\mathcal{K}$ is a CI-object.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects. Find all CI-groups with respect to $\mathcal{K}$.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects. Find all CI-groups with respect to $\mathcal{K}$.

Problem 18

Let $\mathcal{K}$ be a class of combinatorial objects and G a group.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects. Find all CI-groups with respect to $\mathcal{K}$.

Problem 18

Let $\mathcal{K}$ be a class of combinatorial objects and G a group. Find a minimal list L of permutations in S_G such that any two Cayley objects of G in $\mathcal{K}$ are isomorphic if and only if they are isomorphic by a permutation in L.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects. Find all CI-groups with respect to $\mathcal{K}$.

Problem 18

Let $\mathcal{K}$ be a class of combinatorial objects and G a group. Find a minimal list L of permutations in S_G such that any two Cayley objects of G in $\mathcal{K}$ are isomorphic if and only if they are isomorphic by a permutation in L.

In reality the problem is even more general as we may also consider the problem for objects which have transitive automorphism groups but are not Cayley objects of any group G.

Problem 17

Let $\mathcal{K}$ be a class of combinatorial objects. Find all CI-groups with respect to $\mathcal{K}$.

Problem 18

Let $\mathcal{K}$ be a class of combinatorial objects and G a group. Find a minimal list L of permutations in S_G such that any two Cayley objects of G in $\mathcal{K}$ are isomorphic if and only if they are isomorphic by a permutation in L.

In reality the problem is even more general as we may also consider the problem for objects which have transitive automorphism groups but are not Cayley objects of any group G. Or just objects which have a large automorphism group that need not be transitive!

A general strategy to solve the isomorphism problem for digraphs with some symmetry

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive)

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$.

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$.

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism.

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism. As $G \leq \mathrm{Aut}(\Delta)$, we see that $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$:

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism. As $G \leq \mathrm{Aut}(\Delta)$, we see that $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$:

$$\Gamma \overset{\delta}{\mapsto} \Delta$$

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism. As $G \leq \mathrm{Aut}(\Delta)$, we see that $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$:

$$\Gamma \overset{\delta}{\mapsto} \Delta \overset{g}{\mapsto} \Delta$$

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism. As $G \leq \mathrm{Aut}(\Delta)$, we see that $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$:

$$\Gamma \overset{\delta}{\mapsto} \Delta \overset{g}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma.$$

A general strategy to solve the isomorphism problem for digraphs with some symmetry

Suppose that Γ and Δ are digraphs (not necessarily vertex-transitive) with $1 \neq G \leq \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\Delta)$. Notice that if Γ and Δ are Cayley digraphs of a group H then we may take $G = H_L$. Suppose that Γ and Δ are isomorphic, with $\delta : V(\Gamma) \mapsto V(\Delta)$ an isomorphism. As $G \leq \mathrm{Aut}(\Delta)$, we see that $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$:

$$\Gamma \overset{\delta}{\mapsto} \Delta \overset{g}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma.$$

Of course, if $\delta^{-1} g \delta \in \mathrm{Aut}(\Gamma)$ for every $g \in G$, then $\delta^{-1} G \delta \leq \mathrm{Aut}(\Gamma)$.

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

$$\Gamma \overset{\gamma}{\mapsto} \Gamma$$

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

$$\Gamma \overset{\gamma}{\mapsto} \Gamma \overset{\delta}{\mapsto} \Delta.$$

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

$$\Gamma \overset{\gamma}{\mapsto} \Gamma \overset{\delta}{\mapsto} \Delta.$$

So $\delta\gamma : \Gamma \mapsto \Delta$ is another isomorphism from Γ to Δ

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

$$\Gamma \overset{\gamma}{\mapsto} \Gamma \overset{\delta}{\mapsto} \Delta.$$

So $\delta\gamma : \Gamma \mapsto \Delta$ is another isomorphism from Γ to Δ and $\gamma^{-1}\delta^{-1}G\delta\gamma \leq \mathrm{Aut}(\Gamma)$ by previous arguments.

If one knows that $\gamma : \Gamma \mapsto \Delta$ is an isomorphism, then an obvious way of producing other isomorphisms is to first apply an automorphism of Γ and then map Γ to Δ with γ:

$$\Gamma \overset{\gamma}{\mapsto} \Gamma \overset{\delta}{\mapsto} \Delta.$$

So $\delta\gamma : \Gamma \mapsto \Delta$ is another isomorphism from Γ to Δ and $\gamma^{-1}\delta^{-1}G\delta\gamma \leq \mathrm{Aut}(\Gamma)$ by previous arguments. So the effect on $\delta^{-1}G\delta$ of replacing δ with $\gamma\delta$ is to conjugate $\delta^{-1}G\delta$ by γ.

Let's now consider the nicest possible case:

Let's now consider the nicest possible case: Suppose that there exists $\delta \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$.

Let's now consider the nicest possible case: Suppose that there exists $\delta \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. Then $\delta\gamma \in N_{S_n}(G)$.

Let's now consider the nicest possible case: Suppose that there exists $\delta \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. Then $\delta\gamma \in N_{S_n}(G)$. Calculating the normalizer of G in S_n solves the isomorphism problem!

Let's now consider the nicest possible case: Suppose that there exists $\delta \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. Then $\delta\gamma \in N_{S_n}(G)$. Calculating the normalizer of G in S_n solves the isomorphism problem! In the case we are most interested in we have:

Let's now consider the nicest possible case: Suppose that there exists $\delta \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. Then $\delta\gamma \in N_{S_n}(G)$. Calculating the normalizer of G in S_n solves the isomorphism problem! In the case we are most interested in we have:

Lemma 19

$N_{S_G}(G_L) = \mathrm{Aut}(G) \cdot G_L$.

Proof.

Let $\delta \in N_{S_G}(G_L)$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L\beta =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L\beta = (\lambda(\lambda^{-1})(g))_L =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L\beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) = g_L(\lambda\beta)(1) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) = g_L(\lambda\beta)(1) = (\lambda\beta)g_L(1) =$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L\beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) = g_L(\lambda\beta)(1) = (\lambda\beta)g_L(1) = (\lambda\beta)(g)$$

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L\beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) = g_L(\lambda\beta)(1) = (\lambda\beta)g_L(1) = (\lambda\beta)(g)$$

and $\lambda\beta = 1$.

Proof.

Let $\delta \in N_{S_G}(G_L)$. As G_L is transitive, there exists $h \in G$ such that $\delta h_L(1) = 1$. Let $\beta = \delta h_L$. Define $\lambda : G \to G$ by $\lambda(g) = k$ if and only if $\beta^{-1} g_L \beta = k_L$. Then λ is the automorphism of G induced by conjugation of G_L by δ, and $\lambda(1) = 1$. We wish to show $\beta = \lambda^{-1}$. Now, $\beta^{-1} g_L \beta = (\lambda(g))_L$ for all $g \in G$. Also, for $x, g \in G$,

$$\lambda^{-1} g_L \lambda(x) = \lambda^{-1}(g\lambda(x)) = \lambda^{-1}(g)\lambda^{-1}(\lambda(x)) = \lambda^{-1}(g)x,$$

and $\lambda^{-1} g_L \lambda = (\lambda^{-1}(g))_L$. Thus

$$\beta^{-1}\lambda^{-1} g_L \lambda\beta = \beta^{-1}(\lambda^{-1}(g))_L \beta = (\lambda(\lambda^{-1})(g))_L = g_L$$

so that $\lambda\beta$ centralizes G_L and fixes 1. Let $g \in G$. Then

$$g = g_L(1) = g_L(\lambda\beta)(1) = (\lambda\beta)g_L(1) = (\lambda\beta)(g)$$

and $\lambda\beta = 1$. So $\beta = \lambda^{-1} \in \mathrm{Aut}(G)$. $\square$

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$.

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$. As $g_L \in \mathrm{Aut}(\Gamma)$, we see that $\alpha : \Gamma \mapsto \Delta$ is an isomorphism.

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$. As $g_L \in \mathrm{Aut}(\Gamma)$, we see that $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Summarizing this we have the following result:

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$. As $g_L \in \mathrm{Aut}(\Gamma)$, we see that $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Summarizing this we have the following result:

Lemma 20

Let Γ and Δ be isomorphic Cayley digraphs of G with $\delta : \Gamma \mapsto \Delta$ an isomorphism.

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$. As $g_L \in \mathrm{Aut}(\Gamma)$, we see that $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Summarizing this we have the following result:

Lemma 20

Let Γ and Δ be isomorphic Cayley digraphs of G with $\delta : \Gamma \mapsto \Delta$ an isomorphism. If there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$, then Γ and Δ are isomorphic by a group automorphism of G.

Returning now to our isomorphism $\delta\gamma : \Gamma \mapsto \Delta$, under our hypothesis that $\delta\gamma$ normalizes G_L, we may conclude that $\delta\gamma = \alpha g_L$ for some $\alpha \in \mathrm{Aut}(G)$ and $g \in G$. As $g_L \in \mathrm{Aut}(\Gamma)$, we see that $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Summarizing this we have the following result:

Lemma 20

Let Γ and Δ be isomorphic Cayley digraphs of G with $\delta : \Gamma \mapsto \Delta$ an isomorphism. If there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$, then Γ and Δ are isomorphic by a group automorphism of G.

The converse is also true!

Lemma 21

Let Γ *and* Δ *be isomorphic Cayley digraphs with* $\delta : \Gamma \mapsto \Delta$ *an isomorphism.*

Lemma 21

Let Γ *and* Δ *be isomorphic Cayley digraphs with* $\delta : \Gamma \mapsto \Delta$ *an isomorphism.* Γ *and* Δ *are isomorphic by a group automorphism of* G *if and only if there exists* $\gamma \in \mathrm{Aut}(\Gamma)$ *such that* $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Lemma 21

Let Γ and Δ be isomorphic Cayley digraphs with $\delta : \Gamma \mapsto \Delta$ an isomorphism. Γ and Δ are isomorphic by a group automorphism of G if and only if there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism.

Lemma 21

Let Γ *and* Δ *be isomorphic Cayley digraphs with* $\delta : \Gamma \mapsto \Delta$ *an isomorphism.* Γ *and* Δ *are isomorphic by a group automorphism of* G *if and only if there exists* $\gamma \in \mathrm{Aut}(\Gamma)$ *such that* $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism

Lemma 21

Let Γ and Δ be isomorphic Cayley digraphs with $\delta : \Gamma \mapsto \Delta$ an isomorphism. Γ and Δ are isomorphic by a group automorphism of G if and only if there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism and as

$$\Gamma \overset{\alpha}{\mapsto} \Delta$$

Lemma 21

Let Γ and Δ be isomorphic Cayley digraphs with $\delta : \Gamma \mapsto \Delta$ an isomorphism. Γ and Δ are isomorphic by a group automorphism of G if and only if there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism and as

$$\Gamma \overset{\alpha}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma$$

Lemma 21

Let Γ and Δ be isomorphic Cayley digraphs with $\delta : \Gamma \mapsto \Delta$ an isomorphism. Γ and Δ are isomorphic by a group automorphism of G if and only if there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism and as

$$\Gamma \overset{\alpha}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma$$

we see that $\gamma = \alpha\delta^{-1}$ is an automorphism of Γ.

Lemma 21

Let Γ and Δ be isomorphic Cayley digraphs with $\delta : \Gamma \mapsto \Delta$ an isomorphism. Γ and Δ are isomorphic by a group automorphism of G if and only if there exists $\gamma \in \mathrm{Aut}(\Gamma)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism and as

$$\Gamma \overset{\alpha}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma$$

we see that $\gamma = \alpha\delta^{-1}$ is an automorphism of Γ. As α normalizes G_L by Lemma 19,

Lemma 21

Let Γ *and* Δ *be isomorphic Cayley digraphs with* $\delta : \Gamma \mapsto \Delta$ *an isomorphism.* Γ *and* Δ *are isomorphic by a group automorphism of* G *if and only if there exists* $\gamma \in \mathrm{Aut}(\Gamma)$ *such that* $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$*.*

Proof.

Suppose that Γ and Δ are also isomorphic by $\alpha \in \mathrm{Aut}(G)$, so $\alpha : \Gamma \mapsto \Delta$ is an isomorphism. Then $\delta^{-1} : \Delta \mapsto \Gamma$ is an isomorphism and as

$$\Gamma \overset{\alpha}{\mapsto} \Delta \xmapsto{\delta^{-1}} \Gamma$$

we see that $\gamma = \alpha\delta^{-1}$ is an automorphism of Γ. As α normalizes G_L by Lemma 19,

$$\gamma^{-1}\delta^{-1}G_L\delta\gamma = \alpha^{-1}\delta\delta^{-1}G_L\delta\delta^{-1}\alpha = G_L.$$

□

Lemma 22

Let G be a group and $S \subseteq G$.

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G,

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G,
2. *whenever* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, *there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G,
2. *whenever* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, *there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.

Lemma 23 (Babai, 1977 [3])

Let G be a group.

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G,
2. *whenever* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, *there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.

Lemma 23 (Babai, 1977 [3])

Let G be a group. The following are equivalent:

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G,
2. *whenever* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, *there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.

Lemma 23 (Babai, 1977 [3])

Let G be a group. The following are equivalent:

1. *G is a CI-group with respect to digraphs,*

Lemma 22

Let G be a group and $S \subseteq G$. The following are equivalent:

1. $\mathrm{Cay}(G, S)$ *is a CI-digraph of* G*,*
2. *whenever* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$*, there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$*.*

Lemma 23 (Babai, 1977 [3])

Let G be a group. The following are equivalent:

1. *G is a CI-group with respect to digraphs,*
2. *whenever* $S \subseteq G$ *and* $\delta \in S_G$ *such that* $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$*, there exists* $\gamma \in \mathrm{Aut}(\mathrm{Cay}(G, S))$ *such that* $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$*.*

Theorem 24 (Turner, 1967 [39])

Let p be prime.

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p,

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p.

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$.

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. Then $(\mathbb{Z}_p)_L$ and $\delta^{-1}(\mathbb{Z}_p)_L\delta$ are Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and are thus conjugate in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$.

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. Then $(\mathbb{Z}_p)_L$ and $\delta^{-1}(\mathbb{Z}_p)_L\delta$ are Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and are thus conjugate in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. The result follows by Lemma 23. □

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. Then $(\mathbb{Z}_p)_L$ and $\delta^{-1}(\mathbb{Z}_p)_L\delta$ are Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and are thus conjugate in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. The result follows by Lemma 23. □

What here is special about digraphs?

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. Then $(\mathbb{Z}_p)_L$ and $\delta^{-1}(\mathbb{Z}_p)_L\delta$ are Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and are thus conjugate in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. The result follows by Lemma 23. $\square$

What here is special about digraphs? Nothing!

Theorem 24 (Turner, 1967 [39])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs.

Proof.

As the highest power of p that divides $|S_p| = p!$ is p, $(\mathbb{Z}_p)_L \cong \mathbb{Z}_p$ is a Sylow p-subgroup of S_p. Now let $S \subseteq \mathbb{Z}_p$, and $\delta \in S_p$ such that $\delta^{-1}(\mathbb{Z}_p)_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. Then $(\mathbb{Z}_p)_L$ and $\delta^{-1}(\mathbb{Z}_p)_L\delta$ are Sylow p-subgroups of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and are thus conjugate in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$. The result follows by Lemma 23. $\square$

What here is special about digraphs? Nothing! With almost identical proofs we have the following results.

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$.

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*
2. *whenever $\delta \in S_G$ such that $\delta^{-1}G_L\delta \le \mathrm{Aut}(\mathrm{Cay}(G,S))$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.*

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*
2. *whenever $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.*

Lemma 26

Let G be a group and $\mathcal{K}$ a class of combinatorial objects.

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*
2. *whenever $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(G,S))$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1}G_L\delta\gamma = G_L$.*

Lemma 26

Let G be a group and $\mathcal{K}$ a class of combinatorial objects. The following are equivalent:

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*
2. *whenever $\delta \in S_G$ such that $\delta^{-1} G_L \delta \le \mathrm{Aut}(\mathrm{Cay}(G, S))$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.*

Lemma 26

Let G be a group and $\mathcal{K}$ a class of combinatorial objects. The following are equivalent:

1. *G is a CI-group with respect to $\mathcal{K}$,*

Lemma 25 (Babai, 1977 [3])

Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and X a Cayley object of G in $\mathcal{K}$. The following are equivalent:

1. *X is a CI-object of G,*
2. *whenever $\delta \in S_G$ such that $\delta^{-1} G_L \delta \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.*

Lemma 26

Let G be a group and $\mathcal{K}$ a class of combinatorial objects. The following are equivalent:

1. *G is a CI-group with respect to $\mathcal{K}$,*
2. *whenever X is a Cayley object of G in $\mathcal{K}$ and $\delta \in S_G$ such that $\delta^{-1} G_L \delta \leq \mathrm{Aut}(X)$, there exists $\gamma \in \mathrm{Aut}(X)$ such that $\gamma^{-1}\delta^{-1} G_L \delta\gamma = G_L$.*

Definition 27

A group G which is a CI-group with respect to every class of combinatorial objects is called a **CI-group**.

Definition 27

A group G which is a CI-group with respect to every class of combinatorial objects is called a **CI-group**.

Theorem 28 (Babai, 1977 [3])

Let p be prime. Then $\mathbb{Z}_p$ is a CI-group.

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point.

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point. The normalizer in this case is quite similar to the regular case:

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point. The normalizer in this case is quite similar to the regular case:

Lemma 29

Let $\bar{A} \leq \mathrm{Aut}(G)$ consist of all automorphisms of G that map H to H.

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point. The normalizer in this case is quite similar to the regular case:

Lemma 29

Let $\bar{A} \leq \mathrm{Aut}(G)$ consist of all automorphisms of G that map H to H. Then $N_{S_n}(G) = \bar{A} \cdot G$.

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point. The normalizer in this case is quite similar to the regular case:

Lemma 29

Let $\bar{A} \leq \mathrm{Aut}(G)$ consist of all automorphisms of G that map H to H. Then $N_{S_n}(G) = \bar{A} \cdot G$.

For intransitive G the normalizer can be computed,

Back to the general case now where G is transitive on n points but not necessarily regular with $H \leq G$ the stabilizer of a point. The normalizer in this case is quite similar to the regular case:

Lemma 29

Let $\bar{A} \leq \mathrm{Aut}(G)$ consist of all automorphisms of G that map H to H. Then $N_{S_n}(G) = \bar{A} \cdot G$.

For intransitive G the normalizer can be computed, but the statement is complicated.

Farther back now to the case where there does not exist $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$.

Farther back now to the case where there does not exist $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. That is, there is more than one conjugacy class of G in $\mathrm{Aut}(\Gamma)$.

Farther back now to the case where there does not exist $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. That is, there is more than one conjugacy class of G in $\mathrm{Aut}(\Gamma)$. Suppose that $C_1, \ldots, C_m$ are the conjugacy classes of G in $\mathrm{Aut}(\Gamma)$, with say $G \in C_1$.

Farther back now to the case where there does not exist $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. That is, there is more than one conjugacy class of G in $\mathrm{Aut}(\Gamma)$. Suppose that $C_1, \ldots, C_m$ are the conjugacy classes of G in $\mathrm{Aut}(\Gamma)$, with say $G \in C_1$. In this case one would need to find $s_1, \ldots, s_m$ such that $s_i^{-1}C_is_i = C_1$ (so one can take $s_1 = 1$).

Farther back now to the case where there does not exist $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}\delta^{-1}G\delta\gamma = G$. That is, there is more than one conjugacy class of G in $\mathrm{Aut}(\Gamma)$. Suppose that $C_1, \ldots, C_m$ are the conjugacy classes of G in $\mathrm{Aut}(\Gamma)$, with say $G \in C_1$. In this case one would need to find $s_1, \ldots, s_m$ such that $s_i^{-1} C_i s_i = C_1$ (so one can take $s_1 = 1$). Then Δ and Γ will be isomorphic by $s_i\omega$ where ω normalizes G.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B.*

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**. *Any other block is nontrivial.*

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**. *Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive**.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**. *Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive**. *If G is not imprimitive, we say that G is* **primitive**.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**. *Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive**. *If G is not imprimitive, we say that G is* **primitive**. *Note that if B is a block of G, then $g(B)$ is also a block of B for every $g \in G$, and is called a* **conjugate block of** *B.*

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block**. *Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive**. *If G is not imprimitive, we say that G is* **primitive**. *Note that if B is a block of G, then $g(B)$ is also a block of B for every $g \in G$, and is called a* **conjugate block of** *B. The set of all blocks conjugate to B, denoted $\mathcal{B}$, is a partition of X, and $\mathcal{B}$ is called a* **complete block system of** *G.*

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block***. Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive***. If G is not imprimitive, we say that G is* **primitive***. Note that if B is a block of G, then $g(B)$ is also a block of B for every $g \in G$, and is called a* **conjugate block of** *B. The set of all blocks conjugate to B, denoted $\mathcal{B}$, is a partition of X, and $\mathcal{B}$ is called a* **complete block system of** *G.*

There does not seem to be a standard term for what is called here a complete block system of G.

Imprimitive Permutation Groups

Definition 30

Let G be a transitive group acting on X. A subset $B \subseteq X$ is a **block** *of G if whenever $g \in G$, then $g(B) \cap B = \emptyset$ or B. If $B = \{x\}$ for some $x \in X$ or $B = X$, then B is a* **trivial block***. Any other block is nontrivial. If G has a nontrivial block then it is* **imprimitive***. If G is not imprimitive, we say that G is* **primitive***. Note that if B is a block of G, then $g(B)$ is also a block of B for every $g \in G$, and is called a* **conjugate block of** *B. The set of all blocks conjugate to B, denoted $\mathcal{B}$, is a partition of X, and $\mathcal{B}$ is called a* **complete block system of** *G.*

There does not seem to be a standard term for what is called here a complete block system of G. Other authors use a **system of imprimitivity** or a G-**invariant partition** for this term.

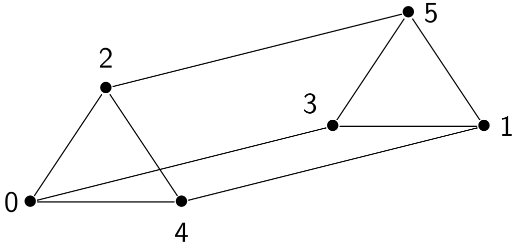


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

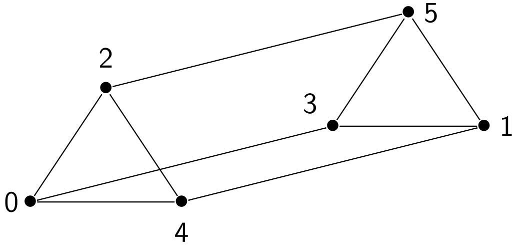


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

Note that the graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$ has exactly two triangles, and it is easy to see that an automorphism of a graph must map a triangle to a triangle.

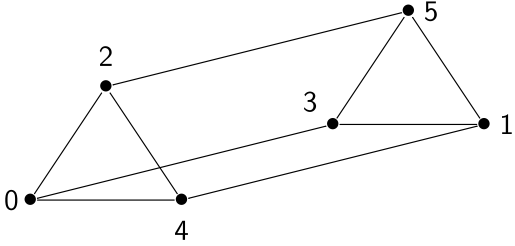


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

Note that the graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$ has exactly two triangles, and it is easy to see that an automorphism of a graph must map a triangle to a triangle. So $\mathrm{Aut}(\Gamma)$ has a complete block system with 2 blocks of size 3.

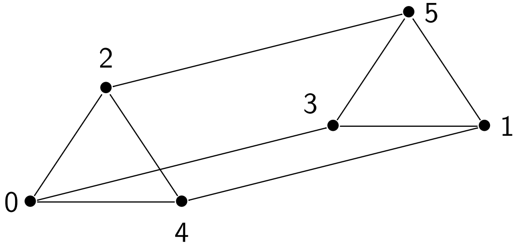


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

Note that the graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$ has exactly two triangles, and it is easy to see that an automorphism of a graph must map a triangle to a triangle. So $\mathrm{Aut}(\Gamma)$ has a complete block system with 2 blocks of size 3. Also, edges not in a triangle are mapped by a graph automorphism to edges not in a triangle,

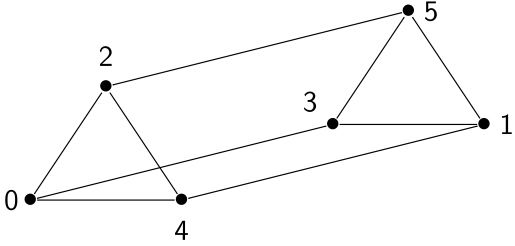


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

Note that the graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$ has exactly two triangles, and it is easy to see that an automorphism of a graph must map a triangle to a triangle. So $\mathrm{Aut}(\Gamma)$ has a complete block system with 2 blocks of size 3. Also, edges not in a triangle are mapped by a graph automorphism to edges not in a triangle, so $\mathrm{Aut}(\Gamma)$ also has a complete block system with 3 blocks of size 2.

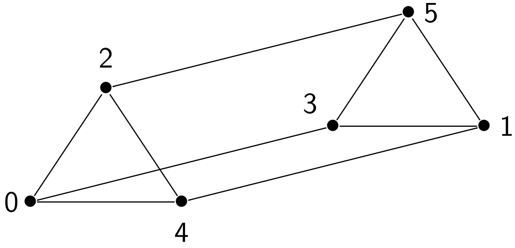


Figure: $\mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$

Note that the graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_6, \{2, 3, 4\})$ has exactly two triangles, and it is easy to see that an automorphism of a graph must map a triangle to a triangle. So $\mathrm{Aut}(\Gamma)$ has a complete block system with 2 blocks of size 3. Also, edges not in a triangle are mapped by a graph automorphism to edges not in a triangle, so $\mathrm{Aut}(\Gamma)$ also has a complete block system with 3 blocks of size 2. One can then see that $\mathrm{Aut}(\Gamma) = S_2 \times S_3$.

Definition 31

The **degree** *of a transitive group is the number of points that it permutes.*

Definition 31

The **degree** *of a transitive group is the number of points that it permutes.*

Theorem 32

Let $\mathcal{B}$ be a complete block system of G. Then every block in $\mathcal{B}$ has the same cardinality, say k. Further, if m is the number of blocks in $\mathcal{B}$ then mk is the degree of G.

The following result is often used to find complete block systems.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \lhd G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x,

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$,

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

Hence $g(B)$ is the orbit of N that contains $g(x)$,

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

Hence $g(B)$ is the orbit of N that contains $g(x)$, and as the orbits of N form a partition of X,

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

Hence $g(B)$ is the orbit of N that contains $g(x)$, and as the orbits of N form a partition of X, $g(B) \cap B = \emptyset$ or B.

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

Hence $g(B)$ is the orbit of N that contains $g(x)$, and as the orbits of N form a partition of X, $g(B) \cap B = \emptyset$ or B. Thus B is a block,

The following result is often used to find complete block systems.

Theorem 33

Let G be a transitive group acting on X. If $N \triangleleft G$, then the orbits of N form a complete block system of G.

Proof: Let $x \in X$ and B the orbit of N that contains x, so $B = \{h(x) : h \in N\}$. Let $g \in G$, and for $h \in N$, denote by h' the element of N such that $gh = h'g$. Note h' always exists as $N \triangleleft G$, and that $\{h' : h \in N\} = N$ as conjugation by g induces an automorphism of N. Then

$$g(B) = \{gh(x) : h \in N\} = \{h'g(x) : h \in N\} = \{h(g(x)) : h \in N\}.$$

Hence $g(B)$ is the orbit of N that contains $g(x)$, and as the orbits of N form a partition of X, $g(B) \cap B = \emptyset$ or B. Thus B is a block, and as every conjugate block $g(B)$ of B is an orbit of N, the orbits of N do indeed form a complete block system of G.

Corollary 34

A transitive group G of prime degree p is primitive.

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. □

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. □

Corollary 35

A nontrivial normal subgroup of a primitive group is transitive.

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. $\square$

Corollary 35

A nontrivial normal subgroup of a primitive group is transitive.

Proof.

Let $G \leq S_n$ be primitive with $N \triangleleft G$.

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. $\square$

Corollary 35

A nontrivial normal subgroup of a primitive group is transitive.

Proof.

Let $G \leq S_n$ be primitive with $N \triangleleft G$. Towards a contradiction, suppose that N is not transitive.

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. $\square$

Corollary 35

A nontrivial normal subgroup of a primitive group is transitive.

Proof.

Let $G \leq S_n$ be primitive with $N \triangleleft G$. Towards a contradiction, suppose that N is not transitive. As the orbits of N form a complete block system $\mathcal{B}$ of G by Theorem 33, and, as N is nontrivial, $\mathcal{B}$ is nontrivial.

Corollary 34

A transitive group G of prime degree p is primitive.

Proof.

The only divisors of p are 1 and p, and so the only possible blocks are singleton sets and the entire set on which G acts by Theorem 32. $\square$

Corollary 35

A nontrivial normal subgroup of a primitive group is transitive.

Proof.

Let $G \leq S_n$ be primitive with $N \triangleleft G$. Towards a contradiction, suppose that N is not transitive. As the orbits of N form a complete block system $\mathcal{B}$ of G by Theorem 33, and, as N is nontrivial, $\mathcal{B}$ is nontrivial. Thus G is imprimitive, contradicting Corollary 34. $\square$

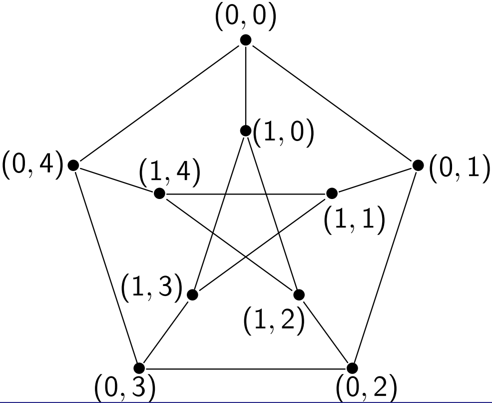
Example: Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i,j) = (i, j+1)$ and $\tau(i,j) = (i+1, 2j)$.

Example: Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i,j) = (i, j+1)$ and $\tau(i,j) = (i+1, 2j)$. Note that in these formulas, arithmetic is performed modulo 2 in the first coordinate

Example: Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i,j) = (i, j+1)$ and $\tau(i,j) = (i+1, 2j)$. Note that in these formulas, arithmetic is performed modulo 2 in the first coordinate and modulo 5 in the second coordinate.

Example: Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i,j) = (i, j+1)$ and $\tau(i,j) = (i+1, 2j)$. Note that in these formulas, arithmetic is performed modulo 2 in the first coordinate and modulo 5 in the second coordinate. It is straightforward but tedious to check that $\langle \rho, \tau \rangle$ is a subgroup of the automorphism group of the Petersen graph with the labeling shown below:

Example: Define $\rho, \tau : \mathbb{Z}_2 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_2 \times \mathbb{Z}_5$ by $\rho(i, j) = (i, j + 1)$ and $\tau(i, j) = (i + 1, 2j)$. Note that in these formulas, arithmetic is performed modulo 2 in the first coordinate and modulo 5 in the second coordinate. It is straightforward but tedious to check that $\langle \rho, \tau \rangle$ is a subgroup of the automorphism group of the Petersen graph with the labeling shown below:



Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j)$$

Additionally, $\tau^{-1}(i,j) = (i-1,3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1,2j) = (i+1-1,3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1,2j) = \tau^{-1}(i+1,2j+1)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1))$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho, \tau\rangle$.

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho,\tau\rangle$. Then by Theorem 33 the orbits of $\langle\rho\rangle$,

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho, \tau\rangle$. Then by Theorem 33 the orbits of $\langle\rho\rangle$, which are the sets $\{\{i,j\} : j \in \mathbb{Z}_5\} : i \in \mathbb{Z}_2\}$,

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho,\tau\rangle$. Then by Theorem 33 the orbits of $\langle\rho\rangle$, which are the sets $\{\{i,j\} : j \in \mathbb{Z}_5\} : i \in \mathbb{Z}_2\}$, form a complete block system of $\langle\rho,\tau\rangle$.

Additionally, $\tau^{-1}(i,j) = (i-1, 3j)$ as

$$\tau^{-1}\tau(i,j) = \tau^{-1}(i+1, 2j) = (i+1-1, 3(2j)) = (i,j).$$

Also,

$$\tau^{-1}\rho\tau(i,j) = \tau^{-1}\rho(i+1, 2j) = \tau^{-1}(i+1, 2j+1)$$

$$= (i+1-1, 3(2j+1)) = (i, j+3) = \rho^3(i,j)$$

and so $\langle\rho\rangle \triangleleft \langle\rho,\tau\rangle$. Then by Theorem 33 the orbits of $\langle\rho\rangle$, which are the sets $\{\{i,j\} : j \in \mathbb{Z}_5\} : i \in \mathbb{Z}_2\}$, form a complete block system of $\langle\rho,\tau\rangle$. Although we will not show this here, the full automorphism group of the Petersen graph is primitive.

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G.

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a normal complete block system of G, A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a normal complete block system of G, - the automorphism group of the line graph of the Petersen graph (of order 15) is imprimitive but has no nontrivial normal complete block systems

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a normal complete block system of G, - the automorphism group of the line graph of the Petersen graph (of order 15) is imprimitive but has no nontrivial normal complete block systems but we will not show that here.

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of G**. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a normal complete block system of G, - the automorphism group of the line graph of the Petersen graph (of order 15) is imprimitive but has no nontrivial normal complete block systems but we will not show that here.

Our next goal is to show that every complete block system of a transitive group which contains a regular abelian subgroup is necessarily a normal complete block system.

A complete block system of G formed by the orbits of normal subgroup of G is called a **normal complete block system of** G. Note that not every complete block system $\mathcal{B}$ of every transitive group G is a normal complete block system of G, - the automorphism group of the line graph of the Petersen graph (of order 15) is imprimitive but has no nontrivial normal complete block systems but we will not show that here.

Our next goal is to show that every complete block system of a transitive group which contains a regular abelian subgroup is necessarily a normal complete block system. We will need several preliminary results.

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$.

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$.

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$.
Now,

$$\mathrm{Stab}_G(h(x)) \quad =$$

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$.
Now,

$$\begin{aligned}\mathrm{Stab}_G(h(x)) &= \{g \in G : g(h(x)) = h(x)\} \\ &= \end{aligned}$$

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$. Now,

$$\begin{aligned} \mathrm{Stab}_G(h(x)) &= \{g \in G : g(h(x)) = h(x)\} \\ &= \{g \in G : h^{-1}gh(x) = x\} \\ &= \end{aligned}$$

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$.
Now,

$$\begin{array}{rcl}
\mathrm{Stab}_G(h(x)) & = & \{g \in G : g(h(x)) = h(x)\} \\
 & = & \{g \in G : h^{-1}gh(x) = x\} \\
 & = & \{g \in G : h^{-1}gh \in \mathrm{Stab}_G(x)\} \\
 & = &
\end{array}$$

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$. Now,

$$\begin{aligned}
\mathrm{Stab}_G(h(x)) &= \{g \in G : g(h(x)) = h(x)\} \\
&= \{g \in G : h^{-1}gh(x) = x\} \\
&= \{g \in G : h^{-1}gh \in \mathrm{Stab}_G(x)\} \\
&= \{g \in G : g \in h\mathrm{Stab}_G(x)h^{-1}\} \\
&=
\end{aligned}$$

Lemma 36

Let $G \leq S_n$ be transitive, and $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x)$ is conjugate to $\mathrm{Stab}_G(y)$ in G.

Proof.

We show that for $x \in \mathbb{Z}_n$ and $h \in G$, $\mathrm{Stab}_G(h(x)) = h\,\mathrm{Stab}_G(x)\,h^{-1}$.
Now,

$$\begin{aligned}
\mathrm{Stab}_G(h(x)) &= \{g \in G : g(h(x)) = h(x)\} \\
&= \{g \in G : h^{-1}gh(x) = x\} \\
&= \{g \in G : h^{-1}gh \in \mathrm{Stab}_G(x)\} \\
&= \{g \in G : g \in h\mathrm{Stab}_G(x)h^{-1}\} \\
&= h\,\mathrm{Stab}_G(x)\,h^{-1}.
\end{aligned}$$

$\square$

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$.

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian,

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$.

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$. As G is transitive, $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$ for all $x, y \in \mathbb{Z}_n$.

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$. As G is transitive, $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$ for all $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x) = 1$ and G is regular. □

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$. As G is transitive, $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$ for all $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x) = 1$ and G is regular. $\square$

Lemma 38

A transitive group $G \leq S_n$ is regular if and only if the order of G is the degree of G.

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$. As G is transitive, $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$ for all $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x) = 1$ and G is regular. □

Lemma 38

A transitive group $G \leq S_n$ is regular if and only if the order of G is the degree of G.

Proof.

By the Orbit-Stabilizer Theorem (the size of an orbit G that contains x times the size of the stabilizer of x is the order of the group),

Corollary 37

A transitive abelian group $G \leq S_n$ is regular.

Proof.

Let $g \in G$ and $x \in \mathbb{Z}_n$. Then $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(g(x))$ by Corollary 36 and as G is abelian, $g\mathrm{Stab}_G(x)g^{-1} = \mathrm{Stab}_G(x)$. As G is transitive, $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(y)$ for all $x, y \in \mathbb{Z}_n$. Then $\mathrm{Stab}_G(x) = 1$ and G is regular. $\square$

Lemma 38

A transitive group $G \leq S_n$ is regular if and only if the order of G is the degree of G.

Proof.

By the Orbit-Stabilizer Theorem (the size of an orbit G that contains x times the size of the stabilizer of x is the order of the group), we see that $|G| = n \cdot |\mathrm{Stab}_G(x)| = n$. $\square$

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, denoted $\mathrm{fix}_G(\mathcal{B})$, Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, denoted $\mathrm{fix}_G(\mathcal{B})$, to be $\{g \in G : g/\mathcal{B} = 1\}$.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of $\mathcal{B}$ in G**, denoted $\mathrm{fix}_G(\mathcal{B})$, to be $\{g \in G : g/\mathcal{B} = 1\}$. That is, $\mathrm{fix}_G(\mathcal{B})$ is the subgroup of G which fixes each block of $\mathcal{B}$ set-wise.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, denoted $\mathrm{fix}_G(\mathcal{B})$, to be $\{g \in G : g/\mathcal{B} = 1\}$. That is, $\mathrm{fix}_G(\mathcal{B})$ is the subgroup of G which fixes each block of $\mathcal{B}$ set-wise. Furthermore, $\mathrm{fix}_G(\mathcal{B})$ is the kernel of the induced homomorphism $G \to S_{\mathcal{B}}$, and as such is normal in G.

Now suppose that $G \leq S_n$ is a transitive group which admits a complete block system $\mathcal{B}$ consisting m blocks of size k. Then G has an **induced action on** $\mathcal{B}$, which we denote by $G/\mathcal{B}$. Namely, for specific $g \in G$, we define $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$, and set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. We also define the **fixer of** $\mathcal{B}$ **in** G, denoted $\mathrm{fix}_G(\mathcal{B})$, to be $\{g \in G : g/\mathcal{B} = 1\}$. That is, $\mathrm{fix}_G(\mathcal{B})$ is the subgroup of G which fixes each block of $\mathcal{B}$ set-wise. Furthermore, $\mathrm{fix}_G(\mathcal{B})$ is the kernel of the induced homomorphism $G \to S_{\mathcal{B}}$, and as such is normal in G. Additionally, $|G| = |G/\mathcal{B}| \cdot |\mathrm{fix}_G(\mathcal{B})|$.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal,

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian,

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37. Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$ by Lemma 38,

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37. Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$ by Lemma 38, and so there exists nontrivial $K \leq \mathrm{fix}_H(\mathcal{B})$ of order $|B|$.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37. Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$ by Lemma 38, and so there exists nontrivial $K \leq \mathrm{fix}_H(\mathcal{B})$ of order $|B|$. Then the orbits of K form a complete block system $\mathcal{C}$ of H with blocks of size $|B|$ by Theorem 33,

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37. Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$ by Lemma 38, and so there exists nontrivial $K \leq \mathrm{fix}_H(\mathcal{B})$ of order $|B|$. Then the orbits of K form a complete block system $\mathcal{C}$ of H with blocks of size $|B|$ by Theorem 33, and each block of $\mathcal{C}$ is contained in a block of $\mathcal{B}$.

Theorem 39

Let $G \leq S_n$ be transitive with an abelian regular subgroup H. Then any complete block system of G is normal, and is formed by the orbits of a subgroup of H.

Proof: We only need show that $\mathrm{fix}_H(\mathcal{B})$ has orbits of size $|B|$, $B \in \mathcal{B}$. Now, $H/\mathcal{B}$ is transitive and abelian, and so $H/\mathcal{B}$ is regular by Corollary 37. Then $H/\mathcal{B}$ has degree $|\mathcal{B}|$ by Lemma 38, and so there exists nontrivial $K \leq \mathrm{fix}_H(\mathcal{B})$ of order $|B|$. Then the orbits of K form a complete block system $\mathcal{C}$ of H with blocks of size $|B|$ by Theorem 33, and each block of $\mathcal{C}$ is contained in a block of $\mathcal{B}$. We conclude that $\mathcal{C} = \mathcal{B}$.

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$.

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$.

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$. We will show the orbit B of $\bar{H}_L$ that contains g is $g + H$.

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$. We will show the orbit B of $\bar{H}_L$ that contains g is $g + H$. Indeed, $\bar{H}_L \leq \mathrm{fix}_{G_L}(\mathcal{B})$ and the orbit of $\bar{H}_L$ that contains g is

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$. We will show the orbit B of $\bar{H}_L$ that contains g is $g + H$. Indeed, $\bar{H}_L \leq \mathrm{fix}_{G_L}(\mathcal{B})$ and the orbit of $\bar{H}_L$ that contains g is

$$\{h_L(g) : h \in H\} = \{g + h : h \in H\} = g + H.$$

$\square$

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$. We will show the orbit B of $\bar{H}_L$ that contains g is $g + H$. Indeed, $\bar{H}_L \leq \mathrm{fix}_{G_L}(\mathcal{B})$ and the orbit of $\bar{H}_L$ that contains g is

$$\{h_L(g) : h \in H\} = \{g + h : h \in H\} = g + H.$$

□

Example: If $G = \mathbb{Z}_n$, then any complete block system $\mathcal{B}$ of $(\mathbb{Z}_n)_L$ with blocks of size k will be formed by the orbits of the unique subgroup of order k,

Lemma 40

Let G be an abelian group, and $\mathcal{B}$ a complete blocks system of G_L formed by the orbits of $\bar{H}_L = \{h_L : h \in H\}$ for some subgroup $H \leq G$. Then $\mathcal{B}$ consists of the cosets of H in G.

Proof.

Let $g \in G$. We will show the orbit B of $\bar{H}_L$ that contains g is $g + H$. Indeed, $\bar{H}_L \leq \mathrm{fix}_{G_L}(\mathcal{B})$ and the orbit of $\bar{H}_L$ that contains g is

$$\{h_L(g) : h \in H\} = \{g + h : h \in H\} = g + H.$$

□

Example: If $G = \mathbb{Z}_n$, then any complete block system $\mathcal{B}$ of $(\mathbb{Z}_n)_L$ with blocks of size k will be formed by the orbits of the unique subgroup of order k, and $\mathcal{B}$ will consist of the cosets $m + \langle n/k \rangle$, $m \in \mathbb{Z}_n$.

Lemma 41

Let G be a transitive group acting on X.

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$,

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$.

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$. Then

$$g(B_x) = \{g(y) : y \in X \text{ and } x \equiv y\}$$

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$. Then

$$\begin{aligned} g(B_x) &= \{g(y) : y \in X \text{ and } x \equiv y\} \\ &= \{g(y) : y \in X \text{ and } g(y) \equiv g(x)\} \end{aligned}$$

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$. Then

$$\begin{aligned} g(B_x) &= \{g(y) : y \in X \text{ and } x \equiv y\} \\ &= \{g(y) : y \in X \text{ and } g(y) \equiv g(x)\} \\ &= B_{g(x)}. \end{aligned}$$

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$. Then

$$\begin{aligned} g(B_x) &= \{g(y) : y \in X \text{ and } x \equiv y\} \\ &= \{g(y) : y \in X \text{ and } g(y) \equiv g(x)\} \\ &= B_{g(x)}. \end{aligned}$$

As $\mathcal{B}$ is a partition of X, it follows that $g(B_x) \cap B_x = B_{g(x)} \cap B_x = \emptyset$ or B_x, and B_x is a block of G.

Lemma 41

Let G be a transitive group acting on X. If $\equiv$ is an equivalence relation on X such that $x \equiv y$ if and only if $g(x) \equiv g(y)$ for all $g \in G$, then the equivalence classes of $\equiv$ form a complete block system of G.

Proof.

Let $x \in X$, $g \in G$, and B_x the equivalence class of $\equiv$ that contains x, and $\mathcal{B}$ the set of equivalence classes of $\equiv$. Then

$$\begin{aligned} g(B_x) &= \{g(y) : y \in X \text{ and } x \equiv y\} \\ &= \{g(y) : y \in X \text{ and } g(y) \equiv g(x)\} \\ &= B_{g(x)}. \end{aligned}$$

As $\mathcal{B}$ is a partition of X, it follows that $g(B_x) \cap B_x = B_{g(x)} \cap B_x = \emptyset$ or B_x, and B_x is a block of G. As $g(B_x) = B_{g(x)}$, the blocks conjugate to B_x are equivalence classes of $\equiv$. □

Definition 42

An equivalence relation $\equiv$ *as in the previous result is a* G-**congruence**.

The Embedding Theorem

The Embedding Theorem

Definition 43

Let Γ_1 and Γ_2 be digraphs.

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2,

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2*, denoted* $\Gamma_1 \wr \Gamma_2$,

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2, *denoted* $\Gamma_1 \wr \Gamma_2$, *is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2, *denoted* $\Gamma_1 \wr \Gamma_2$, *is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$ *and edge set*

$$\{(u,v)(u,v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u,v)(u',v') : uu' \in E(\Gamma_1) \text{ and } v,v' \in V(\Gamma_2)\}.$$

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2*, denoted* $\Gamma_1 \wr \Gamma_2$*, is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$ *and edge set*

$$\{(u,v)(u,v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup \{(u,v)(u',v') : uu' \in E(\Gamma_1) \text{ and } v,v' \in V(\Gamma_2)\}.$$

Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows.

The Embedding Theorem

Definition 43

Let Γ_1 and Γ_2 be digraphs. The **wreath product of Γ_1 and Γ_2**, *denoted $\Gamma_1 \wr \Gamma_2$, is the digraph with vertex set $V(\Gamma_1) \times V(\Gamma_2)$ and edge set*

$$\{(u, v)(u, v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u, v)(u', v') : uu' \in E(\Gamma_1) \text{ and } v, v' \in V(\Gamma_2)\}.$$

Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2,

The Embedding Theorem

Definition 43

Let Γ_1 and Γ_2 be digraphs. The **wreath product of Γ_1 and Γ_2**, *denoted $\Gamma_1 \wr \Gamma_2$, is the digraph with vertex set $V(\Gamma_1) \times V(\Gamma_2)$ and edge set*

$$\{(u, v)(u, v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u, v)(u', v') : uu' \in E(\Gamma_1) \text{ and } v, v' \in V(\Gamma_2)\}.$$

Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2, with these $|V(\Gamma_1)|$ copies indexed by elements of $V(\Gamma_1)$.

The Embedding Theorem

Definition 43

Let Γ_1 and Γ_2 be digraphs. The **wreath product of Γ_1 and Γ_2**, *denoted $\Gamma_1 \wr \Gamma_2$, is the digraph with vertex set $V(\Gamma_1) \times V(\Gamma_2)$ and edge set*

$$\{(u,v)(u,v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u,v)(u',v') : uu' \in E(\Gamma_1) \text{ and } v,v' \in V(\Gamma_2)\}.$$

Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2, with these $|V(\Gamma_1)|$ copies indexed by elements of $V(\Gamma_1)$. Next, between corresponding copies of Γ_2 we place every possible directed from one copy to another

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2, *denoted* $\Gamma_1 \wr \Gamma_2$, *is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$ *and edge set*

$$\{(u,v)(u,v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u,v)(u',v') : uu' \in E(\Gamma_1) \text{ and } v,v' \in V(\Gamma_2)\}.$$

Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2, with these $|V(\Gamma_1)|$ copies indexed by elements of $V(\Gamma_1)$. Next, between corresponding copies of Γ_2 we place every possible directed from one copy to another if in Γ_1 there is a directed edge between the indexing labels of the copies of Γ_2,

The Embedding Theorem

Definition 43

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2, *denoted* $\Gamma_1 \wr \Gamma_2$, *is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$ *and edge set*

$$\{(u, v)(u, v') : u \in V(\Gamma_1) \text{ and } vv' \in E(\Gamma_2)\}$$

$$\cup\{(u, v)(u', v') : uu' \in E(\Gamma_1) \text{ and } v, v' \in V(\Gamma_2)\}.$$

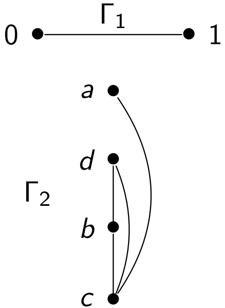
Intuitively, $\Gamma_1 \wr \Gamma_2$ is constructed as follows. First, we have $|V(\Gamma_1)|$ copies of the digraph Γ_2, with these $|V(\Gamma_1)|$ copies indexed by elements of $V(\Gamma_1)$. Next, between corresponding copies of Γ_2 we place every possible directed from one copy to another if in Γ_1 there is a directed edge between the indexing labels of the copies of Γ_2, and no edges otherwise.

To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.

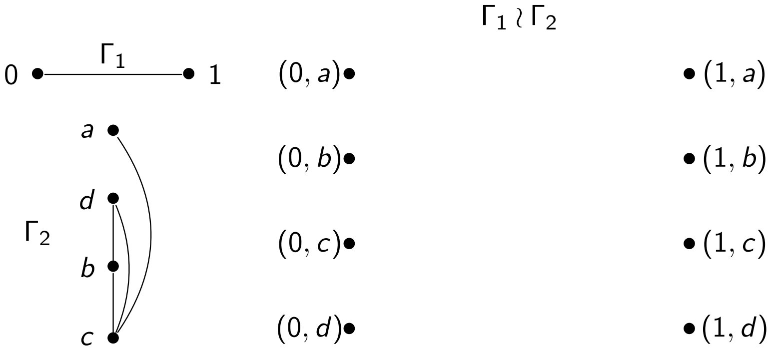
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2.



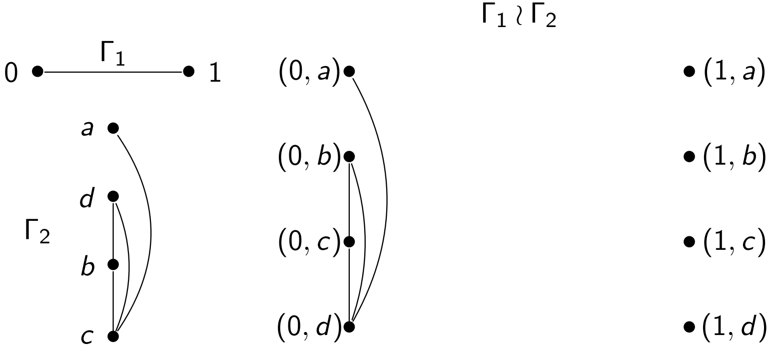
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2.



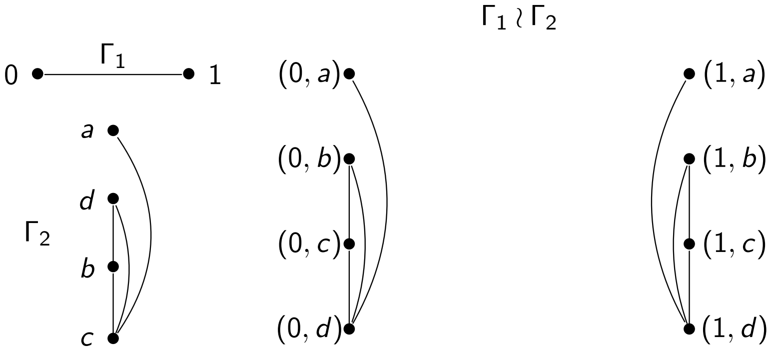
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2.



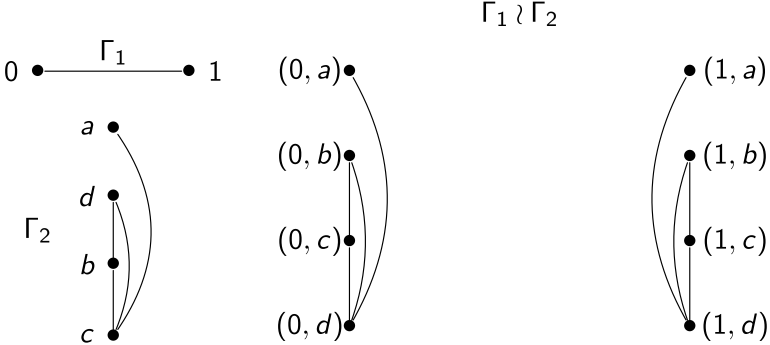
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2.



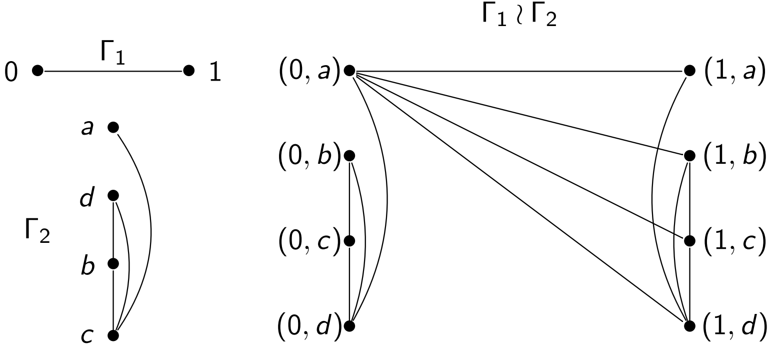
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.



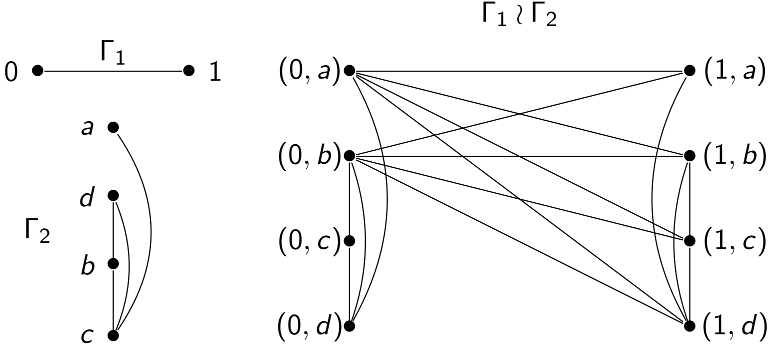
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.



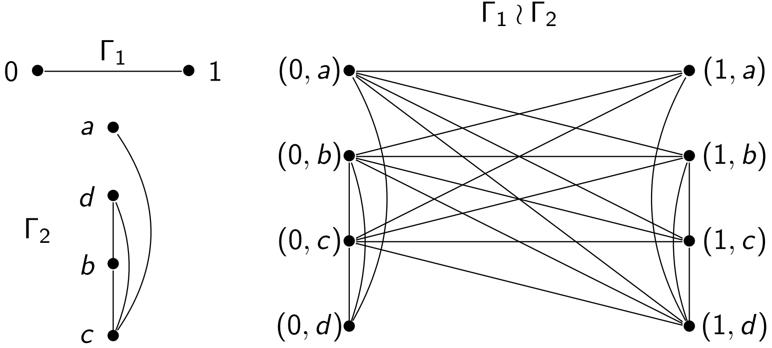
To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.



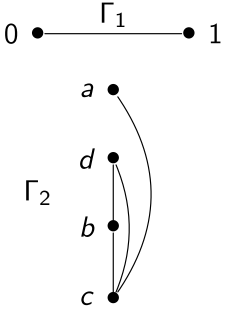
To find the wreath product of any two graphs Γ_1 and Γ_2:

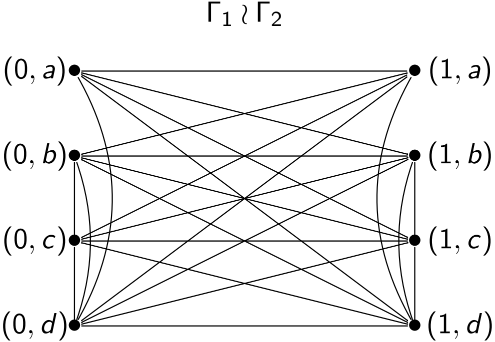
1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.



To find the wreath product of any two graphs Γ_1 and Γ_2:

1. First corresponding to each vertex of Γ_1, put a copy of Γ_2.
2. If v_1 and v_2 are adjacent in Γ_1, put every edge between corresponding copies of Γ_2.

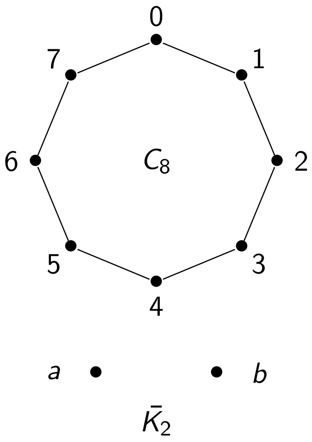


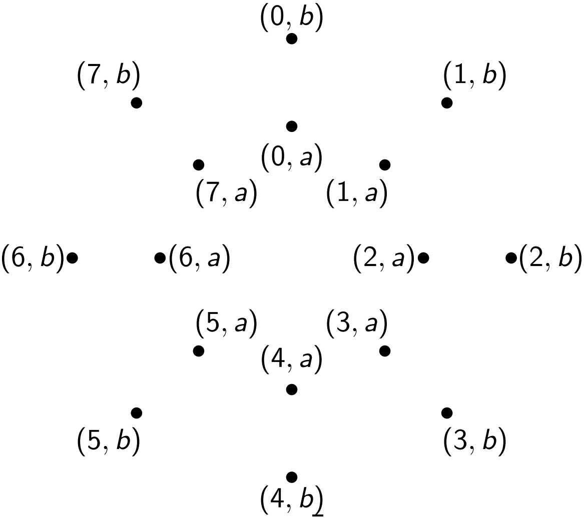


The wreath product of digraphs has many names, The wreath product of digraphs has many names, the lexicographic product, The wreath product of digraphs has many names, the lexicographic product, graph composition, The wreath product of digraphs has many names, the lexicographic product, graph composition, and the Γ_2-extension of Γ_1.

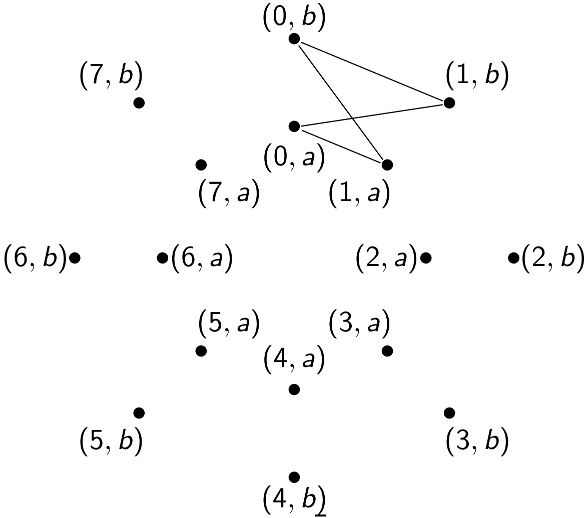
Let us consider the graph $C_8 \wr \bar{K}_2$.

Let us consider the graph $C_8 \wr \bar{K}_2$.

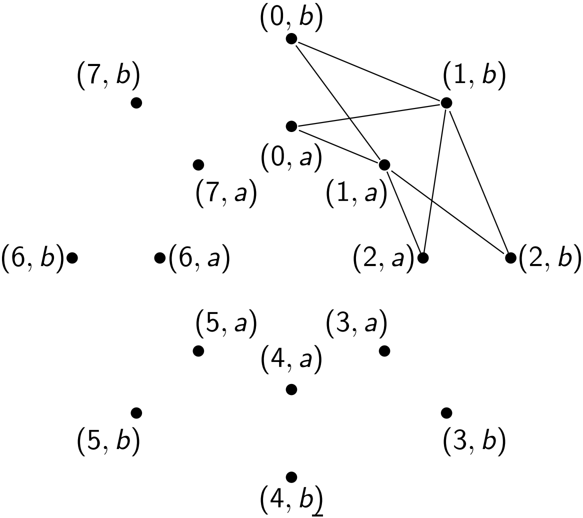




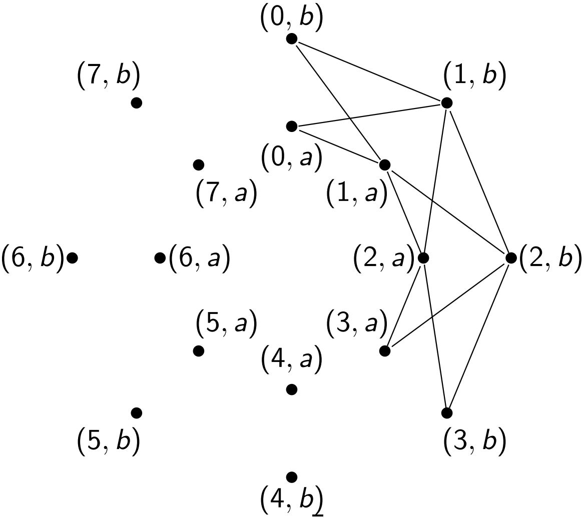
$C_8 \wr K_2$



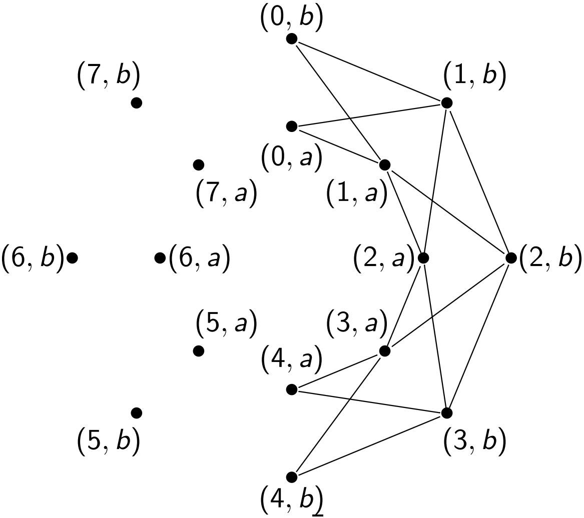
$C_8 \wr \bar{K}_2$



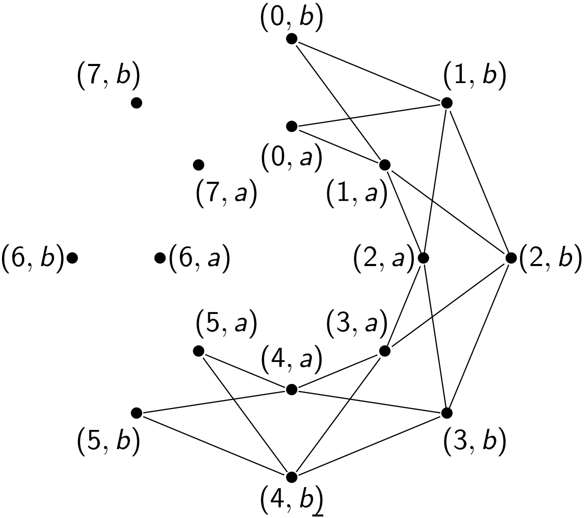
$C_8 \wr K_2$



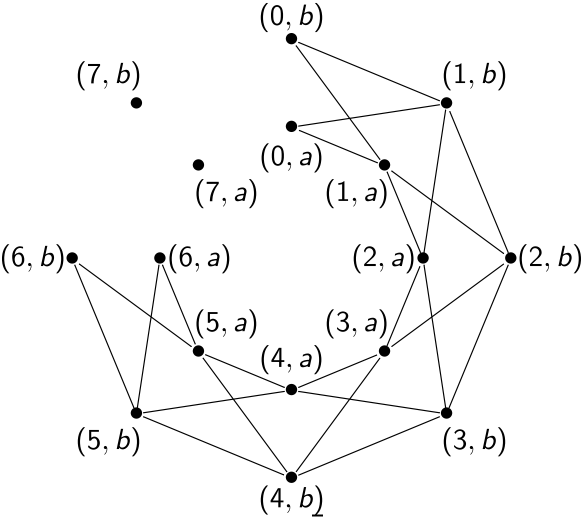
$C_8 \wr K_2$



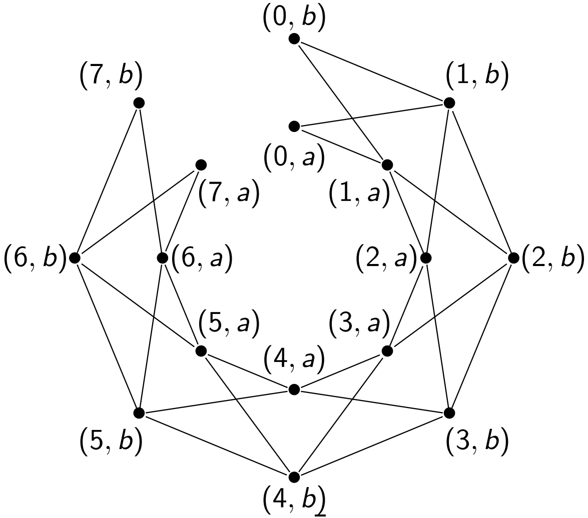
$C_8 \wr K_2$



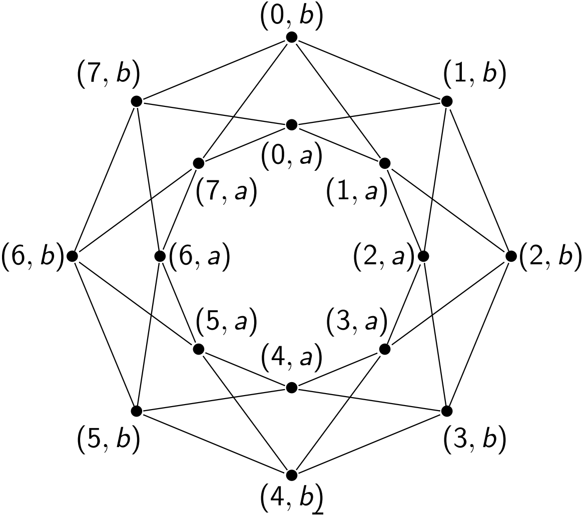
$C_8 \wr \bar{K}_2$



$C_8 \wr K_2$



$C_8 \wr \bar{K}_2$



$C_8 \wr \bar{K}_2$

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks.

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks.

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks.

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 44

Let G be a permutation group acting on X and H a permutation group acting on Y.

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 44

Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of G and H**,

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 44

Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of G and H**, *denoted $G \wr H$,*

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 44

Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of G and H**, *denoted $G \wr H$, to be the set of all permutations of $X \times Y$ of the form $(x,y) \to (g(x), h_x(y))$.*

In the previous graph, think of the sets $\{(i,j) : j \in \mathbb{Z}_2\}$ as blocks. Take any automorphism of C_8, and think of it as "permuting" the blocks. A block is mapped to a block by any automorphism of $\bar{K}_2$, and we can have different automorphisms of $\bar{K}_2$ for different blocks. This is the group $\mathrm{Aut}(C_8) \wr \mathrm{Aut}(\bar{K}_2)$.

Definition 44

Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of G and H**, *denoted $G \wr H$, to be the set of all permutations of $X \times Y$ of the form $(x,y) \to (g(x), h_x(y))$.*

It is easy to see that for digraphs Γ and Δ, $\mathrm{Aut}(\Gamma) \wr \mathrm{Aut}(\Delta) \leq \mathrm{Aut}(\Gamma \wr \Delta)$.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$ and so the highest power of p that divides $p^2!$ is p^{p+1}.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$ and so the highest power of p that divides $p^2!$ is p^{p+1}.
In general, $G \wr H$ has order $|G| \cdot |H|^{|X|}$.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i.
Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$ and so the highest power of p that divides $p^2!$ is p^{p+1}.
In general, $G \wr H$ has order $|G| \cdot |H|^{|X|}$. Also, $G \wr H$ contains a normal subgroup $H \times H \times \cdots \times H$ ($|X|$ times)

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$ and so the highest power of p that divides $p^2!$ is p^{p+1}.
In general, $G \wr H$ has order $|G| \cdot |H|^{|X|}$. Also, $G \wr H$ contains a normal subgroup $H \times H \times \cdots \times H$ ($|X|$ times) and so $G \wr H$ admits a complete block system with $|X|$ blocks of size $|Y|$ with blocks the fibers $\{(x,y) : y \in Y\}$.

Example: The group $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ and has order p^{p+1}. If p is prime, then $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ is isomorphic to a Sylow p-subgroup of S_{p^2}.

Note that $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p \times \mathbb{Z}_p$ as $(\mathbb{Z}_p)_L$ permutes $\mathbb{Z}_p$ and so is of degree p^2. It is apparent that
$(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$ by definition. Also, there are p choices for a and p choices for each b_i, and there are p b_i. Hence $(\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L$ has order $p \cdot p^p = p^{p+1}$. If p is prime, then the distinct multiples of p that divide $p^2!$ are $p, 2p, \ldots, (p-1)p, p^2$ and so the highest power of p that divides $p^2!$ is p^{p+1}.
In general, $G \wr H$ has order $|G| \cdot |H|^{|X|}$. Also, $G \wr H$ contains a normal subgroup $H \times H \times \cdots \times H$ ($|X|$ times) and so $G \wr H$ admits a complete block system with $|X|$ blocks of size $|Y|$ with blocks the fibers $\{(x,y) : y \in Y\}$. Finally, $G \times H \leq G \wr H$.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

The following immediate corollary is often useful.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

The following immediate corollary is often useful.

Corollary 46

Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ consisting of m blocks of size k.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

The following immediate corollary is often useful.

Corollary 46

Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ consisting of m blocks of size k. Then G is permutation isomorphic to a subgroup of $S_m \wr S_k$.

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

The following immediate corollary is often useful.

Corollary 46

Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ consisting of m blocks of size k. Then G is permutation isomorphic to a subgroup of $S_m \wr S_k$.

So, with an imprimitive permutation group, there is a natural labeling of the set on which the group acts!

Theorem 45 (The Embedding Theorem)

Let G be a transitive permutation group acting on X that admits a complete block system $\mathcal{B}$. Then G is permutation isomorphic to a subgroup of $(G/\mathcal{B}) \wr (\mathrm{Stab}_G(B_0)|_{B_0})$, where $B_0 \in \mathcal{B}$.

The following immediate corollary is often useful.

Corollary 46

Let G be a transitive permutation group that admits a complete block system $\mathcal{B}$ consisting of m blocks of size k. Then G is permutation isomorphic to a subgroup of $S_m \wr S_k$.

So, with an imprimitive permutation group, there is a natural labeling of the set on which the group acts! Do not be afraid to use this!

One must be slightly careful with this labeling, as it is not always the most natural labeling.

One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q.

One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q. Define $\rho, \tau : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau(i,j) = (i+1, \alpha j)$ and $\rho(i,j) = (i, j+1)$.

One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q. Define $\rho, \tau : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau(i,j) = (i+1, \alpha j)$ and $\rho(i,j) = (i, j+1)$. Then $\langle \rho, \tau \rangle$ is isomorphic to the nonabelian group of order qp.

One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q. Define $\rho, \tau : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau(i,j) = (i+1, \alpha j)$ and $\rho(i,j) = (i, j+1)$. Then $\langle \rho, \tau \rangle$ is isomorphic to the nonabelian group of order qp. The labeling that one would get for this group by applying the Embedding Theorem is $\langle \rho', \tau' \rangle$, One must be slightly careful with this labeling, as it is not always the most natural labeling. For example, let q and p be prime with $q|(p-1)$ and $\alpha \in \mathbb{Z}_p^*$ of order q. Define $\rho, \tau : \mathbb{Z}_q \times \mathbb{Z}_p \mapsto \mathbb{Z}_q \times \mathbb{Z}_p$ by $\tau(i,j) = (i+1, \alpha j)$ and $\rho(i,j) = (i, j+1)$. Then $\langle \rho, \tau \rangle$ is isomorphic to the nonabelian group of order qp. The labeling that one would get for this group by applying the Embedding Theorem is $\langle \rho', \tau' \rangle$, where $\rho'(i,j) = (i, j+\alpha^i)$, $\tau'(i,j) = (i+1, j)$.

Transitive groups of prime degree

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes.

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes. Additionally, any element of order p in S_p must be a p-cycle ρ, and then $\langle\rho\rangle$ is a Sylow p-subgroup of G that is isomorphic to $(\mathbb{Z}_p)_L$.

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes. Additionally, any element of order p in S_p must be a p-cycle ρ, and then $\langle\rho\rangle$ is a Sylow p-subgroup of G that is isomorphic to $(\mathbb{Z}_p)_L$. So we may assume without loss of generality that a transitive group of prime degree p contains $(\mathbb{Z}_p)_L$.

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes. Additionally, any element of order p in S_p must be a p-cycle ρ, and then $\langle\rho\rangle$ is a Sylow p-subgroup of G that is isomorphic to $(\mathbb{Z}_p)_L$. So we may assume without loss of generality that a transitive group of prime degree p contains $(\mathbb{Z}_p)_L$. We have already seen that

$$N_{S_p}((\mathbb{Z}_p)_L) \quad = \quad \mathrm{Aut}(\mathbb{Z}_p)\cdot(\mathbb{Z}_p)_L$$

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes. Additionally, any element of order p in S_p must be a p-cycle ρ, and then $\langle\rho\rangle$ is a Sylow p-subgroup of G that is isomorphic to $(\mathbb{Z}_p)_L$. So we may assume without loss of generality that a transitive group of prime degree p contains $(\mathbb{Z}_p)_L$. We have already seen that

$$\begin{aligned} N_{S_p}((\mathbb{Z}_p)_L) &= \mathrm{Aut}(\mathbb{Z}_p)\cdot(\mathbb{Z}_p)_L \\ &= \{x \mapsto mx + b : m \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\} \end{aligned}$$

Transitive groups of prime degree

First, as the size of an orbit of a group acting on a set divides the order of the group, a transitive group G of prime degree p must have order divisible by p as a transitive group has one orbit the size of the set it permutes. Additionally, any element of order p in S_p must be a p-cycle ρ, and then $\langle\rho\rangle$ is a Sylow p-subgroup of G that is isomorphic to $(\mathbb{Z}_p)_L$. So we may assume without loss of generality that a transitive group of prime degree p contains $(\mathbb{Z}_p)_L$. We have already seen that

$$\begin{aligned} N_{S_p}((\mathbb{Z}_p)_L) &= \mathrm{Aut}(\mathbb{Z}_p)\cdot(\mathbb{Z}_p)_L \\ &= \{x \mapsto mx + b : m \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\} \\ &= \mathrm{AGL}(1,p). \end{aligned}$$

Definition 47

A group $G \leq S_n$ *is* **doubly-transitive** *if for every two ordered pairs of points* (x_1, y_1) *and* (x_2, y_2)

Definition 47

A group $G \leq S_n$ *is* **doubly-transitive** *if for every two ordered pairs of points* (x_1, y_1) *and* (x_2, y_2) *with* $x_1 \neq y_1$ *and* $x_2 \neq y_2$

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive,

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement.

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Theorem 48 (Burnside 1901 [6])

Let p be prime and $G \leq S_p$ be transitive with $(\mathbb{Z}_p)_L \leq G$.

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Theorem 48 (Burnside 1901 [6])

Let p be prime and $G \leq S_p$ be transitive with $(\mathbb{Z}_p)_L \leq G$. Then either $G \leq \mathrm{AGL}(1, p)$ or G is doubly-transitive.

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Theorem 48 (Burnside 1901 [6])

Let p be prime and $G \leq S_p$ be transitive with $(\mathbb{Z}_p)_L \leq G$. Then either $G \leq \mathrm{AGL}(1, p)$ or G is doubly-transitive.

An equivalent formulation of this result is [8, Exercise 3.5.1]:

Definition 47

A group $G \leq S_n$ *is* **doubly-transitive** *if for every two ordered pairs of points* (x_1, y_1) *and* (x_2, y_2) *with* $x_1 \neq y_1$ *and* $x_2 \neq y_2$ *there exists* $g \in G$ *with* $g(x_1, y_1) = (x_2, y_2)$.

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Theorem 48 (Burnside 1901 [6])

Let p *be prime and* $G \leq S_p$ *be transitive with* $(\mathbb{Z}_p)_L \leq G$. *Then either* $G \leq \mathrm{AGL}(1, p)$ *or* G *is doubly-transitive.*

An equivalent formulation of this result is [8, Exercise 3.5.1]:

Theorem 49

Let p *be prime and* $G \leq S_p$ *be transitive.*

Definition 47

A group $G \leq S_n$ is **doubly-transitive** *if for every two ordered pairs of points (x_1, y_1) and (x_2, y_2) with $x_1 \neq y_1$ and $x_2 \neq y_2$ there exists $g \in G$ with $g(x_1, y_1) = (x_2, y_2)$.*

Note that if Γ is a digraph whose automorphism group is doubly-transitive, then Γ is either the complete graph or its complement. Consequently, $\mathrm{Aut}(\Gamma)$ is a symmetric group.

Theorem 48 (Burnside 1901 [6])

Let p be prime and $G \leq S_p$ be transitive with $(\mathbb{Z}_p)_L \leq G$. Then either $G \leq \mathrm{AGL}(1, p)$ or G is doubly-transitive.

An equivalent formulation of this result is [8, Exercise 3.5.1]:

Theorem 49

Let p be prime and $G \leq S_p$ be transitive. Then either G has a unique normal Sylow p-subgroup or G is doubly-transitive.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_p, T)$ *be isomorphic circulant digraphs of prime order* p *that are neither complete graphs or complements of complete graphs.*

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_p, T)$ *be isomorphic circulant digraphs of prime order* p *that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in* $\mathrm{AGL}(1, p)$.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_p, T)$ *be isomorphic circulant digraphs of prime order* p *that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in* $\mathrm{AGL}(1, p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ be isomorphic circulant digraphs of prime order p that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in $\mathrm{AGL}(1, p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive. By Burnside's Theorem 48 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T))$ are contained in $\mathrm{AGL}(1, p)$.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ be isomorphic circulant digraphs of prime order p that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in $\mathrm{AGL}(1, p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive. By Burnside's Theorem 48 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T))$ are contained in $\mathrm{AGL}(1, p)$. Let $\delta : \mathrm{Cay}(\mathbb{Z}_p, S) \mapsto \mathrm{Cay}(\mathbb{Z}_p, T)$ be an isomorphism.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_p, T)$ *be isomorphic circulant digraphs of prime order* p *that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in* $\mathrm{AGL}(1,p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive. By Burnside's Theorem 48 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T))$ are contained in $\mathrm{AGL}(1,p)$. Let $\delta : \mathrm{Cay}(\mathbb{Z}_p, S) \mapsto \mathrm{Cay}(\mathbb{Z}_p, T)$ be an isomorphism. Then a Sylow p-subgroup of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ is $(\mathbb{Z}_p)_L$ as well as $\delta^{-1}(\mathbb{Z}_p)_L\delta$.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ be isomorphic circulant digraphs of prime order p that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in $\mathrm{AGL}(1, p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive. By Burnside's Theorem 48 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T))$ are contained in $\mathrm{AGL}(1, p)$. Let $\delta : \mathrm{Cay}(\mathbb{Z}_p, S) \mapsto \mathrm{Cay}(\mathbb{Z}_p, T)$ be an isomorphism. Then a Sylow p-subgroup of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ is $(\mathbb{Z}_p)_L$ as well as $\delta^{-1}(\mathbb{Z}_p)_L\delta$. As $\mathrm{AGL}(1, p)$ has a unique normal Sylow p-subgroup $(\mathbb{Z}_p)_L$, $\delta^{-1}(\mathbb{Z}_p)_L\delta = (\mathbb{Z}_p)_L$ and δ normalizes $(\mathbb{Z}_p)_L$.

Corollary 50

Let $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ be isomorphic circulant digraphs of prime order p that are neither complete graphs or complements of complete graphs. Then the only isomorphisms between them are in $\mathrm{AGL}(1, p)$.

Proof.

As $\mathrm{Cay}(\mathbb{Z}_p, S)$ and $\mathrm{Cay}(\mathbb{Z}_p, T)$ are neither complete not complements of complete graphs, their automorphism groups are not doubly-transitive. By Burnside's Theorem 48 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ and $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T))$ are contained in $\mathrm{AGL}(1, p)$. Let $\delta : \mathrm{Cay}(\mathbb{Z}_p, S) \mapsto \mathrm{Cay}(\mathbb{Z}_p, T)$ be an isomorphism. Then a Sylow p-subgroup of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S))$ is $(\mathbb{Z}_p)_L$ as well as $\delta^{-1}(\mathbb{Z}_p)_L\delta$. As $\mathrm{AGL}(1, p)$ has a unique normal Sylow p-subgroup $(\mathbb{Z}_p)_L$, $\delta^{-1}(\mathbb{Z}_p)_L\delta = (\mathbb{Z}_p)_L$ and δ normalizes $(\mathbb{Z}_p)_L$. Thus $\delta \in \mathrm{AGL}(1, p)$. □

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B).

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and
$\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and $\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Lemma 51 (Dobson 1995 [9])

Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and
$\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Lemma 51 (Dobson 1995 [9])

Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Let $\equiv$ and $\mathcal{E}$ be defined as in the preceding paragraph.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and
$\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Lemma 51 (Dobson 1995 [9])

Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Let $\equiv$ and $\mathcal{E}$ be defined as in the preceding paragraph. Then $\mathcal{E}$ is a complete block system of G

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B\in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and
$\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Lemma 51 (Dobson 1995 [9])

Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Let $\equiv$ and $\mathcal{E}$ be defined as in the preceding paragraph. Then $\mathcal{E}$ is a complete block system of G and for every $g \in \mathrm{fix}_G(\mathcal{B})$, $g|_E \in \mathrm{Aut}(\Gamma)$ for every $E \in \mathcal{E}$.

Let G be a transitive group that admits a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Then $\mathrm{fix}_G(\mathcal{B})|_B$ is a transitive group of prime degree p, and so contains a p-cycle. Define a relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\gamma \in \mathrm{fix}_G(\mathcal{B})$ then $\gamma|_B$ is a p-cycle if and only if $\gamma|_{B'}$ is also a p-cycle (here $\gamma|_B$ is the induced permutation of g on B). It is straightforward to verify that $\equiv$ is an equivalence relation. Let C be an equivalence class of $\equiv$ and $E_C = \cup_{B \in C} B$ (remember that the equivalence classes of $\equiv$ consist of *blocks* of $\mathcal{B}$), and $\mathcal{E} = \{E_C : C \text{ is an equivalence class of } \equiv\}$.

Lemma 51 (Dobson 1995 [9])

Let Γ be a digraph with $G \leq \mathrm{Aut}(\Gamma)$ admit a normal complete block system $\mathcal{B}$ consisting of m blocks of prime size p. Let $\equiv$ and $\mathcal{E}$ be defined as in the preceding paragraph. Then $\mathcal{E}$ is a complete block system of G and for every $g \in \mathrm{fix}_G(\mathcal{B})$, $g|_E \in \mathrm{Aut}(\Gamma)$ for every $E \in \mathcal{E}$. Here $g|_E(x) = g(x)$ if $x \in E$ while $g(x) = x$ if $x \notin E$.

Proof:

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence.

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G.

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$.

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

$B \equiv B'$

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

$$B \equiv B' \quad \text{iff} \quad \gamma|_B \text{ is a } p-\text{cycle iff } \gamma|'_B \text{ is a } p-\text{cycle}$$

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

$$\begin{aligned} B \equiv B' \quad & \text{iff} \quad \gamma|_B \text{ is a } p-\text{cycle iff } \gamma|_B' \text{ is a } p-\text{cycle} \\ & \text{iff} \quad g\gamma g^{-1}|_{g(B)} \text{ is a } p-\text{cycle iff } g\gamma g^{-1}|_{g(B')} \text{ is a } p-\text{cycle} \end{aligned}$$

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

$$\begin{aligned} B \equiv B' \quad & \text{iff} \quad \gamma|_B \text{ is a } p-\text{cycle iff } \gamma|'_B \text{ is a } p-\text{cycle} \\ & \text{iff} \quad g\gamma g^{-1}|_{g(B)} \text{ is a } p-\text{cycle iff } g\gamma g^{-1}|_{g(B')} \text{ is a } p-\text{cycle} \\ & \text{iff} \quad g(B) \equiv g(B'). \end{aligned}$$

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

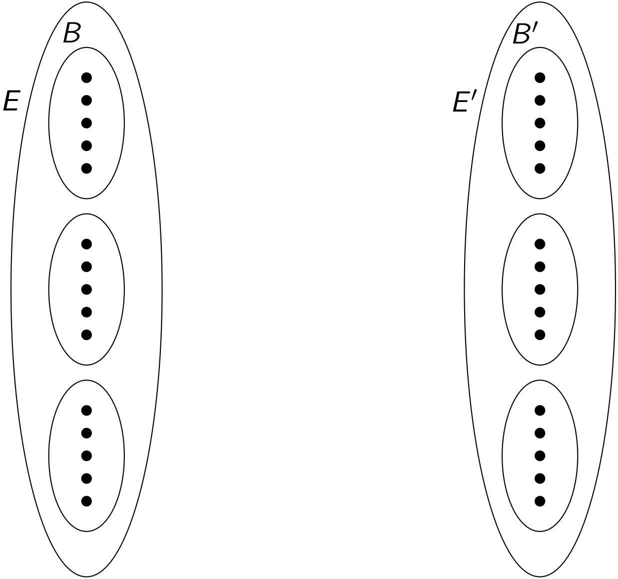
$$\begin{aligned} B \equiv B' & \quad \text{iff} \quad \gamma|_B \text{ is a } p-\text{cycle iff } \gamma|'_B \text{ is a } p-\text{cycle} \\ & \quad \text{iff} \quad g\gamma g^{-1}|_{g(B)} \text{ is a } p-\text{cycle iff } g\gamma g^{-1}|_{g(B')} \text{ is a } p-\text{cycle} \\ & \quad \text{iff} \quad g(B) \equiv g(B'). \end{aligned}$$

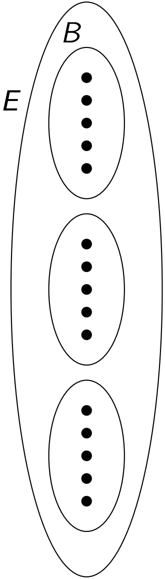
So $\equiv$ is a G-congruence.

Proof: To show that $\mathcal{E}$ is a complete block system of G, we show that $\equiv$ is a G-congruence. This will show that an equivalence class of $\equiv$ is a block of $G/\mathcal{B}$ by Lemma 41, which will show that the union of an equivalence class is a block of G. To show $\equiv$ is a G congruence, first recall that if $\gamma = (a_0, \ldots, a_{p-1})$ is a p-cycle, then $g\gamma g^{-1} = (g(a_0), \ldots, g(a_{p-1}))$. So if $B = \{a_0, \ldots, a_{p-1}\}$ then $g\gamma g^{-1}$ permutes $g(B)$. Now

$$\begin{aligned} B \equiv B' \quad & \text{iff} \quad \gamma|_B \text{ is a } p-\text{cycle iff } \gamma|'_B \text{ is a } p-\text{cycle} \\ & \text{iff} \quad g\gamma g^{-1}|_{g(B)} \text{ is a } p-\text{cycle iff } g\gamma g^{-1}|_{g(B')} \text{ is a } p-\text{cycle} \\ & \text{iff} \quad g(B) \equiv g(B'). \end{aligned}$$

So $\equiv$ is a G-congruence. For the rest,


B
E
B'
E'



choose

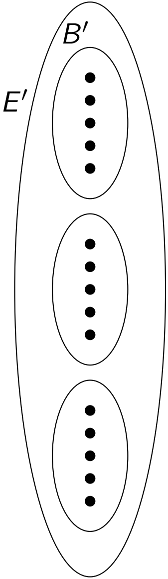
$\gamma \in \mathrm{fix}_G(\mathcal{B})$

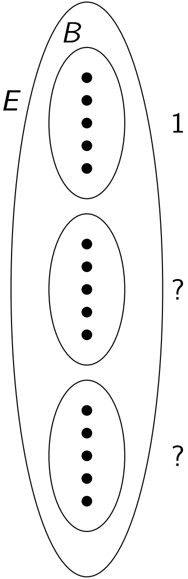
with

$\gamma|_{B'}$ a p-cycle

and

$\gamma|_B = 1$





choose

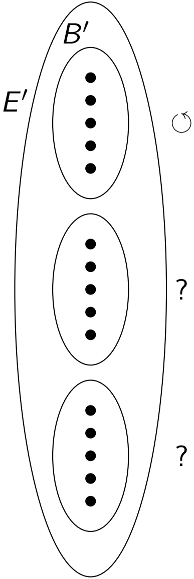
$\gamma \in \mathrm{fix}_G(\mathcal{B})$

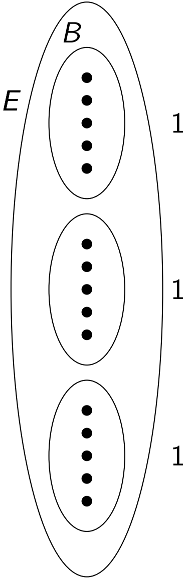
with

$\gamma|_{B'}$ a p-cycle

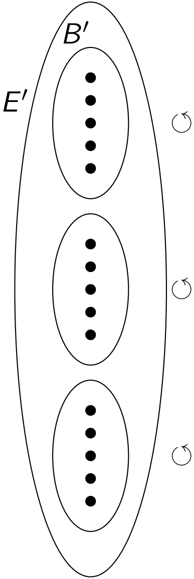
and

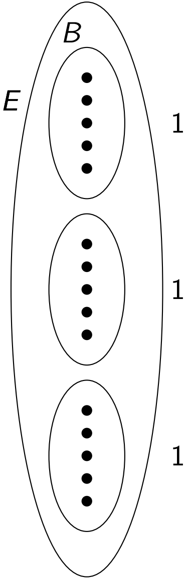
$\gamma|_B = 1$



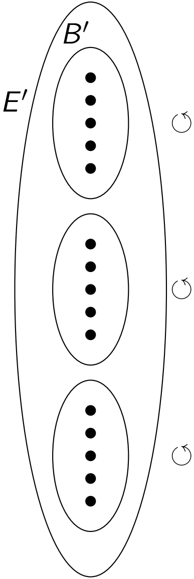


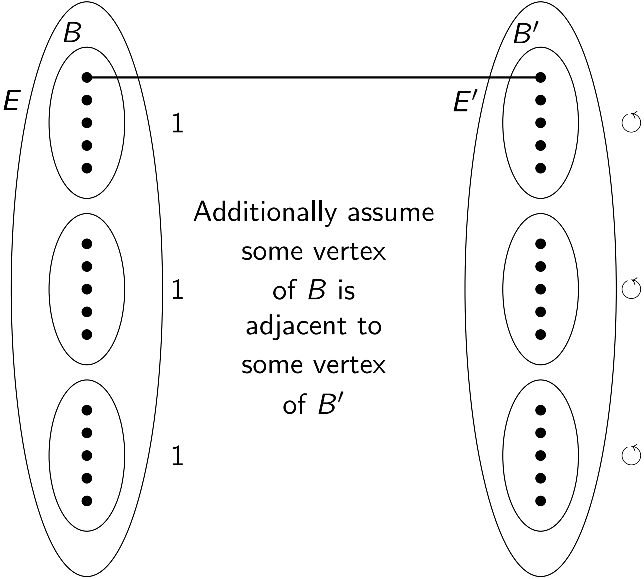
choose
$\gamma \in \mathrm{fix}_G(\mathcal{B})$
with
$\gamma|_{B'}$ a p-cycle
and
$\gamma|_B = 1$



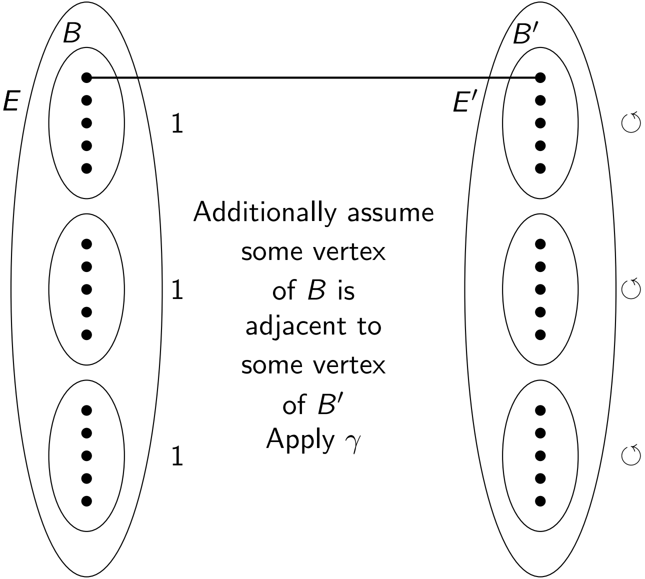


Additionally assume some vertex of B is adjacent to some vertex of B'



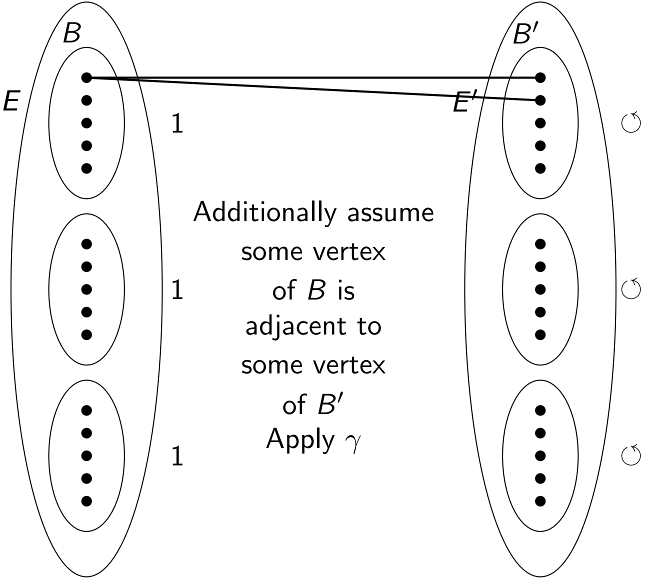


Additionally assume some vertex of B is adjacent to some vertex of B'



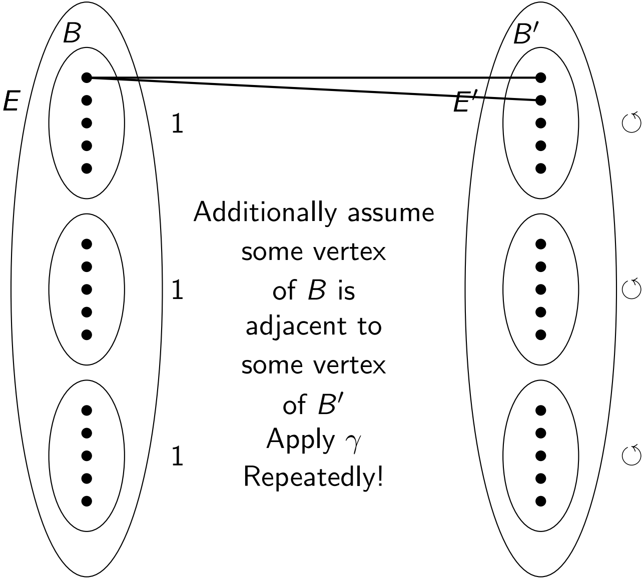
Additionally assume some vertex of B is adjacent to some vertex of B'

Apply γ



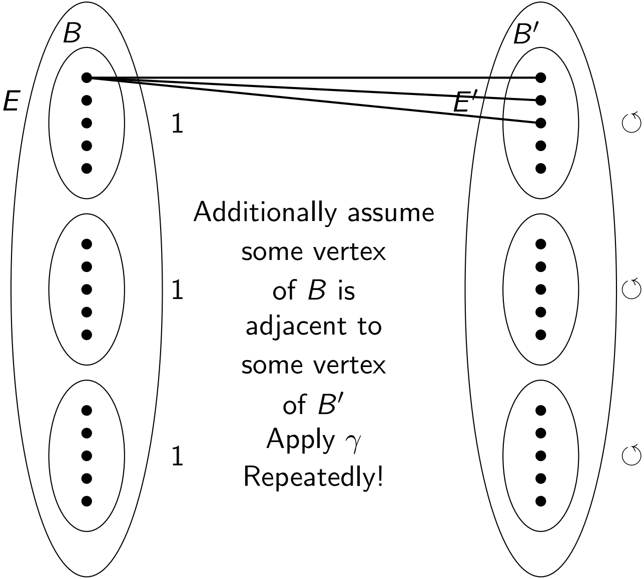
Additionally assume some vertex of B is adjacent to some vertex of B'

Apply γ



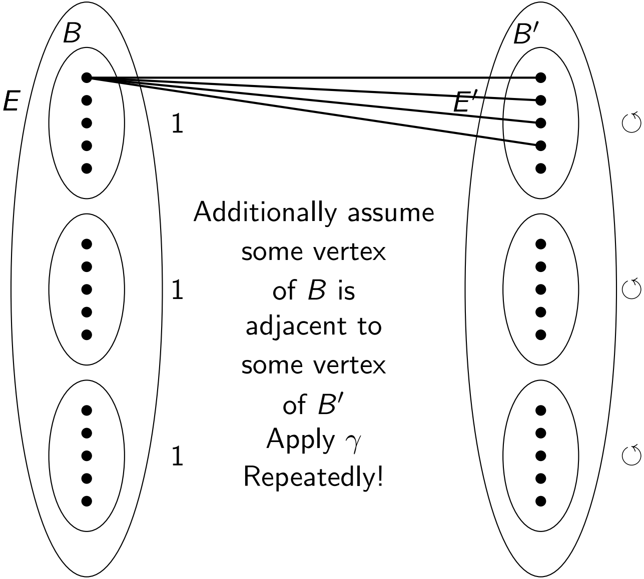
Additionally assume some vertex of B is adjacent to some vertex of B'

Apply γ Repeatedly!



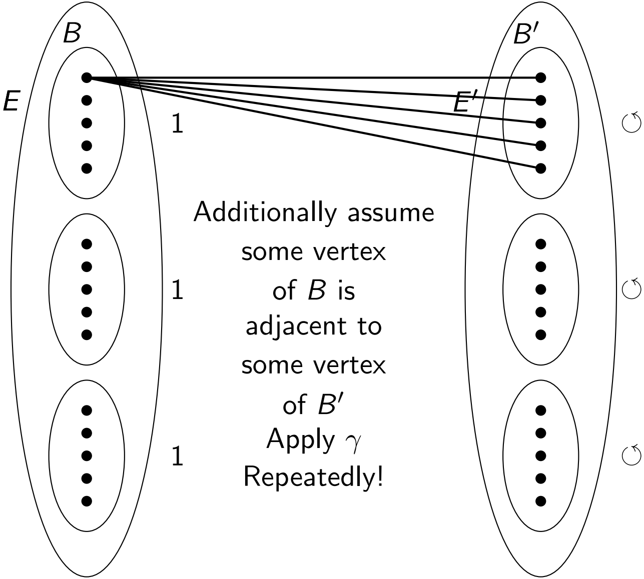
Additionally assume some vertex of B is adjacent to some vertex of B'

Apply γ Repeatedly!



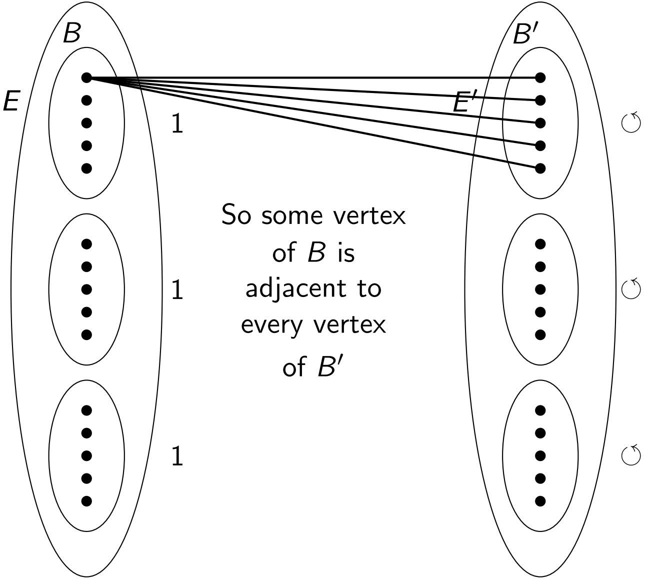
Additionally assume some vertex of B is adjacent to some vertex of B'

Apply γ Repeatedly!

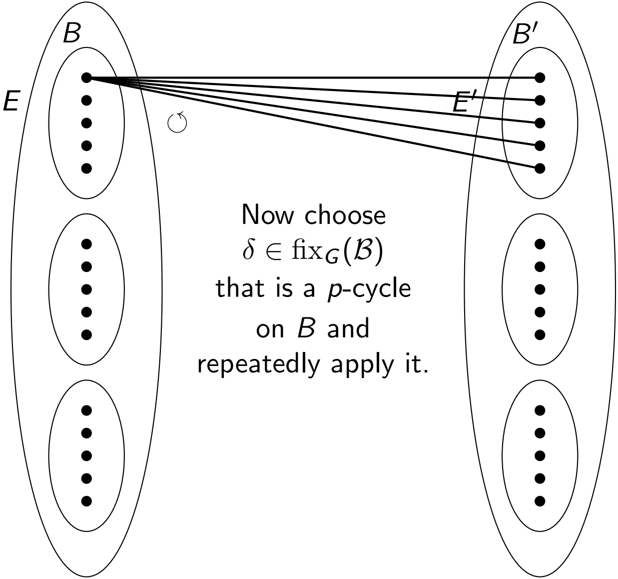


Additionally assume some vertex of B is adjacent to some vertex of B'

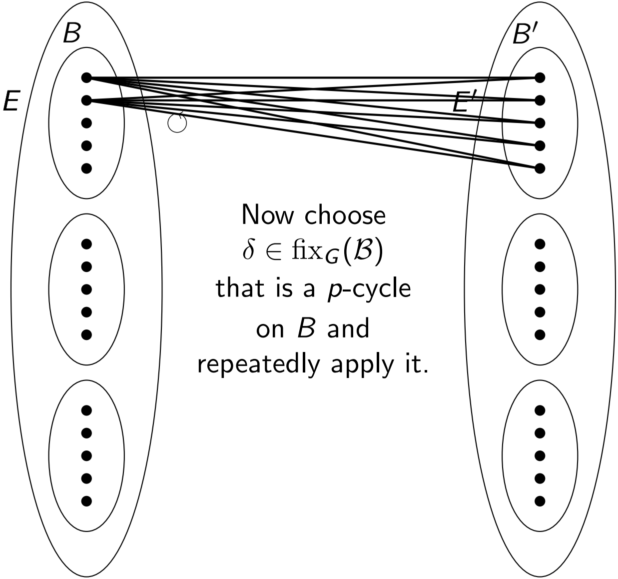
Apply γ Repeatedly!



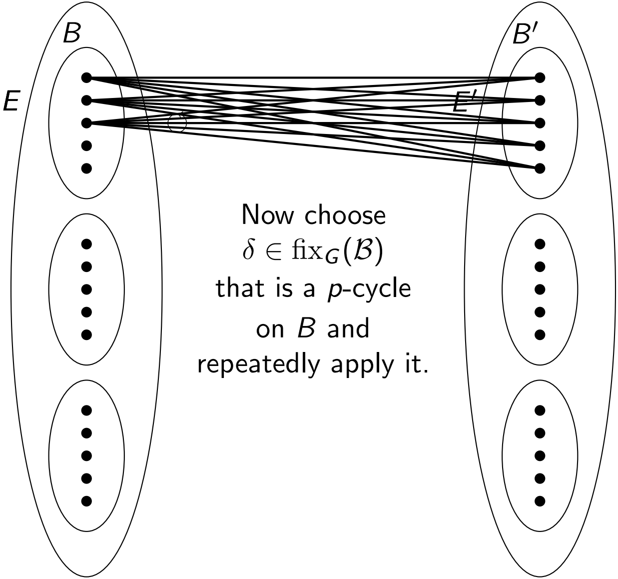
So some vertex of B is adjacent to every vertex of B'



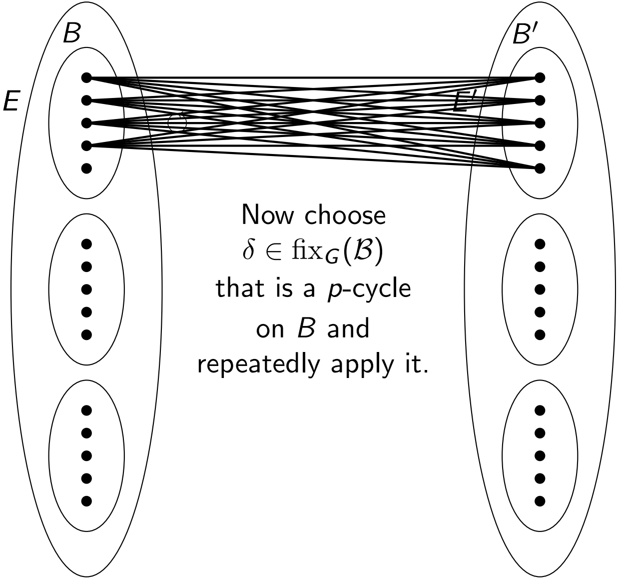
Now choose
$\delta \in \mathrm{fix}_G(\mathcal{B})$
that is a p-cycle
on B and
repeatedly apply it.



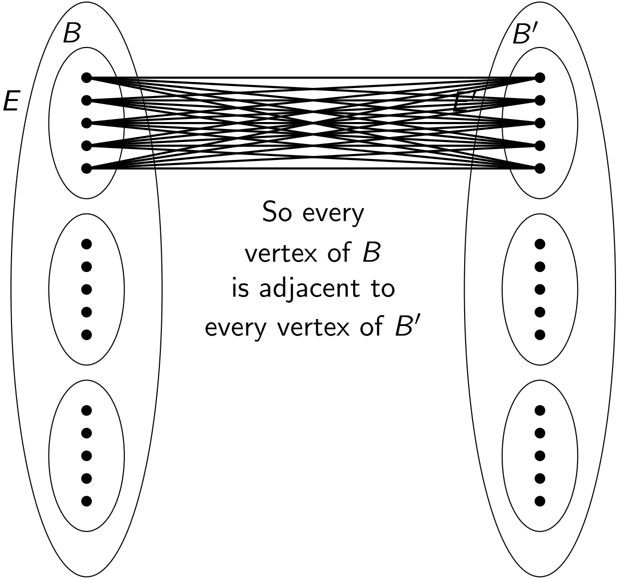
Now choose
$\delta \in \mathrm{fix}_G(\mathcal{B})$
that is a p-cycle
on B and
repeatedly apply it.



Now choose
$\delta \in \mathrm{fix}_G(\mathcal{B})$
that is a p-cycle
on B and
repeatedly apply it.



Now choose
$\delta \in \mathrm{fix}_G(\mathcal{B})$
that is a p-cycle
on B and
repeatedly apply it.



So every vertex of B is adjacent to every vertex of B'

So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge.

So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$.

So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$. If both endpoints of e are contained in some block E' of $\mathcal{E}$, then $g|_E(e) \in E(\Gamma)$ as $g|_E(e) = h(e)$ for $h = g$ if $E = E'$ and $h = 1$ if $E \neq E'$.

So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$. If both endpoints of e are contained in some block E' of $\mathcal{E}$, then $g|_E(e) \in E(\Gamma)$ as $g|_E(e) = h(e)$ for $h = g$ if $E = E'$ and $h = 1$ if $E \neq E'$. Otherwise, if $B \in \mathcal{B}$ contains one endpoint of e and $B' \in \mathcal{B}$ contains the other, So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$. If both endpoints of e are contained in some block E' of $\mathcal{E}$, then $g|_E(e) \in E(\Gamma)$ as $g|_E(e) = h(e)$ for $h = g$ if $E = E'$ and $h = 1$ if $E \neq E'$. Otherwise, if $B \in \mathcal{B}$ contains one endpoint of e and $B' \in \mathcal{B}$ contains the other, then B and B' are contained in different blocks of $\mathcal{E}$, So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$. If both endpoints of e are contained in some block E' of $\mathcal{E}$, then $g|_E(e) \in E(\Gamma)$ as $g|_E(e) = h(e)$ for $h = g$ if $E = E'$ and $h = 1$ if $E \neq E'$. Otherwise, if $B \in \mathcal{B}$ contains one endpoint of e and $B' \in \mathcal{B}$ contains the other, then B and B' are contained in different blocks of $\mathcal{E}$, and Γ contains every edge from B to B'.

So between two blocks of $\mathcal{B}$ contained in different blocks of $\mathcal{E}$ there is either no edge or every edge. Now let $g \in \mathrm{fix}_G(\mathcal{B})$ and $e \in E(\Gamma)$. If both endpoints of e are contained in some block E' of $\mathcal{E}$, then $g|_E(e) \in E(\Gamma)$ as $g|_E(e) = h(e)$ for $h = g$ if $E = E'$ and $h = 1$ if $E \neq E'$. Otherwise, if $B \in \mathcal{B}$ contains one endpoint of e and $B' \in \mathcal{B}$ contains the other, then B and B' are contained in different blocks of $\mathcal{E}$, and Γ contains every edge from B to B'. Then $g|_E(e) \in E(\Gamma)$ and $g|_E \in \mathrm{Aut}(\Gamma)$ for every $g \in \mathrm{fix}_G(\mathcal{B})$ and $E \in \mathcal{E}$.

Corollary 52

Let p and q be (not necessarily distinct primes),

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp,

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp,

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial. Indeed, otherwise $\mathrm{fix}_G(\mathcal{B})$ acting on any block of $\mathcal{B}$ (the image of the restriction homomorphism)

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial. Indeed, otherwise $\mathrm{fix}_G(\mathcal{B})$ acting on any block of $\mathcal{B}$ (the image of the restriction homomorphism) is primitive as $|B|$ is prime by Corollary 34.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial. Indeed, otherwise $\mathrm{fix}_G(\mathcal{B})$ acting on any block of $\mathcal{B}$ (the image of the restriction homomorphism) is primitive as $|B|$ is prime by Corollary 34. Also, if K is nontrivial on some other block B' then as a normal subgroup of primitive group is transitive by Corollary 35, K in its action on B' is transitive.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial. Indeed, otherwise $\mathrm{fix}_G(\mathcal{B})$ acting on any block of $\mathcal{B}$ (the image of the restriction homomorphism) is primitive as $|B|$ is prime by Corollary 34. Also, if K is nontrivial on some other block B' then as a normal subgroup of primitive group is transitive by Corollary 35, K in its action on B' is transitive. As B' has order p, p divides $|K|$.

Corollary 52

Let p and q be (not necessarily distinct primes), Γ a vertex-transitive digraph of order qp, and $G \leq \mathrm{Aut}(\Gamma)$ be transitive and have a normal complete block system with blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or $\Gamma \cong \Gamma_1 \wr \Gamma_2$, where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

Proof: If $\mathcal{E}$ consists of one block of size qp, then we first claim the kernel K of the restriction homomorphism from $\mathrm{fix}_G(\mathcal{B})$ into S_B, $B \in \mathcal{B}$, must be trivial. Indeed, otherwise $\mathrm{fix}_G(\mathcal{B})$ acting on any block of $\mathcal{B}$ (the image of the restriction homomorphism) is primitive as $|B|$ is prime by Corollary 34. Also, if K is nontrivial on some other block B' then as a normal subgroup of primitive group is transitive by Corollary 35, K in its action on B' is transitive. As B' has order p, p divides $|K|$. Then there is an element of order p that is trivial on B but a p-cycle on B', so $B \not\equiv B'$, a contradiction. This gives that a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p.

If $\mathcal{E}$ does not consist of one block of size qp, the only other possibility is that $\mathcal{E} = \mathcal{B}$.

If $\mathcal{E}$ does not consist of one block of size qp, the only other possibility is that $\mathcal{E} = \mathcal{B}$. Recall that in the wreath product $\Gamma_1 \wr \Gamma_2$ we have either no edges between copies of Γ_2 or every edge between copies of Γ_2.

If $\mathcal{E}$ does not consist of one block of size qp, the only other possibility is that $\mathcal{E} = \mathcal{B}$. Recall that in the wreath product $\Gamma_1 \wr \Gamma_2$ we have either no edges between copies of Γ_2 or every edge between copies of Γ_2. This is exactly what happens between the blocks of $\mathcal{B}$ by the proof of our previous result, If $\mathcal{E}$ does not consist of one block of size qp, the only other possibility is that $\mathcal{E} = \mathcal{B}$. Recall that in the wreath product $\Gamma_1 \wr \Gamma_2$ we have either no edges between copies of Γ_2 or every edge between copies of Γ_2. This is exactly what happens between the blocks of $\mathcal{B}$ by the proof of our previous result, and so $\Gamma \cong \Gamma_1 \wr \Gamma_2$ where $\Gamma_1 = \Gamma/\mathcal{B}$ and $\Gamma_2 = \Gamma[B]$, $B \in \mathcal{B}$.

A Useful Trick

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ is a CI-digraph of G if and only if $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is a CI-digraph of G, where α is any automorhpism of G.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ is a CI-digraph of G if and only if $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is a CI-digraph of G, where α is any automorhpism of G.

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ is a CI-digraph of G if and only if $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is a CI-digraph of G, where α is any automorhpism of G.

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Then $\beta\alpha^{-1}(\mathrm{Cay}(G, \alpha(S))) = \beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Then $\beta\alpha^{-1}(\mathrm{Cay}(G, \alpha(S))) = \beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Conversely, if $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph and $S' \subset G$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$,

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Then $\beta\alpha^{-1}(\mathrm{Cay}(G, \alpha(S))) = \beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Conversely, if $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph and $S' \subset G$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$, then $\mathrm{Cay}(G, \alpha(S)) \cong \mathrm{Cay}(G, S')$.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Then $\beta\alpha^{-1}(\mathrm{Cay}(G, \alpha(S))) = \beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Conversely, if $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph and $S' \subset G$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$, then $\mathrm{Cay}(G, \alpha(S)) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph of G, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, \alpha(S))) = \mathrm{Cay}(G, S')$.

A Useful Trick

Lemma 53

$\mathrm{Cay}(G, S)$ *is a CI-digraph of* G *if and only if* $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ *is a CI-digraph of* G*, where* α *is any automorhpism of* G*.*

Proof.

That $\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, \alpha(S))$ is Lemma 4. If $\mathrm{Cay}(G, S)$ is a CI-digraph, and $S' \subset G$ such that $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, \alpha(S))$, then $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, S)$ is a CI-digraph, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Then $\beta\alpha^{-1}(\mathrm{Cay}(G, \alpha(S))) = \beta(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. Conversely, if $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph and $S' \subset G$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S')$, then $\mathrm{Cay}(G, \alpha(S)) \cong \mathrm{Cay}(G, S')$. As $\mathrm{Cay}(G, \alpha(S))$ is a CI-digraph of G, there exists $\beta \in \mathrm{Aut}(G)$ such that $\beta(\mathrm{Cay}(G, \alpha(S))) = \mathrm{Cay}(G, S')$. Then $\beta\alpha(\mathrm{Cay}(G, S)) = \mathrm{Cay}(G, S')$. □

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \leq \mathrm{Aut}(\Gamma)$.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \leq \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \leq \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23,

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \leq \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23, we wish to show that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ and $(\mathbb{Z}_p^2)_L$ are conjugate in $\mathrm{Aut}(\Gamma)$.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \le \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23, we wish to show that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ and $(\mathbb{Z}_p^2)_L$ are conjugate in $\mathrm{Aut}(\Gamma)$. Typically, one first likes to show that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ is imprimitive,

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \leq \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23, we wish to show that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ and $(\mathbb{Z}_p^2)_L$ are conjugate in $\mathrm{Aut}(\Gamma)$. Typically, one first likes to show that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ is imprimitive, remembering that we may replace $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by a conjugate, if necessary.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \le \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23, we wish to show that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ and $(\mathbb{Z}_p^2)_L$ are conjugate in $\mathrm{Aut}(\Gamma)$. Typically, one first likes to show that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ is imprimitive, remembering that we may replace $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by a conjugate, if necessary. This is easy as both $(\mathbb{Z}_p^2)_L$ and $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ are contained in Sylow p-subgroups P_1 and P_2, respectively, of $\mathrm{Aut}(\Gamma)$.

$\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs (Godsil, 1983 [18])

Let p be prime. Our goal is to show that $\mathbb{Z}_p \times \mathbb{Z}_p$ is a CI-group with respect to digraphs. So let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p^2, S)$, and $\delta \in S_{\mathbb{Z}_p^2}$ such that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta \le \mathrm{Aut}(\Gamma)$. Remember this means $\delta(\Gamma)$ is a Cayley digraph of $\mathbb{Z}_p^2$ isomorphic to Γ. To apply Lemma 23, we wish to show that $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ and $(\mathbb{Z}_p^2)_L$ are conjugate in $\mathrm{Aut}(\Gamma)$. Typically, one first likes to show that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ is imprimitive, remembering that we may replace $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by a conjugate, if necessary. This is easy as both $(\mathbb{Z}_p^2)_L$ and $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ are contained in Sylow p-subgroups P_1 and P_2, respectively, of $\mathrm{Aut}(\Gamma)$. So there exists $\gamma \in \mathrm{Aut}(\Gamma)$ with $\gamma^{-1}P_2\gamma = P_1$, and $\langle(\mathbb{Z}_p^2)_L, \gamma^{-1}\delta^{-1}(\mathbb{Z}_p^2)_L\delta\gamma\rangle \le P_1$.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. $\square$

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \lhd G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40,

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems,

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems, one for each (normal) subgroup of order p.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems, one for each (normal) subgroup of order p. This follow as any two subgroups of order p can only intersect in the identity, and $(p+1)(p-1)+1 = p^2$.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems, one for each (normal) subgroup of order p. This follow as any two subgroups of order p can only intersect in the identity, and $(p+1)(p-1)+1 = p^2$. Let $\mathcal{B}$ consist of the cosets of $H \leq \mathbb{Z}_p^2$.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems, one for each (normal) subgroup of order p. This follow as any two subgroups of order p can only intersect in the identity, and $(p+1)(p-1)+1 = p^2$. Let $\mathcal{B}$ consist of the cosets of $H \leq \mathbb{Z}_p^2$. It is most convenient if $H = \langle(0,1)\rangle$.

Lemma 54

A transitive p-group G has a normal complete block system with blocks of size p.

Proof.

A p-group has nontrivial center, so may choose an element ρ in the center of G of order p. Then $\langle\rho\rangle \triangleleft G$ so its orbits form a complete block system $\mathcal{B}$. The blocks are nontrivial and as the order of an orbit of a group divides the order of the group, $\mathcal{B}$ has blocks of size p. □

So we may assume without loss of generality that $\langle(\mathbb{Z}_p^2)_L, \delta^{-1}(\mathbb{Z}_p^2)_L\delta\rangle$ has a complete block system $\mathcal{B}$ with blocks of size p. Then $\mathcal{B}$ is also a complete block system of $(\mathbb{Z}_p^2)_L$ by Lemma 40, and this latter group has $p+1$ different complete block systems, one for each (normal) subgroup of order p. This follow as any two subgroups of order p can only intersect in the identity, and $(p+1)(p-1)+1 = p^2$. Let $\mathcal{B}$ consist of the cosets of $H \leq \mathbb{Z}_p^2$. It is most convenient if $H = \langle(0,1)\rangle$. We now show how to arrange this.

One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle(0,1)\rangle$.

One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle(0,1)\rangle$. A linear transformation is of course a group automorphism of $\mathbb{Z}_p^2$, One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle(0,1)\rangle$. A linear transformation is of course a group automorphism of $\mathbb{Z}_p^2$, so replacing δ with $\delta\alpha$

One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle (0,1) \rangle$. A linear transformation is of course a group automorphism of $\mathbb{Z}_p^2$, so replacing δ with $\delta\alpha$ (or equivalently conjugating $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by α

One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle(0,1)\rangle$. A linear transformation is of course a group automorphism of $\mathbb{Z}_p^2$, so replacing δ with $\delta\alpha$ (or equivalently conjugating $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by α - and remember conjugating by α replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their image under α), One can think of $\mathbb{Z}_p^2$ as a vector space in the obvious way, and as there is a linear transformation which will map any one-dimensional subspace to any other one-dimensional subspace, there is a linear transformation α of the two-dimensional vector space $\mathbb{Z}_p^2$ which maps H to $\langle(0,1)\rangle$. A linear transformation is of course a group automorphism of $\mathbb{Z}_p^2$, so replacing δ with $\delta\alpha$ (or equivalently conjugating $\delta^{-1}(\mathbb{Z}_p^2)_L\delta$ by α - and remember conjugating by α replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their image under α), we may assume without loss of generality that $H = \langle(0,1)\rangle$ by Lemma 53.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p. In this case, $\delta^{-1}(\mathbb{Z}_p^2)_L\delta = (\mathbb{Z}_p^2)_L$ and we are finished!

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p. In this case, $\delta^{-1}(\mathbb{Z}_p^2)_L\delta = (\mathbb{Z}_p^2)_L$ and we are finished!
So we assume that Γ is isomorphic to a wreath product of two circulant digraphs of order p.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p. In this case, $\delta^{-1}(\mathbb{Z}_p^2)_L\delta = (\mathbb{Z}_p^2)_L$ and we are finished!
So we assume that Γ is isomorphic to a wreath product of two circulant digraphs of order p. This gives that
$P_1 = (\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p. In this case, $\delta^{-1}(\mathbb{Z}_p^2)_L\delta = (\mathbb{Z}_p^2)_L$ and we are finished!

So we assume that Γ is isomorphic to a wreath product of two circulant digraphs of order p. This gives that $P_1 = (\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$. Note that we have equality as opposed to "isomorphic to" as we know that $\mathcal{B}$ consists of the cosets of $\langle(0,1)\rangle$.

We now apply Lemma 52 (from the equivalence relation $\equiv$) to the Sylow p-subgroup P_1 and conclude that either $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p or that Γ is isomorphic to a wreath product of two circulant digraphs of order p. If $\mathrm{fix}_{P_1}(\mathcal{B})$ has order p then P_1 has order p^2 as $P_1/\mathcal{B}$ has order p. In this case, $\delta^{-1}(\mathbb{Z}_p^2)_L\delta = (\mathbb{Z}_p^2)_L$ and we are finished!

So we assume that Γ is isomorphic to a wreath product of two circulant digraphs of order p. This gives that

$P_1 = (\mathbb{Z}_p)_L \wr (\mathbb{Z}_p)_L = \{(i,j) \mapsto (i+a, j+b_i) : a, b_i \in \mathbb{Z}_p\}$. Note that we have equality as opposed to "isomorphic to" as we know that $\mathcal{B}$ consists of the cosets of $\langle(0,1)\rangle$.

We may similarly assume that $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40. This then implies that $\delta(\mathcal{B}) = \mathcal{B}$ (remembering again conjugating by δ replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their images under δ).

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40. This then implies that $\delta(\mathcal{B}) = \mathcal{B}$ (remembering again conjugating by δ replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their images under δ). By the Embedding Theorem 45 we then have $\delta \in S_p \wr S_p$.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40. This then implies that $\delta(\mathcal{B}) = \mathcal{B}$ (remembering again conjugating by δ replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their images under δ). By the Embedding Theorem 45 we then have $\delta \in S_p \wr S_p$. As $\delta/\mathcal{B}$ normalizes $(\mathbb{Z}_p^2)_L/\mathcal{B} = (\mathbb{Z}_p)_L$, $\delta \in \mathrm{AGL}(1,p) \wr S_p$.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40. This then implies that $\delta(\mathcal{B}) = \mathcal{B}$ (remembering again conjugating by δ replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their images under δ). By the Embedding Theorem 45 we then have $\delta \in S_p \wr S_p$. As $\delta/\mathcal{B}$ normalizes $(\mathbb{Z}_p^2)_L/\mathcal{B} = (\mathbb{Z}_p)_L$, $\delta \in \mathrm{AGL}(1,p) \wr S_p$. Similarly, δ normalizes $\mathrm{fix}_{P_1}(\mathcal{B}) \cong [(\mathbb{Z}_p)_L]^p$ and so $\delta \in \mathrm{AGL}(1,p) \wr \mathrm{AGL}(1,p)$.

As $P_1 \leq \mathrm{Aut}(\delta(\Gamma))$, $\delta^{-1}P_1\delta \leq \mathrm{Aut}(\Gamma)$ and is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. Applying a Sylow Theorem, after an appropriate conjugation, if necessary, we may assume that $\delta^{-1}P_1\delta = P_1$ so that δ normalizes P_1. As P_1 is also a Sylow p-subgroup of $S_{\mathbb{Z}_p^2}$, P_1 contains a regular cyclic subgroup and so $\mathcal{B}$ is the unique complete block system of P_1 with blocks of size p by Lemma 40. This then implies that $\delta(\mathcal{B}) = \mathcal{B}$ (remembering again conjugating by δ replaces orbits of $\bar{H}_L = \{h_L : h \in H\}$ with their images under δ). By the Embedding Theorem 45 we then have $\delta \in S_p \wr S_p$. As $\delta/\mathcal{B}$ normalizes $(\mathbb{Z}_p^2)_L/\mathcal{B} = (\mathbb{Z}_p)_L$, $\delta \in \mathrm{AGL}(1,p) \wr S_p$. Similarly, δ normalizes $\mathrm{fix}_{P_1}(\mathcal{B}) \cong [(\mathbb{Z}_p)_L]^p$ and so $\delta \in \mathrm{AGL}(1,p) \wr \mathrm{AGL}(1,p)$. Thus $\delta(i,j) = (mi + a, n_i j + b_i)$, where $m, n_i \in \mathbb{Z}_p^*$ and $a, b_i \in \mathbb{Z}_p$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\tau^{-1}\delta^{-1}\tau\delta(i,j)$$

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\tau^{-1}\delta^{-1}\tau\delta(i,j) \quad = \quad \tau^{-1}\delta^{-1}\tau(i, n_i j)$$

Now, as the map ω defined by $\omega(i,j) = (i - a, j - b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned} \tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\ &= \tau^{-1}\delta^{-1}(i+1, n_i j) \end{aligned}$$

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j) \\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j)
\end{aligned}$$

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1}j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j) \\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j) \\
&= (i, n_i n_{i+1}^{-1} j)
\end{aligned}$$

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \le \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \le \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned} \tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\ &= \tau^{-1}\delta^{-1}(i+1, n_i j) \\ &= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j) \\ &= (i, n_i n_{i+1}^{-1} j) \end{aligned}$$

As $\tau, \delta^{-1}\tau\delta \in P_1$, $\tau^{-1}\delta^{-1}\tau\delta \in P_1$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1}j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j)\\
&= \tau^{-1}\delta^{-1}(i+1, n_i j)\\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j)\\
&= (i, n_i n_{i+1}^{-1} j)
\end{aligned}$$

As $\tau, \delta^{-1}\tau\delta \in P_1$, $\tau^{-1}\delta^{-1}\tau\delta \in P_1$. As $|\mathbb{Z}_p^*| = p-1$, $|\tau^{-1}\delta^{-1}\tau\delta|$ is relatively prime to p and $\tau^{-1}\delta^{-1}\tau\delta = 1$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1}j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j) \\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j) \\
&= (i, n_i n_{i+1}^{-1} j)
\end{aligned}$$

As $\tau, \delta^{-1}\tau\delta \in P_1$, $\tau^{-1}\delta^{-1}\tau\delta \in P_1$. As $|\mathbb{Z}_p^*| = p-1$, $|\tau^{-1}\delta^{-1}\tau\delta|$ is relatively prime to p and $\tau^{-1}\delta^{-1}\tau\delta = 1$. Thus $n_i n_{i+1}^{-1} = 1$ and $n_i = n_{i+1}$.

Now, as the map ω defined by $\omega(i,j) = (i-a, j-b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j) \\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j) \\
&= (i, n_i n_{i+1}^{-1} j)
\end{aligned}$$

As $\tau, \delta^{-1}\tau\delta \in P_1$, $\tau^{-1}\delta^{-1}\tau\delta \in P_1$. As $|\mathbb{Z}_p^*| = p-1$, $|\tau^{-1}\delta^{-1}\tau\delta|$ is relatively prime to p and $\tau^{-1}\delta^{-1}\tau\delta = 1$. Thus $n_i n_{i+1}^{-1} = 1$ and $n_i = n_{i+1}$. Then $\delta \in \mathrm{Aut}(\mathbb{Z}_p^2)$

Now, as the map ω defined by $\omega(i,j) = (i - a, j - b_i)$ is in $P_1 \leq \mathrm{Aut}(\Gamma)$, replacing δ with $\delta\omega$ we may assume that $\delta(i,j) = (mi, n_i j)$. As the map $(i,j) \mapsto (m^{-1}i, j)$ is an automorphism of $\mathbb{Z}_p^2$, replacing $\delta(\Gamma)$ by its image under this map by Lemma 53 we may also assume that $m = 1$ and $\delta(i,j) = (i, n_i j)$. Then $\delta^{-1} = (i, n_i^{-1} j)$, and letting $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ by $\tau(i,j) = (i+1, j)$ (so $\tau \in (\mathbb{Z}_p^2)_L \leq \mathrm{Aut}(\Gamma)$) we have

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j) \\
&= \tau^{-1}(i+1, n_i n_{i+1}^{-1} j) \\
&= (i, n_i n_{i+1}^{-1} j)
\end{aligned}$$

As $\tau, \delta^{-1}\tau\delta \in P_1$, $\tau^{-1}\delta^{-1}\tau\delta \in P_1$. As $|\mathbb{Z}_p^*| = p - 1$, $|\tau^{-1}\delta^{-1}\tau\delta|$ is relatively prime to p and $\tau^{-1}\delta^{-1}\tau\delta = 1$. Thus $n_i n_{i+1}^{-1} = 1$ and $n_i = n_{i+1}$. Then $\delta \in \mathrm{Aut}(\mathbb{Z}_p^2)$ and $\mathbb{Z}_p^2$ is a CI-group with respect to digraphs.

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$.

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$.

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\tau^k(i,j)$$

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\tau^k(i,j) = \tau^{k-1}(i+1, j+b_i)$$

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\begin{aligned} \tau^k(i,j) &= \tau^{k-1}(i+1, j+b_i) \\ &= \tau^{k-2}(i+2, j+b_i+b_{i+1}) \end{aligned}$$

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\begin{aligned} \tau^k(i,j) &= \tau^{k-1}(i+1, j+b_i) \\ &= \tau^{k-2}(i+2, j+b_i+b_{i+1}) \\ &= (i+k, j+b_i+b_{i+1}+\ldots+b_{i+k-1}) \end{aligned}$$

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\begin{aligned} \tau^k(i,j) &= \tau^{k-1}(i+1, j+b_i) \\ &= \tau^{k-2}(i+2, j+b_i+b_{i+1}) \\ &= (i+k, j+b_i+b_{i+1}+\ldots+b_{i+k-1}) \end{aligned}$$

and so $\tau^p(i,j) = (i, j+1)$ and τ has order p^2.

What about $\mathbb{Z}_{p^2}$? Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Most of the argument for $\mathbb{Z}_{p^2}$ is the same as for $\mathbb{Z}_p^2$. In fact, I like to think of $(\mathbb{Z}_{p^2})_L$ (or more accurately a regular cyclic subgroup) acting on $\mathbb{Z}_p \times \mathbb{Z}_p$ as being generated by the map $\tau : \mathbb{Z}_p^2 \mapsto \mathbb{Z}_p^2$ be given by $\tau(i,j) = (i+1, j+b_i)$, where $b_i = 0$ if $i \neq p-1$ and $b_{p-1} = 1$. Note that

$$\begin{aligned}
\tau^k(i,j) &= \tau^{k-1}(i+1, j+b_i) \\
&= \tau^{k-2}(i+2, j+b_i+b_{i+1}) \\
&= (i+k, j+b_i+b_{i+1}+\ldots+b_{i+k-1})
\end{aligned}$$

and so $\tau^p(i,j) = (i, j+1)$ and τ has order p^2. The argument is a little easier as $\langle\tau\rangle$ has a unique subgroup of order p, and so exactly one complete block system with blocks of size p instead of $p+1$ for $\mathbb{Z}_p^2$.

But the end is different!

But the end is different! The similar arguments will get us to $\delta(i, j) = (ni, mj)$ as before, but there are typically more such maps

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms).

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem!

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity.

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs.

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups.

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups. If $p = 3$ and Γ is a graph, then all choices for m and n are contained in $\mathrm{Aut}(\Gamma)$ and so $\mathbb{Z}_9$ is a CI-group with respect to graphs.

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups. If $p = 3$ and Γ is a graph, then all choices for m and n are contained in $\mathrm{Aut}(\Gamma)$ and so $\mathbb{Z}_9$ is a CI-group with respect to graphs. For all other cases, we can choose m and n to be different, for an appropriate graph or digraph

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups. If $p = 3$ and Γ is a graph, then all choices for m and n are contained in $\mathrm{Aut}(\Gamma)$ and so $\mathbb{Z}_9$ is a CI-group with respect to graphs. For all other cases, we can choose m and n to be different, for an appropriate graph or digraph (for example choosing both (di)graphs in the wreath product to be (directed) cycles of length p will work), But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups. If $p = 3$ and Γ is a graph, then all choices for m and n are contained in $\mathrm{Aut}(\Gamma)$ and so $\mathbb{Z}_9$ is a CI-group with respect to graphs. For all other cases, we can choose m and n to be different, for an appropriate graph or digraph (for example choosing both (di)graphs in the wreath product to be (directed) cycles of length p will work), and straightforward computations show that such a map is not an automorphism of $\mathbb{Z}_{p^2}$.

But the end is different! The similar arguments will get us to $\delta(i,j) = (ni, mj)$ as before, but there are typically more such maps (there are exactly $(p-1)^2$) than there are automorphisms of $\mathbb{Z}_{p^2}$ relatively prime to p (there are $p-1$ such automorphisms). Note that we have solved the isomorphism problem! If $p = 2$ these numbers are the same and the only choices for m and n are both 1 which gives δ is the identity. So $\mathbb{Z}_4$ is a CI-group with respect to digraphs. Pretty much the same argument will show that in fact $\mathbb{Z}_2^2$ and $\mathbb{Z}_4$ are CI-groups. If $p = 3$ and Γ is a graph, then all choices for m and n are contained in $\mathrm{Aut}(\Gamma)$ and so $\mathbb{Z}_9$ is a CI-group with respect to graphs. For all other cases, we can choose m and n to be different, for an appropriate graph or digraph (for example choosing both (di)graphs in the wreath product to be (directed) cycles of length p will work), and straightforward computations show that such a map is not an automorphism of $\mathbb{Z}_{p^2}$. So in all other cases $\mathbb{Z}_{p^2}$ is not a CI-group with respect to (di)graphs.

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes.

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder.

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations.

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations. We will use a well known method for finding blocks:

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations. We will use a well known method for finding blocks:

Definition 55

Let G be a group of order n.

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations. We will use a well known method for finding blocks:

Definition 55

Let G be a group of order n. We say that G is a **Burnside group** *if whenever $H \leq S_n$ contains G as a transitive and regular subgroup*

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations. We will use a well known method for finding blocks:

Definition 55

Let G be a group of order n. We say that G is a **Burnside group** *if whenever $H \leq S_n$ contains G as a transitive and regular subgroup then H is either doubly-transitive or imprimitive.*

$\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs. Alspach and Parsons 1979 [2] and Klin and Pöschel 1981 [20]

Let $q < p$ be distinct primes. The basic structure of the proof is more or less the same as the previous proof - but some parts are easier and others harder. The first thing we will do is to find blocks of size p after appropriate conjugations. We will use a well known method for finding blocks:

Definition 55

Let G be a group of order n. We say that G is a **Burnside group** *if whenever $H \leq S_n$ contains G as a transitive and regular subgroup then H is either doubly-transitive or imprimitive.*

Theorem 56

An abelian group with a cyclic Sylow subgroup is a Burnside group.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$. So we assume it is imprimitive, and will also assume that it has a complete block system $\mathcal{B}$ with blocks of size q as otherwise we have blocks of size p which is our goal.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$. So we assume it is imprimitive, and will also assume that it has a complete block system $\mathcal{B}$ with blocks of size q as otherwise we have blocks of size p which is our goal. As $p > q$, a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ must be trivial, and as $G/\mathcal{B} \leq S_p$ a Sylow p-subgroup of G has order p.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle (\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L \rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$. So we assume it is imprimitive, and will also assume that it has a complete block system $\mathcal{B}$ with blocks of size q as otherwise we have blocks of size p which is our goal. As $p > q$, a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ must be trivial, and as $G/\mathcal{B} \leq S_p$ a Sylow p-subgroup of G has order p. Thus there exists $\gamma \in G$ such that a Sylow p-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow p-subgroup P of $(\mathbb{Z}_{qp})_L$.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$. So we assume it is imprimitive, and will also assume that it has a complete block system $\mathcal{B}$ with blocks of size q as otherwise we have blocks of size p which is our goal. As $p > q$, a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ must be trivial, and as $G/\mathcal{B} \leq S_p$ a Sylow p-subgroup of G has order p. Thus there exists $\gamma \in G$ such that a Sylow p-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow p-subgroup P of $(\mathbb{Z}_{qp})_L$. Then $P \triangleleft (\mathbb{Z}_{qp})_L$ and $P \triangleleft \gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ so $P \triangleleft \langle(\mathbb{Z}_{qp})_L, \gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma\rangle$ and admits a complete block system with blocks of size p.

Let $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ be a Cayley digraph of $\mathbb{Z}_{qp}$, and $\delta \in S_{qp}$ such that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta \le \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{qp}, S))$. Then $G = \langle(\mathbb{Z}_{qp})_L, \delta^{-1}\mathbb{Z}_{qp})_L\rangle$ contains a regular cyclic subgroup and so is doubly-transitive or imprimitive by Theorem 56. If it is doubly-transitive, then $\mathrm{Cay}(\mathbb{Z}_{qp}, S)$ is either a complete graph or its complement, and is a CI-digraph of $\mathbb{Z}_{qp}$. So we assume it is imprimitive, and will also assume that it has a complete block system $\mathcal{B}$ with blocks of size q as otherwise we have blocks of size p which is our goal. As $p > q$, a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ must be trivial, and as $G/\mathcal{B} \le S_p$ a Sylow p-subgroup of G has order p. Thus there exists $\gamma \in G$ such that a Sylow p-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow p-subgroup P of $(\mathbb{Z}_{qp})_L$. Then $P \triangleleft (\mathbb{Z}_{qp})_L$ and $P \triangleleft \gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ so $P \triangleleft \langle(\mathbb{Z}_{qp})_L, \gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma\rangle$ and admits a complete block system with blocks of size p. We may thus assume without loss of generality that $\mathcal{B}$ consists of blocks of size p.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$. Again we will not repeat this argument.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$. Again we will not repeat this argument. This give $\delta(i, j) = (mi + a, n_i j + b_i)$ where $m \in \mathbb{Z}_q^*$, $b \in \mathbb{Z}_q$, $n_i \in \mathbb{Z}_p^*$, and $b_i \in \mathbb{Z}_p$.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$. Again we will not repeat this argument. This give $\delta(i, j) = (mi + a, n_i j + b_i)$ where $m \in \mathbb{Z}_q^*$, $b \in \mathbb{Z}_q$, $n_i \in \mathbb{Z}_p^*$, and $b_i \in \mathbb{Z}_p$. As the map $(i, j) \mapsto (i - a, j)$ is contained in $\mathrm{Aut}(\Gamma)$ we may assume that $a = 1$, Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$. Again we will not repeat this argument. This give $\delta(i, j) = (mi + a, n_i j + b_i)$ where $m \in \mathbb{Z}_q^*$, $b \in \mathbb{Z}_q$, $n_i \in \mathbb{Z}_p^*$, and $b_i \in \mathbb{Z}_p$. As the map $(i, j) \mapsto (i - a, j)$ is contained in $\mathrm{Aut}(\Gamma)$ we may assume that $a = 1$, and as the map $(i, j) \mapsto (mi, j)$ is an automorphism of $\mathbb{Z}_{qp}$ we may assume that $m = 1$.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1, q) \wr \mathrm{AGL}(1, p)$. Again we will not repeat this argument. This give $\delta(i, j) = (mi + a, n_i j + b_i)$ where $m \in \mathbb{Z}_q^*$, $b \in \mathbb{Z}_q$, $n_i \in \mathbb{Z}_p^*$, and $b_i \in \mathbb{Z}_p$. As the map $(i, j) \mapsto (i - a, j)$ is contained in $\mathrm{Aut}(\Gamma)$ we may assume that $a = 1$, and as the map $(i, j) \mapsto (mi, j)$ is an automorphism of $\mathbb{Z}_{qp}$ we may assume that $m = 1$. Thus $\delta(i, j) = (i, n_i j + b_i)$, and $G/\mathcal{B} \cong \mathbb{Z}_q$.

Next, we show that after appropriate conjugations we may assume that $\delta(\mathcal{B}) = \mathcal{B}$. This works pretty much as in the the argument for $\mathbb{Z}_p^2$, but is easier as $(\mathbb{Z}_{qp})_L$ contains a unique complete block system with blocks of size p. So we will not repeat this argument. This gives $\delta \in S_q \wr S_p$, and again similar arguments to the $\mathbb{Z}_p^2$ argument give that after appropriate conjugations we may assume that $\delta \in \mathrm{AGL}(1,q) \wr \mathrm{AGL}(1,p)$. Again we will not repeat this argument. This give $\delta(i,j) = (mi + a, n_i j + b_i)$ where $m \in \mathbb{Z}_q^*$, $b \in \mathbb{Z}_q$, $n_i \in \mathbb{Z}_p^*$, and $b_i \in \mathbb{Z}_p$. As the map $(i,j) \mapsto (i-a,j)$ is contained in $\mathrm{Aut}(\Gamma)$ we may assume that $a = 1$, and as the map $(i,j) \mapsto (mi,j)$ is an automorphism of $\mathbb{Z}_{qp}$ we may assume that $m = 1$. Thus $\delta(i,j) = (i, n_i j + b_i)$, and $G/\mathcal{B} \cong \mathbb{Z}_q$. We will now deviate from our task and consider what happens if G has a Sylow q-subgroup of order q.

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G,

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$.

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup.

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$.

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$. Now, $\delta^{-1}(i,j) = (i, n_i^{-1}j - n_i^{-1}b_i)$ as

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$. Now, $\delta^{-1}(i,j) = (i, n_i^{-1}j - n_i^{-1}b_i)$ as

$$\delta(i, n_i^{-1}j - n_i b_i)$$

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$. Now, $\delta^{-1}(i,j) = (i, n_i^{-1}j - n_i^{-1}b_i)$ as

$$\delta(i, n_i^{-1}j - n_i b_i) \quad = \quad (i, n_i(n_i^{-1}j - n_i^{-1}b_i) + b_i)$$

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$. Now, $\delta^{-1}(i,j) = (i, n_i^{-1}j - n_i^{-1}b_i)$ as

$$\begin{aligned}\delta(i, n_i^{-1}j - n_i b_i) &= (i, n_i(n_i^{-1}j - n_i^{-1}b_i) + b_i)\\ &= (i, j - b_i + b_i)\end{aligned}$$

Lemma 57

If G has a Sylow q-subgroup of order q, then Γ is a CI-digraph with respect to $\mathbb{Z}_{qp}$.

Proof.

If G has a Sylow q-subgroup of order q, then $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ contain Sylow q-subgroups of G, so there exists $\gamma \in G$ such that a Sylow q-subgroup of $\gamma^{-1}\delta^{-1}(\mathbb{Z}_{qp})_L\delta\gamma$ is a Sylow q-subgroup of $(\mathbb{Z}_{qp})_L$. So we assume without loss of generality that $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$ have the same Sylow q-subgroup. Let $\tau \in (\mathbb{Z}_{qp})_L$ be given by $\tau(i,j) = (i+1,j)$ so that $\langle\tau\rangle$ is a Sylow q-subgroup of both $(\mathbb{Z}_{qp})_L$ and $\delta^{-1}(\mathbb{Z}_{qp})_L\delta$. Now, $\delta^{-1}(i,j) = (i, n_i^{-1}j - n_i^{-1}b_i)$ as

$$\begin{aligned}
\delta(i, n_i^{-1}j - n_ib_i) &= (i, n_i(n_i^{-1}j - n_i^{-1}b_i) + b_i) \\
&= (i, j - b_i + b_i) \\
&= (i, j)
\end{aligned}$$

Then

Then

$$\tau^{-1}\delta^{-1}\tau\delta(i,j)$$

Then

$$\tau^{-1}\delta^{-1}\tau\delta(i,j) \quad = \quad \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)$$

Then

$$\begin{aligned}\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)\\ &= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i)\end{aligned}$$

Then

$$\begin{aligned}\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)\\ &= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i)\\ &= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1})\end{aligned}$$

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1}))
\end{aligned}$$

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}$$

Then

$$\begin{aligned} \tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\ &= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\ &= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\ &= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\ &= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})). \end{aligned}$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle \tau \rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$.

Then

$$
\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}
$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$.

Then

$$
\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)\\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i)\\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1})\\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1}))\\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}
$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$.

Then

$$
\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}
$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$. Set $n_i = n$.

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)\\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i)\\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1})\\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1}))\\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$. Set $n_i = n$. Then $n^{-1}(b_i - b_{i+1}) = 0$ and $b_i = b_{i+1}$ for all $i \in \mathbb{Z}_p$. Then $b_i = b$ for all $i \in \mathbb{Z}_p$,

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$. Set $n_i = n$. Then $n^{-1}(b_i - b_{i+1}) = 0$ and $b_i = b_{i+1}$ for all $i \in \mathbb{Z}_p$. Then $b_i = b$ for all $i \in \mathbb{Z}_p$, and $\delta(i,j) = (i, nj + b)$.

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i)\\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i)\\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1})\\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1}))\\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1}n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$. Set $n_i = n$. Then $n^{-1}(b_i - b_{i+1}) = 0$ and $b_i = b_{i+1}$ for all $i \in \mathbb{Z}_p$. Then $b_i = b$ for all $i \in \mathbb{Z}_p$, and $\delta(i,j) = (i, nj + b)$. We may assume $b = 0$,

Then

$$\begin{aligned}
\tau^{-1}\delta^{-1}\tau\delta(i,j) &= \tau^{-1}\delta^{-1}\tau(i, n_i j + b_i) \\
&= \tau^{-1}\delta^{-1}(i+1, n_i j + b_i) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1}(n_i j + b_i) - n_{i+1}^{-1} b_{i+1}) \\
&= \tau^{-1}(i+1, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})) \\
&= (i, n_{i+1}^{-1} n_i j + n_{i+1}^{-1}(b_i - b_{i+1})).
\end{aligned}$$

Also, $\tau^{-1}\delta^{-1}\tau\delta \in \langle\tau\rangle$ we see that $\tau^{-1}\delta^{-1}\tau\delta = 1$. Hence $n_{i+1}^{-1} n_i = 1$ and $n_i = n_{i+1}$ for all $i \in \mathbb{Z}_p$. Thus $n_i = n_j$ for all $i, j \in \mathbb{Z}_p$. Set $n_i = n$. Then $n^{-1}(b_i - b_{i+1}) = 0$ and $b_i = b_{i+1}$ for all $i \in \mathbb{Z}_p$. Then $b_i = b$ for all $i \in \mathbb{Z}_p$, and $\delta(i,j) = (i, nj + b)$. We may assume $b = 0$, and so $\delta \in \mathrm{Aut}(\mathbb{Z}_{qp})$ and the result follows.

Lemma 58

If $q \nmid (p-1)$ then a Sylow q-subgroup of G has order q.

Lemma 58

If $q \nmid (p-1)$ then a Sylow q-subgroup of G has order q.

Proof.

$|G|$ divides $|\mathrm{AGL}(1,q)| \cdot |\mathrm{AGL}(1,p)|^q$ is not divisible by q^2. □

Lemma 58

If $q \not| (p-1)$ then a Sylow q-subgroup of G has order q.

Proof.

$|G|$ divides $|\mathrm{AGL}(1,q)| \cdot |\mathrm{AGL}(1,p)|^q$ is not divisible by q^2. □

Corollary 59

If $q \not| (p-1)$ then $\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs.

Lemma 58

If $q \nmid (p-1)$ then a Sylow q-subgroup of G has order q.

Proof.

$|G|$ divides $|\mathrm{AGL}(1,q)| \cdot |\mathrm{AGL}(1,p)|^q$ is not divisible by q^2. $\square$

Corollary 59

If $q \nmid (p-1)$ then $\mathbb{Z}_{qp}$ is a CI-group with respect to digraphs.

BUT WE USED NO GRAPH THEORY IN THIS PROOF!

Lemma 58

If $q \not| (p-1)$ *then a Sylow* q*-subgroup of* G *has order* q*.*

Proof.

$|G|$ divides $|\mathrm{AGL}(1,q)| \cdot |\mathrm{AGL}(1,p)|^q$ is not divisible by q^2. $\square$

Corollary 59

If $q \not| (p-1)$ *then* $\mathbb{Z}_{qp}$ *is a CI-group with respect to digraphs.*

BUT WE USED NO GRAPH THEORY IN THIS PROOF!

Theorem 60 (Pálfy 1987 [32])

If $q \not| (p-1)$ *then* $\mathbb{Z}_{qp}$ *is a CI-group.*

We now return from our detour and no longer assume that $q \nmid (p-1)$.

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p.

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p. The case where a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p works exactly as it did with $\mathbb{Z}_p^2$:

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p. The case where a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p works exactly as it did with $\mathbb{Z}_p^2$: $G/\mathcal{B} \cong \mathbb{Z}_q$ and a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ is normal.

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p. The case where a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p works exactly as it did with $\mathbb{Z}_p^2$: $G/\mathcal{B} \cong \mathbb{Z}_q$ and a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ is normal. This implies that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta = (\mathbb{Z}_{qp})_L$ and Γ is a CI-digraph of $\mathbb{Z}_{qp}$.

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p. The case where a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p works exactly as it did with $\mathbb{Z}_p^2$: $G/\mathcal{B} \cong \mathbb{Z}_q$ and a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ is normal. This implies that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta = (\mathbb{Z}_{qp})_L$ and Γ is a CI-digraph of $\mathbb{Z}_{qp}$.
Otherwise, we have that $(\mathbb{Z}_q)_L \wr (\mathbb{Z}_p)_L \leq \mathrm{Aut}(\Gamma)$ (and is in $\mathrm{Aut}(\delta(\Gamma))$), and so the map $(i,j) \mapsto (i, j - b_i)$ is contained in $\mathrm{Aut}(\Gamma)$,

We now return from our detour and no longer assume that $q \not| (p-1)$. We will need to use the digraph structure and applying Lemma 51 as before, we have that either a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p or Γ is isomorphic to a wreath product of a circulant digraph of order q and a circulant digraph of order p. The case where a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ has order p works exactly as it did with $\mathbb{Z}_p^2$: $G/\mathcal{B} \cong \mathbb{Z}_q$ and a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{B})$ is normal. This implies that $\delta^{-1}(\mathbb{Z}_{qp})_L\delta = (\mathbb{Z}_{qp})_L$ and Γ is a CI-digraph of $\mathbb{Z}_{qp}$.
Otherwise, we have that $(\mathbb{Z}_q)_L \wr (\mathbb{Z}_p)_L \leq \mathrm{Aut}(\Gamma)$ (and is in $\mathrm{Aut}(\delta(\Gamma))$), and so the map $(i,j) \mapsto (i, j - b_i)$ is contained in $\mathrm{Aut}(\Gamma)$, and composing this map with δ on the right we may assume without loss of generality that $\delta(i,j) = (i, n_i j)$.

Let $\tau' = \delta^{-1}\tau\delta$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod{q}$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod{q}$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$.

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(0,j)$$

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(0,j) \quad = \quad \omega|_{B_0}\tau'(0,\ell_0^{-1}j)$$

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

$$\begin{aligned}
\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(0,j) &= \omega|_{B_0}\tau'(0, \ell_0^{-1}j) \\
&= \omega|_{B_0}(1, \ell_0\ell_0^{-1}j)
\end{aligned}$$

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

$$\begin{aligned}
\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(0,j) &= \omega|_{B_0}\tau'(0, \ell_0^{-1}j) \\
&= \omega|_{B_0}(1, \ell_0\ell_0^{-1}j) \\
&= \omega|_{B_0}(1,j)
\end{aligned}$$

Let $\tau' = \delta^{-1}\tau\delta$. Then $\tau'(i,j) = (i+1, \ell_i j)$ where $\ell_i \in \mathbb{Z}_p^*$. Of course, we can compute each ℓ_i, but it turns out that this only complicates the proof, so we will stay with the ℓ_i. As $|\tau'|$ has order q as it is a conjugate of τ, it must be the case that $\Pi_{i=0}^{q-1}\ell_i = 1 \pmod q$. Also, let $\omega = \tau^{-1}\tau'$, so that $\omega(i,j) = (i, \ell_i j)$. Let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$ and $\mathcal{B} = \{B_i : i \in \mathbb{Z}_q\}$. By Lemma 51, we have that $\omega|_{B_i} \in \mathrm{Aut}(\Gamma)$ for every $i \in \mathbb{Z}_q$. Now,

$$
\begin{aligned}
\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(0,j) &= \omega|_{B_0}\tau'(0, \ell_0^{-1}j) \\
&= \omega|_{B_0}(1, \ell_0\ell_0^{-1}j) \\
&= \omega|_{B_0}(1,j) \\
&= (1,j)
\end{aligned}
$$

Also,

Also,

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j)$$

Also,

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) \quad = \quad \omega|_{B_0}\tau'(p-1,j)$$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\end{aligned}$$

Also,

$$\begin{aligned}
\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j) \\
&= \omega|_{B_0}(0,\ell_{p-1}j) \\
&= (0,\ell_{p-1}\ell_0 j)
\end{aligned}$$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\\ &= (0,\ell_{p-1}\ell_0 j)\end{aligned}$$

and if $i \neq 0, p-1$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\\ &= (0,\ell_{p-1}\ell_0 j)\end{aligned}$$

and if $i \neq 0, p-1$

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(i,j)$$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\\ &= (0,\ell_{p-1}\ell_0 j)\end{aligned}$$

and if $i \neq 0, p-1$

$$\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(i,j) = \omega|_{B_0}\tau'(i,j)$$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\\ &= (0,\ell_{p-1}\ell_0 j)\end{aligned}$$

and if $i \neq 0, p-1$

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(i,j) &= \omega|_{B_0}\tau'(i,j)\\ &= \omega|_{B_0}(i+1,\ell_i j)\end{aligned}$$

Also,

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(p-1,j) &= \omega|_{B_0}\tau'(p-1,j)\\ &= \omega|_{B_0}(0,\ell_{p-1}j)\\ &= (0,\ell_{p-1}\ell_0 j)\end{aligned}$$

and if $i \neq 0, p-1$

$$\begin{aligned}\omega|_{B_0}\tau'\omega^{-1}|_{B_0}(i,j) &= \omega|_{B_0}\tau'(i,j)\\ &= \omega|_{B_0}(i+1,\ell_i j)\\ &= (i+1,\ell_i j)\end{aligned}$$

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same).

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$).

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times)

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ',

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1} \ell_i = 1$.

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1} \ell_i = 1$. Thus $\ell_1 = 1$ and $\tau' = \tau$.

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1} \ell_i = 1$. Thus $\ell_1 = 1$ and $\tau' = \tau$. The only way this can occur (and we have seen the computation)

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1} \ell_i = 1$. Thus $\ell_1 = 1$ and $\tau' = \tau$. The only way this can occur (and we have seen the computation) is if $n_0 = n_1 = \ldots = n_{q-1}$

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1} \ell_i = 1$. Thus $\ell_1 = 1$ and $\tau' = \tau$. The only way this can occur (and we have seen the computation) is if $n_0 = n_1 = \ldots = n_{q-1}$ in which case $\delta \in \mathrm{Aut}(\mathbb{Z}_{qp})$.

So we may assume without loss of generality that $\ell_0 = 1$ (but that ℓ_{p-1} has changed and all other ℓ_i are the same). Repeat the above conjugation using block B_{p-1} we will see that we may assume that $\ell_{p-1} = 0$, ℓ_{p-2} has changed and $\ell_0 = 1$ (as long as $q \neq 2$). We repeat this procedure for blocks $B_0, B_{p-1}, \ldots, B_2$ (so in total $p-1$ times) and we may assume that

$$1 = \ell_0 = \ell_{p-1} = \ldots = \ell_2.$$

Now, the conjugations of course do not change the order of τ', and so $\Pi_{i=0}^{q-1}\ell_i = 1$. Thus $\ell_1 = 1$ and $\tau' = \tau$. The only way this can occur (and we have seen the computation) is if $n_0 = n_1 = \ldots = n_{q-1}$ in which case $\delta \in \mathrm{Aut}(\mathbb{Z}_{qp})$. Then Γ is a CI-digraph of $\mathbb{Z}_{qp}$ and the result follows.

What is known

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$,

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well. Then $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G,

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well. Then $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G, so there exists $\alpha \in \mathrm{Aut}(G)$ such that $\mathrm{Cay}(G, S_2) = \alpha(\mathrm{Cay}(G, S_1)) = \mathrm{Cay}(G, \alpha(S_1))$.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well. Then $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G, so there exists $\alpha \in \mathrm{Aut}(G)$ such that $\mathrm{Cay}(G, S_2) = \alpha(\mathrm{Cay}(G, S_1)) = \mathrm{Cay}(G, \alpha(S_1))$. Hence $\alpha(S_1) = S_2$,

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well. Then $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G, so there exists $\alpha \in \mathrm{Aut}(G)$ such that $\mathrm{Cay}(G, S_2) = \alpha(\mathrm{Cay}(G, S_1)) = \mathrm{Cay}(G, \alpha(S_1))$. Hence $\alpha(S_1) = S_2$, and so $H = \langle S_2 \rangle = \alpha(\langle S_1 \rangle) = \alpha(H)$.

What is known

Theorem 61 (Babai and Frankl, 1978 [4])

Let G be a CI-group with respect to (di)graphs and $H \leq G$. Then H is a CI-group with respect to (di)graphs.

Proof.

Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not difficult to show that $\mathrm{Cay}(H, S_1)$ is connected if and only if $\langle S_1 \rangle = H$, and so $\langle S_2 \rangle = H$ as well. Then $\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G, so there exists $\alpha \in \mathrm{Aut}(G)$ such that $\mathrm{Cay}(G, S_2) = \alpha(\mathrm{Cay}(G, S_1)) = \mathrm{Cay}(G, \alpha(S_1))$. Hence $\alpha(S_1) = S_2$, and so $H = \langle S_2 \rangle = \alpha(\langle S_1 \rangle) = \alpha(H)$. The restriction of α to H is then an isomorphism from $\mathrm{Cay}(H, S_1)$ to $\mathrm{Cay}(H, S_2)$. $\square$

Corollary 62

If $\mathbb{Z}_n$ is a CI-group with respect to digraphs then $n = m, 2m$, or $4m$ where m is odd and square-free.

Corollary 62

If $\mathbb{Z}_n$ is a CI-group with respect to digraphs then $n = m, 2m$, or $4m$ where m is odd and square-free.

There exists a construction to show that $\mathbb{Z}_{9n}$ is a CI-group with respect to graphs if and only if $n = 1$ or 2.

Corollary 62

If $\mathbb{Z}_n$ is a CI-group with respect to digraphs then $n = m, 2m$, or $4m$ where m is odd and square-free.

There exists a construction to show that $\mathbb{Z}_{9n}$ is a CI-group with respect to graphs if and only if $n = 1$ or 2.

Corollary 63

If $\mathbb{Z}_n$ is a CI-group with respect to graphs then $n = m, 2m$, or $4m$ or $n = 8, 9$ or 18, where m is odd and square-free.

Corollary 62

If $\mathbb{Z}_n$ is a CI-group with respect to digraphs then $n = m, 2m$, or $4m$ where m is odd and square-free.

There exists a construction to show that $\mathbb{Z}_{9n}$ is a CI-group with respect to graphs if and only if $n = 1$ or 2.

Corollary 63

If $\mathbb{Z}_n$ is a CI-group with respect to graphs then $n = m, 2m$, or $4m$ or $n = 8, 9$ or 18, where m is odd and square-free.

Theorem 64 (Muzychuk 1995 [28], 1997 [29])

$\mathbb{Z}_n$ is a CI-group with respect to (di)graphs if and only if $n = m, 2n, 4m$, and additionally in the case of graphs for $n = 8, 9$ and 18, where m is odd and square-free.

The Solution to the Isomorphism Problem for Circulants

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *circulant digraphs with keys* $\mathbf{k}$ *and* $\mathbf{k}'$*, respectively. Then*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
    - 2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   - 2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*
   - 2.2 *$f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ for some $f_{\vec{m}} \in P(\mathbf{k})$, and*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *circulant digraphs with keys* $\mathbf{k}$ *and* $\mathbf{k}'$*, respectively. Then*

1. *if* $\mathbf{k} \neq \mathbf{k}'$*, then* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is not isomorphic to* $\mathrm{Cay}(\mathbb{Z}_n, S')$*,*
2. *if* $\mathbf{k} = \mathbf{k}'$*, then the following are equivalent:*
    - 2.1 $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *are isomorphic,*
    - 2.2 $f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$*, and*
    - 2.3 $f_{\vec{m}}(S) = S'$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$*.*

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   - 2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*
   - 2.2 *$f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ for some $f_{\vec{m}} \in P(\mathbf{k})$, and*
   - 2.3 *$f_{\vec{m}}(S) = S'$ for some $f_{\vec{m}} \in P(\mathbf{k})$.*

More is known about circulants!

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   - 2.1 $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *are isomorphic,*
   - 2.2 $f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$*, and*
   - 2.3 $f_{\vec{m}}(S) = S'$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$.

More is known about circulants! Evdokimov and Ponomarenko in 2003 [17] solved the recognition problem for circulants

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   - 2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*
   - 2.2 *$f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ for some $f_{\vec{m}} \in P(\mathbf{k})$, and*
   - 2.3 *$f_{\vec{m}}(S) = S'$ for some $f_{\vec{m}} \in P(\mathbf{k})$.*

More is known about circulants! Evdokimov and Ponomarenko in 2003 [17] solved the recognition problem for circulants - that is, given graph they have an algorithm to determine if the graph is isomorphic to a circulant graph.

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*
   2.2 *$f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ for some $f_{\vec{m}} \in P(\mathbf{k})$, and*
   2.3 *$f_{\vec{m}}(S) = S'$ for some $f_{\vec{m}} \in P(\mathbf{k})$.*

More is known about circulants! Evdokimov and Ponomarenko in 2003 [17] solved the recognition problem for circulants - that is, given graph they have an algorithm to determine if the graph is isomorphic to a circulant graph. As consequences, they also solve the isomorphism problem

The Solution to the Isomorphism Problem for Circulants

Theorem 65 (Muzychuk 2004 [27])

Let n be a positive integer, $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ circulant digraphs with keys $\mathbf{k}$ and $\mathbf{k}'$, respectively. Then

1. *if $\mathbf{k} \neq \mathbf{k}'$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is not isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S')$,*
2. *if $\mathbf{k} = \mathbf{k}'$, then the following are equivalent:*
   - 2.1 *$\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic,*
   - 2.2 *$f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S)) = \mathrm{Cay}(\mathbb{Z}_n, S')$ for some $f_{\vec{m}} \in P(\mathbf{k})$, and*
   - 2.3 *$f_{\vec{m}}(S) = S'$ for some $f_{\vec{m}} \in P(\mathbf{k})$.*

More is known about circulants! Evdokimov and Ponomarenko in 2003 [17] solved the recognition problem for circulants - that is, given graph they have an algorithm to determine if the graph is isomorphic to a circulant graph. As consequences, they also solve the isomorphism problem and Ponomarenko [33] gave a polynomial time algorithm to compute the full automorphism group of a circulant.

The following result was proven by Babai and Frankl [4] in the special case where H is a characteristic subgroup of G.

The following result was proven by Babai and Frankl [4] in the special case where H is a characteristic subgroup of G.

Theorem 66 (Dobson and Morris, 2015 [15])

Let G be a CI-group with respect to digraphs and $H \triangleleft G$.

The following result was proven by Babai and Frankl [4] in the special case where H is a characteristic subgroup of G.

Theorem 66 (Dobson and Morris, 2015 [15])

Let G be a CI-group with respect to digraphs and $H \triangleleft G$. Then G/H is a CI-group with respect to digraphs.

The following result was proven by Babai and Frankl [4] in the special case where H is a characteristic subgroup of G.

Theorem 66 (Dobson and Morris, 2015 [15])

Let G be a CI-group with respect to digraphs and $H \triangleleft G$. Then G/H is a CI-group with respect to digraphs.

C.H. Li [22] finished off a result begun but not finished by Babai and Frankl [5]

The following result was proven by Babai and Frankl [4] in the special case where H is a characteristic subgroup of G.

Theorem 66 (Dobson and Morris, 2015 [15])

Let G be a CI-group with respect to digraphs and $H \triangleleft G$. Then G/H is a CI-group with respect to digraphs.

C.H. Li [22] finished off a result begun but not finished by Babai and Frankl [5]

Theorem 67

A CI-group with respect to graphs is solvable.

All Possible CI-groups with respect to graphs

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian.

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian. By $\exp(M)$, we denote the largest order of any element of M.

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian. By $\exp(M)$, we denote the largest order of any element of M. Let $n \in \{2, 3, 4, 8\}$ be relatively prime to $|M|$.

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian. By $\exp(M)$, we denote the largest order of any element of M. Let $n \in \{2,3,4,8\}$ be relatively prime to $|M|$. Set
$E(n,M) = \mathbb{Z}_n \ltimes_\phi M$,

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian. By $\exp(M)$*, we denote the largest order of any element of M. Let $n \in \{2,3,4,8\}$ be relatively prime to $|M|$. Set $E(n,M) = \mathbb{Z}_n \ltimes_\phi M$, where if n is even then $\phi(g) = g^{-1}$, while if $n = 3$ then $\phi(g) = g^\ell$, where ℓ is an integer satisfying $\ell^3 \equiv 1 \pmod{\exp(M)}$ and $\gcd(\ell(\ell-1), \exp(M)) = 1$.*

All Possible CI-groups with respect to graphs

Definition 68

Let M be an abelian group of order m such that every Sylow p-subgroup of M is elementary abelian. By $\exp(M)$*, we denote the largest order of any element of M. Let $n \in \{2, 3, 4, 8\}$ be relatively prime to $|M|$. Set $E(n, M) = \mathbb{Z}_n \ltimes_\phi M$, where if n is even then $\phi(g) = g^{-1}$, while if $n = 3$ then $\phi(g) = g^\ell$, where ℓ is an integer satisfying $\ell^3 \equiv 1 \pmod{\exp(M)}$ and $\gcd(\ell(\ell - 1), \exp(M)) = 1$.*

The next result is a combination of a result of Li, Lu, and Pálfy 2007 [24] and Somlai 2011 [36].

Theorem 69

Let G be a CI-group with respect to graphs.

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*
   1.1 *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*
   1.1 *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*
   1.2 *H_2 is isomorphic to one of the groups $E(2, M)$, $E(4, M)$, Q_8, or 1;*

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*
   - 1.1 *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*
   - 1.2 *H_2 is isomorphic to one of the groups $E(2, M)$, $E(4, M)$, Q_8, or 1;*
   - 1.3 *H_3 is isomorphic to one of the groups $E(3, M)$, A_4 , or 1.*

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*
   1.1 *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*
   1.2 *H_2 is isomorphic to one of the groups $E(2, M)$, $E(4, M)$, Q_8, or 1;*
   1.3 *H_3 is isomorphic to one of the groups $E(3, M)$, A_4 , or 1.*
2. *If G contains elements of order 8, then $G \cong E(8, M)$ or $\mathbb{Z}_8$.*

Theorem 69

Let G be a CI-group with respect to graphs.

1. *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*
   1.1 *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*
   1.2 *H_2 is isomorphic to one of the groups $E(2, M)$, $E(4, M)$, Q_8, or 1;*
   1.3 *H_3 is isomorphic to one of the groups $E(3, M)$, A_4 , or 1.*
2. *If G contains elements of order 8, then $G \cong E(8, M)$ or $\mathbb{Z}_8$.*
3. *If G contains elements of order 9, then G is one of the groups $\mathbb{Z}_2 \ltimes \mathbb{Z}_9$, $\mathbb{Z}_4 \ltimes \mathbb{Z}_9$, $\mathbb{Z}_9 \ltimes \mathbb{Z}_2^2$, or $\mathbb{Z}_2^n \times \mathbb{Z}_9$, with $n \leq 5$.*

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];
- F_{3p} (the Frobenius group of order $3p$) [10, Theorem 21], see also [12] and [24];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];
- F_{3p} (the Frobenius group of order $3p$) [10, Theorem 21], see also [12] and [24];
- D_{6p} Dobson, Morris, and Spiga 2015 [16];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];
- F_{3p} (the Frobenius group of order $3p$) [10, Theorem 21], see also [12] and [24];
- D_{6p} Dobson, Morris, and Spiga 2015 [16];
- $E(4, p)$ and $E(8, p)$ where p is prime Li, Lu, and Pálfy [24];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];
- F_{3p} (the Frobenius group of order $3p$) [10, Theorem 21], see also [12] and [24];
- D_{6p} Dobson, Morris, and Spiga 2015 [16];
- $E(4, p)$ and $E(8, p)$ where p is prime Li, Lu, and Pálfy [24];
- $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ (and $\mathbb{Z}_2^2 \times \mathbb{Z}_p$) Dobson 2010 [13];

Which of these groups are CI-groups with respect to graphs?

- $\mathbb{Z}_n$, where $n \in \{8, 9, 18, k, 2k, 4k\}$ and k is odd and square-free Muzychuk 1995, 1997 [28, 29];
- $\mathbb{Z}_p^2$ [18]; $\mathbb{Z}_p^3$ Dobson 1995 [9]; $\mathbb{Z}_p^4$ Royle [34] for $p = 2$, Hirasaka and Muzychuk 2001 [19] for $p > 2$, and Morris 1999 [25] and [26] independently);
- D_{2p} Babai 1977 [3];
- F_{3p} (the Frobenius group of order $3p$) [10, Theorem 21], see also [12] and [24];
- D_{6p} Dobson, Morris, and Spiga 2015 [16];
- $E(4, p)$ and $E(8, p)$ where p is prime Li, Lu, and Pálfy [24];
- $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ (and $\mathbb{Z}_2^2 \times \mathbb{Z}_p$) Dobson 2010 [13];
- $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ Kovács and Muzychuk 2009 [21];

- $Q_8 \times \mathbb{Z}_p$ Somlai 2015 [37];

- $Q_8 \times \mathbb{Z}_p$ Somlai 2015 [37];
- some specific small groups: Q_{12}, A_4, $\mathbb{Z}_3^2.\mathbb{Z}_2$, $\mathbb{Z}_3.\mathbb{Z}_8$, Q_{28}, $D_{10} \times \mathbb{Z}_3$, $D_6 \times \mathbb{Z}_5$, D_{30}, and all of their subgroups Royle 1987 [34]; $\mathbb{Z}_2^5$ Conder and Li 1998 [7]; and $\mathbb{Z}_3^5$ Spiga 2009 [38];

- $Q_8 \times \mathbb{Z}_p$ Somlai 2015 [37];
- some specific small groups: Q_{12}, A_4, $\mathbb{Z}_3^2.\mathbb{Z}_2$, $\mathbb{Z}_3.\mathbb{Z}_8$, Q_{28}, $D_{10} \times \mathbb{Z}_3$, $D_6 \times \mathbb{Z}_5$, D_{30}, and all of their subgroups Royle 1987 [34]; $\mathbb{Z}_2^5$ Conder and Li 1998 [7]; and $\mathbb{Z}_3^5$ Spiga 2009 [38]; and
- D_{2n}, $\mathbb{Z}_n \rtimes \mathbb{Z}_3$, $\mathbb{Z}_p^2 \times \mathbb{Z}_n$ Dobson 2002 [12], and $\mathbb{Z}_p^2 \times \mathbb{Z}_q \times \mathbb{Z}_n$ Dobson 2014 [14], where n satisfies $\gcd(n, \varphi(n)) = 1$ (φ is Euler's phi function) and in the first three cases other additional arithmetic conditions.

- $Q_8 \times \mathbb{Z}_p$ Somlai 2015 [37];
- some specific small groups: Q_{12}, A_4, $\mathbb{Z}_3^2.\mathbb{Z}_2$, $\mathbb{Z}_3.\mathbb{Z}_8$, Q_{28}, $D_{10} \times \mathbb{Z}_3$, $D_6 \times \mathbb{Z}_5$, D_{30}, and all of their subgroups Royle 1987 [34]; $\mathbb{Z}_2^5$ Conder and Li 1998 [7]; and $\mathbb{Z}_3^5$ Spiga 2009 [38]; and
- D_{2n}, $\mathbb{Z}_n \rtimes \mathbb{Z}_3$, $\mathbb{Z}_p^2 \times \mathbb{Z}_n$ Dobson 2002 [12], and $\mathbb{Z}_p^2 \times \mathbb{Z}_q \times \mathbb{Z}_n$ Dobson 2014 [14], where n satisfies $\gcd(n, \varphi(n)) = 1$ (φ is Euler's phi function) and in the first three cases other additional arithmetic conditions.

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ *or* n *where* $\gcd(n, \varphi(n)) = 1$*, where* φ *is Euler's phi function.*

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$.

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{p_i}^{a_i}$, $1 \le i \le r$.

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{p_i}^{a_i}$, $1 \le i \le r$.

The following result follows from results in [14] and [30]:

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{p_i}^{a_i}$, $1 \le i \le r$.

The following result follows from results in [14] and [30]:

Theorem 72

Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$.

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{p_i}^{a_i}$, $1 \le i \le r$.

The following result follows from results in [14] and [30]:

Theorem 72

Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$. Let $n = n_1 \ldots n_r$.

The isomorphism problem for all combinatorial objects

Theorem 70 (Pálfy, 1987 [32])

G is a CI-group if and only if $|G| = 4$ or n where $\gcd(n, \varphi(n)) = 1$, where φ is Euler's phi function.

Theorem 71 (Muzychuk, 1999 [30])

Let $m = p_1 \cdots p_r$ where each p_i is prime and $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{p_i}^{a_i}$, $1 \leq i \leq r$.

The following result follows from results in [14] and [30]:

Theorem 72

Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$. Let $n = n_1 \ldots n_r$. Then the Cayley isomorphism problem for circulant combinatorial objects reduces to that of $\mathbb{Z}_{n_i}$, $1 \leq i \leq r$.

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ *where each* p_i *is prime,* $\gcd(m, \varphi(m)) = 1$*, and* $n = p_1^{a_1} \cdots p_r^{a_r}$*.*

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ *where each* p_i *is prime,* $\gcd(m, \varphi(m)) = 1$*, and* $n = p_1^{a_1} \cdots p_r^{a_r}$*. Then the isomorphism problem for combinatorial objects of a nilpotent group* G *reduces to that of its Sylow subgroups provided that*

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ *where each* p_i *is prime,* $\gcd(m, \varphi(m)) = 1$*, and* $n = p_1^{a_1} \cdots p_r^{a_r}$*. Then the isomorphism problem for combinatorial objects of a nilpotent group* G *reduces to that of its Sylow subgroups provided that whenever* $\delta \in S_G$ *there exists* $\phi \in \langle G_L, \phi^{-1} G_L \phi \rangle$ *such that such that* $\langle G_L, \phi^{-1}\delta^{-1} G_L \phi\delta \rangle$ *is m-step imprimitive.*

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ *where each* p_i *is prime,* $\gcd(m, \varphi(m)) = 1$*, and* $n = p_1^{a_1} \cdots p_r^{a_r}$*. Then the isomorphism problem for combinatorial objects of a nilpotent group* G *reduces to that of its Sylow subgroups provided that whenever* $\delta \in S_G$ *there exists* $\phi \in \langle G_L, \phi^{-1} G_L \phi \rangle$ *such that such that* $\langle G_L, \phi^{-1}\delta^{-1} G_L \phi\delta \rangle$ *is m-step imprimitive.*

Problem 74

Let $H_1, \ldots, H_r$ *be groups and* $G = H_1 \times H_2 \times \cdots \times H_r$*.*

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ *where each* p_i *is prime,* $\gcd(m, \varphi(m)) = 1$*, and* $n = p_1^{a_1} \cdots p_r^{a_r}$*. Then the isomorphism problem for combinatorial objects of a nilpotent group* G *reduces to that of its Sylow subgroups provided that whenever* $\delta \in S_G$ *there exists* $\phi \in \langle G_L, \phi^{-1} G_L \phi \rangle$ *such that such that* $\langle G_L, \phi^{-1}\delta^{-1} G_L \phi\delta \rangle$ *is m-step imprimitive.*

Problem 74

Let $H_1, \ldots, H_r$ *be groups and* $G = H_1 \times H_2 \times \cdots \times H_r$*. Determine necessary and sufficient conditions for the Cayley isomorphism problem of* G *in every class of combinatorial objects to reduce to the Cayley isomorphism problem for Cayley objects of* H_i*,* $1 \leq i \leq r$*.*

Theorem 73 (Dobson 2014 [14])

Let $m = p_1 \cdots p_r$ where each p_i is prime, $\gcd(m, \varphi(m)) = 1$, and $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the isomorphism problem for combinatorial objects of a nilpotent group G reduces to that of its Sylow subgroups provided that whenever $\delta \in S_G$ there exists $\phi \in \langle G_L, \phi^{-1} G_L \phi \rangle$ such that such that $\langle G_L, \phi^{-1}\delta^{-1} G_L \phi\delta \rangle$ is m-step imprimitive.

Problem 74

Let $H_1, \ldots, H_r$ be groups and $G = H_1 \times H_2 \times \cdots \times H_r$. Determine necessary and sufficient conditions for the Cayley isomorphism problem of G in every class of combinatorial objects to reduce to the Cayley isomorphism problem for Cayley objects of H_i, $1 \le i \le r$.

Conjecture 75 (Folklore)

If G and H are CI-groups with respect to digraphs of relatively prime order then $G \times H$ is a CI-group with respect to digraphs.

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs!

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs! Pálfy's Theorem was crucial in the proof of :

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs! Pálfy's Theorem was crucial in the proof of :

Theorem 76 (Dobson 2000 [11])

Let n be a positive integer such that $\gcd(n, \varphi(n)) = 1$.

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs! Pálfy's Theorem was crucial in the proof of :

Theorem 76 (Dobson 2000 [11])

Let n be a positive integer such that $\gcd(n, \varphi(n)) = 1$. A vertex-transitive digraph Γ of order n is isomorphic to a circulant digraph of order n if and only if $\mathrm{Aut}(\Gamma)$ contains a transitive solvable subgroup.

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs! Pálfy's Theorem was crucial in the proof of :

Theorem 76 (Dobson 2000 [11])

Let n be a positive integer such that $\gcd(n, \varphi(n)) = 1$. A vertex-transitive digraph Γ of order n is isomorphic to a circulant digraph of order n if and only if $\mathrm{Aut}(\Gamma)$ contains a transitive solvable subgroup.

We remark that there is a unique group (necessarily cyclic) of order n if and only $\gcd(n, \varphi(n)) = 1$.

This most abstract of the Cayley isomorphism problems is also useful in the classification of vertex-transitive graphs! Pálfy's Theorem was crucial in the proof of :

Theorem 76 (Dobson 2000 [11])

Let n be a positive integer such that $\gcd(n, \varphi(n)) = 1$. A vertex-transitive digraph Γ of order n is isomorphic to a circulant digraph of order n if and only if $\mathrm{Aut}(\Gamma)$ contains a transitive solvable subgroup.

We remark that there is a unique group (necessarily cyclic) of order n if and only $\gcd(n, \varphi(n)) = 1$.

Very little is known about the Cayley isomorphism problem for groups that are not cyclic and are not CI-groups with respect to graphs or digraphs!

Very little is known about the Cayley isomorphism problem for groups that are not cyclic and are not CI-groups with respect to graphs or digraphs! Even less is known about the isomorphism problem for vertex-transitive digraphs that are not Cayley digraphs!

Very little is known about the Cayley isomorphism problem for groups that are not cyclic and are not CI-groups with respect to graphs or digraphs! Even less is known about the isomorphism problem for vertex-transitive digraphs that are not Cayley digraphs! There should be some problems in this area that are quite doable.

Very little is known about the Cayley isomorphism problem for groups that are not cyclic and are not CI-groups with respect to graphs or digraphs! Even less is known about the isomorphism problem for vertex-transitive digraphs that are not Cayley digraphs! There should be some problems in this area that are quite doable. Also, corresponding problems for other classes of combinatorial objects.

Very little is known about the Cayley isomorphism problem for groups that are not cyclic and are not CI-groups with respect to graphs or digraphs! Even less is known about the isomorphism problem for vertex-transitive digraphs that are not Cayley digraphs! There should be some problems in this area that are quite doable. Also, corresponding problems for other classes of combinatorial objects. There should be some quite doable problems here for students/young researchers who are not experts in the area!

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes.

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

1. *Classify the digraphs in terms of a minimal transitive subgroup of their automorphism group.*

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

1. *Classify the digraphs in terms of a minimal transitive subgroup of their automorphism group.*
2. *Solve the isomorphism problem for each minimal transitive subgroup.*

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

1. *Classify the digraphs in terms of a minimal transitive subgroup of their automorphism group.*
2. *Solve the isomorphism problem for each minimal transitive subgroup.*
3. *Determine necessary and sufficient conditions for various digraphs to have different minimal transitive subgroups and to determine what they all are.*

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

1. *Classify the digraphs in terms of a minimal transitive subgroup of their automorphism group.*
2. *Solve the isomorphism problem for each minimal transitive subgroup.*
3. *Determine necessary and sufficient conditions for various digraphs to have different minimal transitive subgroups and to determine what they all are.*
4. *Calculate all automorphism groups.*

Problem 77

Encyclopedic knowledge of vertex-transitive digraphs of order a product of at most three (not necessarily distinct) primes. This includes:

1. *Classify the digraphs in terms of a minimal transitive subgroup of their automorphism group.*
2. *Solve the isomorphism problem for each minimal transitive subgroup.*
3. *Determine necessary and sufficient conditions for various digraphs to have different minimal transitive subgroups and to determine what they all are.*
4. *Calculate all automorphism groups.*

More information about the Cayley isomorphism problem can be found in the still somewhat recent survey of C.H. Li [23].

Thanks!

[1] A. Ádám, *Research problem 2-10*, J. Combin. Theory **2** (1967), 393.

[2] Brian Alspach and T. D. Parsons, *Isomorphism of circulant graphs and digraphs*, Discrete Math. **25** (1979), no. 2, 97–108. MR MR523083 (80e:05064)

[3] L. Babai, *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Acad. Sci. Hungar. **29** (1977), no. 3-4, 329–336. MR MR0485447 (58 #5281)

[4] L. Babai and P. Frankl, *Isomorphisms of Cayley graphs. I*, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I, Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam, 1978, pp. 35–52. MR 519254 (81g:05066a)

[5] ______, *Isomorphisms of Cayley graphs. II*, Acta Math. Acad. Sci. Hungar. **34** (1979), no. 1-2, 177–183. MR 546732 (81g:05066b)

[6] W. Burnside, *On some properties of groups of odd order*, J. London Math. Soc. **33** (1901), 162–185.

[7] Marston Conder and Cai Heng Li, *On isomorphisms of finite Cayley graphs*, European J. Combin. **19** (1998), no. 8, 911–919. MR MR1657923 (99i:05096)

[8] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996. MR MR1409812 (98m:20003)

[9] Edward Dobson, *Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$*, Discrete Math. **147** (1995), no. 1-3, 87–94. MR MR1364506 (96m:05101)

[10] ______, *Isomorphism problem for metacirculant graphs of order a product of distinct primes*, Canad. J. Math. **50** (1998), no. 6, 1176–1188. MR MR1657775 (99k:05119)

[11] ———, *On solvable groups and circulant graphs*, European J. Combin. **21** (2000), no. 7, 881–885. MR MR1787902 (2001j:05065)

[12] ———, *On the Cayley isomorphism problem*, Discrete Math. **247** (2002), no. 1-3, 107–116. MR MR1893021 (2003c:05106)

[13] ———, *Asymptotic automorphism groups of Cayley digraphs and graphs of abelian groups of prime-power order*, Ars Math. Contemp. **3** (2010), no. 2, 200–213. MR 2739429

[14] ———, *On the Cayley isomorphism problem for Cayley objects of nilpotent groups of some orders*, Electron. J. Combin. **21** (2014), no. 3, Paper 3.8, 15. MR 3262245

[15] Edward Dobson and Aleksander Malnič, *Groups that are transitive on all partitions of a given shape*, J. Algebraic Combin. **42** (2015), no. 2, 605–617. MR 3369569

[16] Edward Dobson, Joy Morris, and Pablo Spiga, *Further restrictions on the structure of finite DCI-groups: an addendum*, J. Algebraic Combin. **42** (2015), no. 4, 959–969. MR 3417254

[17] S. A. Evdokimov and I. N. Ponomarenko, *Recognition and verification of an isomorphism of circulant graphs in polynomial time*, Algebra i Analiz **15** (2003), no. 6, 1–34. MR MR2044629 (2005g:68053)

[18] C. D. Godsil, *On Cayley graph isomorphisms*, Ars Combin. **15** (1983), 231–246. MR MR706302 (84m:20011)

[19] M. Hirasaka and M. Muzychuk, *An elementary abelian group of rank 4 is a CI-group*, J. Combin. Theory Ser. A **94** (2001), no. 2, 339–362. MR MR1825792 (2002a:20003)

[20] M. H. Klin and R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), Colloq. Math.

Soc. János Bolyai, vol. 25, North-Holland, Amsterdam, 1981, pp. 405–434. MR MR642055 (83h:05047)

[21] I. Kovács and M. Muzychuk, *The group $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ is a CI-group*, Comm. Algebra **37** (2009), no. 10, 3500–3515. MR 2561859 (2011b:05102)

[22] Cai Heng Li, *Finite CI-groups are soluble*, Bull. London Math. Soc. **31** (1999), no. 4, 419–423. MR 1687493 (2000d:05056)

[23] ______, *On isomorphisms of finite Cayley graphs—a survey*, Discrete Math. **256** (2002), no. 1-2, 301–334. MR MR1927074 (2003i:05067)

[24] Cai Heng Li, Zai Ping Lu, and P. P. Pálfy, *Further restrictions on the structure of finite CI-groups*, J. Algebraic Combin. **26** (2007), no. 2, 161–181. MR 2335710 (2008g:20048)

[25] Joy Morris, *Isomorphisms of cayley graphs*, Ph.D. thesis, Simon Fraser University, 1999.

[26] ———, *Elementary proof that $\mathbb{Z}_p^4$ is a DCI-group*, Discrete Math. **338** (2015), no. 8, 1385–1393. MR 3336107

[27] M. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc. (3) **88** (2004), no. 1, 1–41. MR MR2018956 (2004h:05084)

[28] Mikhail Muzychuk, *Ádám's conjecture is true in the square-free case*, J. Combin. Theory Ser. A **72** (1995), no. 1, 118–134. MR MR1354970 (96m:05141)

[29] ———, *On Ádám's conjecture for circulant graphs*, Discrete Math. **176** (1997), no. 1-3, 285–298. MR MR1477298 (98h:05141b)

[30] ———, *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198** (1999), 589–606, 16th British Combinatorial Conference (London, 1997). MR MR1674890 (2000e:05165)

[31] Oystein Ore, *Theory of graphs*, American Mathematical Society Colloquium Publications, Vol. XXXVIII, American Mathematical Society, Providence, R.I., 1962. MR 0150753 (27 #740)

[32] P. P. Pálfy, *Isomorphism problem for relational structures with a cyclic automorphism*, European J. Combin. **8** (1987), no. 1, 35–43. MR MR884062 (88i:05097)

[33] I. N. Ponomarenko, *Determination of the automorphism group of a circulant association scheme in polynomial time*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **321** (2005), no. Vopr. Teor. Predst. Algebr. i Grupp. 12, 251–267, 301. MR MR2138422 (2005m:05241)

[34] Gordan Royle, *Constructive enumeration of graphs*, Ph.D. thesis, University of Western Australia, 1987.

[35] Gert Sabidussi, *On a class of fixed-point-free graphs*, Proc. Amer. Math. Soc. **9** (1958), 800–804. MR MR0097068 (20 #3548)

[36] Gábor Somlai, *Elementary abelian p-groups of rank $2p+3$ are not CI-groups*, J. Algebraic Combin. **34** (2011), no. 3, 323–335. MR 2836364

[37] ______, *The Cayley isomorphism property for groups of order $8p$*, Ars Math. Contemp. **8** (2015), no. 2, 433–444. MR 3448605

[38] Pablo Spiga, *Ci-property of elementary abelian 3-groups*, Discrete Math. **309** (2009), 3393–3398.

[39] James Turner, *Point-symmetric graphs with a prime number of points*, J. Combinatorial Theory **3** (1967), 136–145. MR MR0211908 (35 #2783)