# 4 Types of Subgroups

10/24: 1. Let $H$ and $K$ be normal subgroups of $G$ such that $H \cap K$ is trivial. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. (Exercise 3.1.42 of Dummit and Foote (2004).)

*Proof.* Let $x \in H$ and $y \in K$ be arbitrary.

Since $H$ is normal, $gxg^{-1} \in H$ for all $g \in G$. Choosing $g = y^{-1}$ reveals that $y^{-1}xy \in H$. Additionally, we know since $H$ is a subgroup that $x^{-1} \in H$. It similarly follows that $x^{-1}y^{-1}xy \in H$.

Similarly, $x^{-1}y^{-1}x \in K$ and $y \in K$ imply that $x^{-1}y^{-1}xy \in K$.

Having proven that $x^{-1}y^{-1}xy \in H$ and $x^{-1}y^{-1}xy \in K$, we know that $x^{-1}y^{-1}xy \in H \cap K = \{e\}$. Therefore,

$$\begin{aligned} x^{-1}y^{-1}xy &= e \\ xy &= yx \end{aligned}$$

as desired. ☐

2. Show that $S_4$ does not have a normal subgroup of order 3 or order 8.

*Proof.* Suppose for the sake of contradiction that $N$ be a normal subgroup of order 3 or 8. We know that $N$ is a subgroup; thus, $e \in N$. We also know that $N$ is a union of conjugacy classes. Thus, if we include any other cycle of a given shape in $N$, we know that all cycles of that shape are elements of $N$. Since there are 5 cycles of shape $(xx)$, 8 cycles of shape $(xxx)$, 6 cycles of shape $(xxxx)$, and 3 cycles of shape $(xx)(xx)$, and 1 plus the sum of any combination of these numbers does not equal 3 or 8, we have arrived at a contradiction. ☐

3. If $H$ is a subgroup of $G$, define the **normalizer** of $H$ to be

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

(a) Prove that $N_G(H) = G$ if and only if $H$ is normal.

*Proof.* Suppose first that $N_G(H) = G$. Then $gHg^{-1} = H$ for all $g \in G$. It follows that $ghg^{-1} \in H$ for all $h \in H$ and $g \in G$. Therefore, by the definition of normality, $H$ is normal, as desired.

Now suppose that $H$ is normal. Then $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. Additionally, if $h' \in H$, then $h = g^{-1}h'g \in H$ by hypothesis, so $h' = ghg^{-1} \in gHg^{-1}$. It follows by the definition of set equality that $gHg^{-1} = H$ for all $g \in G$. But by the definition of $N_G(H)$, this means that $N_G(H) = G$, as desired. ☐

(b) Prove that $N_G(H)$ contains $H$.

*Proof.* Let $h \in H$ be arbitrary. To prove that $h \in N_G(H)$, it will suffice to show that $hHh^{-1} = H$. We will do this with a bidirectional inclusion argument. Suppose first that $hh'h^{-1} \in hHh^{-1}$. Then since $h, h' \in H$ by hypothesis and $H$ is a subgroup (i.e., is closed under multiplication), we have that $hh'h^{-1} \in H$, as desired. Now let $h'' \in H$. Then choosing $h' = h^{-1}h''h \in H$, we have that $h'' = hh'h^{-1} \in hHh^{-1}$, as desired. ☐

(c) Prove that $H$ is a **normal** subgroup of $N_G(H)$.

*Proof.* $H$ is a clearly a subgroup of $N_G(H)$: $H$ is a subset of $N_G(H)$ by part (b) and $H$ is nonempty, closed under multiplication, closed under inverses, and associative as a subgroup of $G$. All that remains now is to prove that $H$ is normal.

To prove that $H \triangleleft N_G(H)$, it will suffice to show that for all $g \in N_G(H)$, $gHg^{-1} \subset H$. But we have this by the definition of $N_G(H)$, as desired. ☐

(d) Compute $N_G(H)$ for the following pairs $(G, H)$.

i. $(S_4, \langle(1,2,3,4)\rangle)$.

*Proof.* We will first prove a lemma.

Lemma: Let $H = \langle x\rangle = \langle y\rangle$ be a subgroup of $G$. If $gxg^{-1} = y$, then $gHg^{-1} = H$.
Proof: We proceed via a bidirectional inclusion argument. Suppose first that $ghg^{-1} \in gHg^{-1}$. Since $h \in H$ by hypothesis, $h = x^n$ for some $n \in \mathbb{N}$. Therefore, since $gxg^{-1} = y \in H$ and by the closure of $H$, $ghg^{-1} = gx^ng^{-1} = (gxg^{-1})^n \in H$, as desired. Now suppose that $h' \in H$. Then $h' = y^n = gx^ng^{-1} \in gHg^{-1}$, as desired. Q.E.D.

Let $x = (1,2,3,4)$. We know that

$$gxg^{-1} = (g(1), g(2), g(3), g(4))$$

There are two 4-cycles in $H$, each of which can be written in four ways:

$$\begin{array}{cc} (1,2,3,4) & (1,4,3,2) \\ (2,3,4,1) & (2,1,4,3) \\ (3,4,1,2) & (3,2,1,4) \\ (4,1,2,3) & (4,3,2,1) \end{array}$$

Thus, the values of $g$ that make $gxg^{-1}$ equal to one of the above are

$$\begin{array}{rr} e & (2,4) \\ (1,2,3,4) & (1,2)(3,4) \\ (1,3)(2,4) & (1,3) \\ (1,4,3,2) & (1,4)(2,3) \end{array}$$

Letting $y = (4,3,2,1)$, we have $H = \langle x\rangle = \langle y\rangle$ and $gxg^{-1} \in \{x, y\}$ for all of the above $g$ and our chosen $x$. Thus, by the lemma, $gHg^{-1} = H$ for all of the above $g$. It follows that they are all elements of $N_G(H)$.
Moreover, any value of $g$ that would make $g(1,3)(2,4)g^{-1}$ equal to some other value of $H$ has already been included in the above list, so we have no additional cases to check from there. Of course, all $g \in G$ satisfy $geg^{-1} \in H$, the $g$ there that have not already been mentioned would take $gxg^{-1}$ outside of $H$.
Therefore,

$$\boxed{N_G(H) = \{e, (2,4), (1,2,3,4), (1,2)(3,4), (1,3)(2,4), (1,3), (1,4,3,2), (1,4)(2,3)\}}$$

□

ii. $(S_5, \langle(1,2,3,4,5)\rangle)$.

*Proof.* Let $x = (1,2,3,4,5)$. As before, we know that

$$gxg^{-1} = (g(1), g(2), g(3), g(4), g(5))$$

There are four 5-cycles in $H$, each of which can be written in five ways:

$$\begin{array}{cccc} (1,2,3,4,5) & (1,3,5,2,4) & (1,4,2,5,3) & (1,5,4,3,2) \\ (2,3,4,5,1) & (2,4,1,3,5) & (2,5,3,1,4) & (2,1,5,4,3) \\ (3,4,5,1,2) & (3,5,2,4,1) & (3,1,4,2,5) & (3,2,1,5,4) \\ (4,5,1,2,3) & (4,1,3,5,2) & (4,2,5,3,1) & (4,3,2,1,5) \\ (5,1,2,3,4) & (5,2,4,1,3) & (5,3,1,4,2) & (5,4,3,2,1) \end{array}$$

Thus, the values of $g$ that make $gxg^{-1}$ equal to one of the following are

$$\begin{array}{cccc} e & (2,3,5,4) & (2,4,5,3) & (2,5)(3,4) \\ (1,2,3,4,5) & (1,2,4,3) & (1,2,5,4) & (1,2)(3,5) \\ (1,3,5,2,4) & (1,3,2,5) & (1,3,4,2) & (1,3)(4,5) \\ (1,4,2,5,3) & (1,4,5,2) & (1,4,3,5) & (1,4)(2,3) \\ (1,5,4,3,2) & (1,5,3,4) & (1,5,2,3) & (1,5)(2,4) \end{array}$$

Since each of the four 5-cycles generates $H$, we have by the lemma to part (d)i that $gHg^{-1}$ for all of the above $g$. It follows that they are all elements of $N_G(H)$. Therefore,

$$\boxed{\begin{aligned} N_G(H) = \{e, &(2,3,5,4), (2,4,5,3), (2,5)(3,4), \\ &(1,2,3,4,5), (1,2,4,3), (1,2,5,4), (1,2)(3,5) \\ &(1,3,5,2,4), (1,3,2,5), (1,3,4,2), (1,3)(4,5) \\ &(1,4,2,5,3), (1,4,5,2), (1,4,3,5), (1,4)(2,3) \\ &(1,5,4,3,2), (1,5,3,4), (1,5,2,3), (1,5)(2,4)\} \end{aligned}}$$

$\square$

4. Prove that the subgroup $N$ generated by elements of the form $x^{-1}y^{-1}xy$ for all $x, y \in G$ is normal. (Exercise 3.1.41 of Dummit and Foote (2004).)

*Proof.* To prove that $N$ is normal, it will suffice to show that for all $z \in N$ and $g \in G$, $gzg^{-1} \in N$. Let $x^{-1}y^{-1}xy \in N$ and $g \in G$ be arbitrary. Then

$$\begin{aligned} gx^{-1}y^{-1}xyg^{-1} &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\ &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &\in N \end{aligned}$$

as desired. $\square$

5. Prove that if $G/Z(G)$ is cyclic, then $G$ is abelian. (For a hint, see Exercise 3.1.36 of Dummit and Foote (2004).)

*Proof.* We first prove the hint. Let $G/Z(G) = \langle xZ(G) \rangle$ and let $\sigma \in G$ be arbitrary. Then $\sigma \in [xZ(G)]^a$ for some $a \in \mathbb{Z}$. It follows by the rules of coset multiplication that $\sigma \in x^a Z(G)$. Therefore, $\sigma = x^a z$ for some $a \in \mathbb{Z}$ and $z \in Z(G)$, as desired.

To prove that $G$ is abelian, it will suffice to show that for all $\sigma, \tau \in G$, $\sigma\tau = \tau\sigma$. Let $\sigma, \tau \in G$ be arbitrary. Let $\sigma = x^a z$ and $\tau = x^b z'$. Then since elements of $Z(G)$ — such as $z, z'$ — commute with any $g \in G$ and exponents commute with each other, we have that

$$\sigma\tau = x^a z x^b z' = z x^a x^b z' = z x^b x^a z' = x^b z' x^a z = \tau\sigma$$

as desired. $\square$

6. Let $G$ be a finite group, and let $H \subset G$ be a subgroup of index two — i.e., $|G|/|H| = 2$. Prove that $H$ is normal.

*Proof.* To prove that $H$ is normal, it will suffice to show that $gH = Hg$ for all $g \in G$. Let $g \in G$ be arbitrary. We divide into two cases ($g \in H$ and $g \notin H$).

Suppose first that $g \in H$. Let $gh \in gH$ be arbitrary. Then by closure under multiplication, $gh \in H$. Choosing $h' = ghg^{-1} \in H$, it follows that $gh = h'g \in Hg$, as desired. The proof that $gH \supset Hg$ is analogous.

Now suppose that $g \notin H$. Since $[G : H] = 2$, $G$ can be partitioned into the disjoint union of $H$ and the coset $gH$ or, symmetrically, $H$ and the coset $Hg$. It follows that

$$gH = G \setminus H = Hg$$

as desired. ☐

7. Let $G$ be a finite group, and let $H \subset G$ be a subgroup of index three — i.e., $|G|/|H| = 3$. Show that $H$ is not necessarily normal.

*Proof.* Let $G = S_3$, $H = \langle(1,2)\rangle$, $h = (1,2)$, and $g = (1,3)$. Since $|G| = 6$ and $|H| = 2$, $[G : H] = 6/2 = 3$. Additionally, $ghg^{-1} = (2,3) \notin H$, so $H$ is not normal, as desired. ☐

8. **Automorphism Groups**. Define an automorphism of a group $G$ to be an isomorphism $\phi : G \to G$ from $G$ to itself. (See §4.4 of Dummit and Foote (2004).)

(a) Prove that the identity map is an automorphism.

*Proof.* To prove that the identity map $\iota$ on an arbitrary group $G$ is an automorphism, it will suffice to show that $\iota$ is a homomorphism, injective, surjective, and sends $G \mapsto G$.
Homomorphism:

$$\iota(xy) = xy = \iota(x)\iota(y)$$

Injective:

$$\iota(x) = \iota(x') \iff x = x'$$

Surjective: If $x \in G$, $\iota(x) = x$.
Naturally, $\iota : G \to G$. ☐

(b) Prove that the composition of two automorphisms is an automorphism.

*Proof.* Suppose $\phi, \psi$ are automorphisms on a group $G$; we seek to prove that $\phi \circ \psi$ is an automorphism. To do so, it will suffice to show that $\phi \circ \psi$ is a homomorphism, injective, surjective, and sends $G \to G$.
Homorphism:

$$[\phi \circ \psi](xy) = \phi(\psi(xy)) = \phi(\psi(x)\psi(y)) = \phi(\psi(x))\phi(\psi(y)) = [\phi \circ \psi](x) \cdot [\phi \circ \psi](y)$$

Injective:

$$\begin{aligned} [\phi \circ \psi](x) &= [\phi \circ \psi](x') \\ \phi(\psi(x)) &= \phi(\psi(x')) \\ \psi(x) &= \psi(x') \\ x &= x' \end{aligned}$$

Surjective: If $z \in G$, then the surjectivity of $\phi$ implies that there exists $y \in G$ such that $\phi(y) = x$. Similarly, there exists $x \in G$ such that $\psi(x) = y$. It follows that

$$z = \phi(\psi(x)) = [\phi \circ \psi](x)$$

$\psi(G) = G$ and $\phi(G) = G$, so

$$[\phi \circ \psi](G) = \phi(\psi(G)) = \phi(G) = G$$

as desired. ☐

(c) Prove that the set of automorphisms forms a group under composition. We will call this group $\mathrm{Aut}(G)$.

*Proof.* To prove that $\mathrm{Aut}(G)$ is a group, it will suffice to show that $\mathrm{Aut}(G)$ contains an identity element, is closed under inverses, and is associative.
Identity: Per part (a), we may choose $\iota$ to be the identity element of $\mathrm{Aut}(G)$. Indeed, if $\phi \in \mathrm{Aut}(G)$ and $g \in G$ are arbitrary, then

$$[\phi \circ \iota](g) = \phi(\iota(g)) = \phi(g) = \iota(\phi(g)) = [\iota \circ \phi](g)$$

Inverses: Since $\phi$ is a bijection, $\phi^{-1} : G \to G$ is a well-defined automorphism in its own right. We can prove in an analogous manner to the above that $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = e$.
Associativity: Let $f, g, h \in \mathrm{Aut}(G)$ and $x \in G$ be arbitrary. Then

$$[(f \circ g) \circ h](x) = [f \circ g](h(x)) = f(g(h(x))) = f([g \circ h](x)) = [f \circ (g \circ h)](x)$$

$\square$

(d) If $g \in G$ is a fixed element, prove that the map $\phi_g : G \to G$ given by $\phi_g(x) = gxg^{-1}$ is an isomorphism.

*Proof.* To prove that $\phi_g$ is an isomorphism, it will suffice to show that it is a homomorphism, injective, and surjective.
Homomorphism:

$$\phi_g(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \phi_g(x)\phi_g(y)$$

Injective:

$$\begin{aligned} \phi_g(x) &= \phi_g(x') \\ gxg^{-1} &= gx'g^{-1} \\ x &= x' && \text{Cancellation Lemma} \end{aligned}$$

Surjective: Let $y \in G$ be arbitrary. Choose $x = g^{-1}yg$. Then

$$y = (gg^{-1})y(gg^{-1}) = g(g^{-1}yg)g^{-1} = gxg^{-1} = \phi_g(x)$$

$\square$

(e) Prove that the map $\psi : G \to \mathrm{Aut}(G)$ given by $\psi(g) = \phi_g$ (sending the element $g$ to the automorphism $\phi_g$) is a homomorphism of groups.

*Proof.* Let $x, y, g \in G$ be arbitrary. Then we have that

$$[\psi(xy)](g) = \phi_{xy}(g) = (xy)g(xy)^{-1} = xygy^{-1}x^{-1} = x\phi_y(g)x^{-1} = \phi_x(\phi_y(g)) = [\phi_x \circ \phi_y](g)$$

as desired. $\square$

(f) Prove that the kernel of the map $\psi : G \to \mathrm{Aut}(G)$ is the center

$$Z(G) = \{g \in G \mid gx = xg,\ \forall x \in G\}$$

*Proof.* To prove that $\ker \psi = Z(G)$, we will use a bidirectional inclusion argument.
Suppose first that $g \in \ker \psi$. Then $\iota = \psi(g) = \phi_g$. It follows that $gxg^{-1} = \phi_g(x) = \iota(x) = x$ for all $x \in X$, but this directly implies that $gx = xg$ for all $x \in G$.
The proof is symmetric in the reverse direction. $\square$

(g) Define the inner automorphism group $\mathrm{Inn}(G)$ of $G$ to be the subgroup of $\mathrm{Aut}(G)$ given by the image of $G$ under $\psi$. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

*Proof.* We have from the lemma in class that $\mathrm{Inn}(G) = \operatorname{im}\psi$ is a subgroup of $\mathrm{Aut}(G)$ since $\psi$ is a homomorphism.

To prove that $\mathrm{Inn}(G)$ is normal, it will suffice to show that if $\phi_g = \psi(g) \in \mathrm{Inn}(G)$ and $\varphi \in \mathrm{Aut}(G)$, then $\varphi\phi_g\varphi^{-1} \in \mathrm{Inn}(G)$. Let $\phi_g \in \mathrm{Inn}(G)$, $\varphi \in \mathrm{Aut}(G)$, and $x \in G$ be arbitrary. Then we have that

$$\begin{aligned}
[\varphi\phi_g\varphi^{-1}](x) &= \varphi(\phi_g(\varphi^{-1}(x))) \\
&= \varphi(g\varphi^{-1}(x)g^{-1}) \\
&= \varphi(g)\varphi(\varphi^{-1}(x))\varphi(g^{-1}) \\
&= \varphi(g)x\varphi(g)^{-1} \\
&= \phi_{\varphi(g)}(x) \\
&\in \mathrm{Inn}(G)
\end{aligned}$$

as desired. □

(h) Show that if $G$ is abelian, then $\mathrm{Inn}(G)$ is trivial.

*Proof.* Suppose $G$ is abelian. Then $gx = xg$ for all $g, x \in G$. It follows that $Z(G) = G$. Thus, by part (f), $\ker\phi = Z(G) = G$, meaning that $\mathrm{Inn}(G) = \operatorname{im}\psi = \{\iota\}$, as desired. □

(i) Let $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$. Prove that...

i. $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \mathrm{Out}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$;

*Proof.* $\mathbb{Z}/3\mathbb{Z}$ is abelian. Thus, by part (h), $\mathrm{Inn}(\mathbb{Z}/3\mathbb{Z})$ is trivial. It follows that $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) = \mathrm{Out}(\mathbb{Z}/3\mathbb{Z})$ as desired.

Constructing $\psi$: Let $\psi : \mathrm{Aut}(G) \to \mathbb{Z}/2\mathbb{Z}$ be the isomorphism we seek to construct. First notice that since $\mathbb{Z}/3\mathbb{Z}$ is cyclic, any homomorphism $\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ is uniquely determined by $\phi(1)$. Indeed, if we know $\phi(1)$, then $\phi(n) = n\phi(1)$. Since $\phi(1)$ can have three possible values, we divide into three cases. If $\phi_1(1) = 0$, then $\phi_1$ sends every element of $\mathbb{Z}/3\mathbb{Z}$ to zero. Thus, $\phi_1$ is not surjective, so $\phi_1 \notin \mathrm{Aut}(G)$. If $\phi_2(1) = 1$, then $\phi_2(n) = n$, i.e., $\phi_2 = \iota$. Thus, take $\psi(\phi_2) = 0$. It follows that $\phi_3$ defined by

$$1 \mapsto 2 \qquad\qquad 2 \mapsto 1 \qquad\qquad 0 \mapsto 0$$

must be sent by $\psi$ to $1 \in \mathbb{Z}/2\mathbb{Z}$.

Verifying that $\psi$ is an isomorphism: We have mapped the two distinct elements of $\mathrm{Aut}(G)$ to the two distinct elements of $\mathbb{Z}/2\mathbb{Z}$. Therefore, $\psi$ is injective and surjective. Moreover, $\psi$ is a homomorphism since

$$\begin{aligned}
\psi(\phi_2 \circ \phi_2) = \psi(\phi_2) = 0 = 0 + 0 = \psi(\phi_2) + \psi(\phi_2) \\
\psi(\phi_2 \circ \phi_3) = \psi(\phi_3) = 1 = 0 + 1 = \psi(\phi_2) + \psi(\phi_3) \\
\psi(\phi_3 \circ \phi_2) = \psi(\phi_3) = 1 = 1 + 0 = \psi(\phi_3) + \psi(\phi_2) \\
\psi(\phi_3 \circ \phi_3) = \psi(\phi_2) = 0 = 1 + 1 = \psi(\phi_3) + \psi(\phi_3)
\end{aligned}$$

□

ii. $\mathrm{Out}(S_3) = \{1\}$;

*Proof.* $S_3$ is not abelian. In fact, it contains no nontrivial elements which commute: We know that disjoint cycles commute, but in $S_3$, any nontrivial cycle is of length at least 2 and thus must share an element with another cycle of length at least 2. Thus $Z(S_3) = \{e\}$. It follows by part (f) that $\psi : S_3 \to \mathrm{Aut}(S_3)$ is an isomorphism. Thus, $\mathrm{Inn}(G) = \mathrm{Aut}(G)$. It follows that $\mathrm{Out}(G) = \{1\}$, as desired. □

iii. $\mathrm{Aut}(K) \cong \mathrm{Out}(K) \cong S_3$, where $K = (\mathbb{Z}/2\mathbb{Z})^2$ is the Klein 4-group.

*Proof.* $K$ is abelian; hence, by part (h), $\text{Aut}(K) \cong \text{Out}(K)$.
$K = \langle (0,1), (1,0) \rangle$; hence, any $\phi \in \text{Aut}(K)$ is uniquely defined by its action on $(0,1)$ and $(1,0)$. In particular, since $\phi$ is a homomorphism, we know $\phi(0,0) = (0,0)$. Additionally, whichever element of $\{(0,1),(1,0),(1,1)\}$ is not in $\phi(\{(0,1),(1,0)\})$ is the element to which $\phi$ maps $(1,1)$. Thus, we can define an isomorphism from $\psi : \text{Aut}(G) \to S_3$ as follows. Let $f : K \setminus \{(0,0)\} \to [3]$ be defined by

$$(0,1) \mapsto 1 \qquad (1,0) \mapsto 2 \qquad (1,1) \mapsto 3$$

Then define $\psi$ by

$$\psi(\phi) = f \circ \phi \circ f^{-1}$$

It follows by an analogous argument to that used in part (d) that $\psi$ is an isomorphism. □

9. Let $p$ be an odd prime number. Prove that there are no surjective homomorphisms from $S_n$ to $\mathbb{Z}/p\mathbb{Z}$ for any prime $p$. (Hint: Consider the image of the two-cycles).

*Proof.* Let $\phi : S_n \to \mathbb{Z}/p\mathbb{Z}$ be an arbitrary homomorphism. Let $(a,b) \in S_n$ be an arbitrary 2-cycle. By Lagrange's theorem, $|\phi(a,b)|$ divides $|\mathbb{Z}/p\mathbb{Z}|$, i.e, $|\phi(a,b)| \in \{1,p\}$. Additionally, we have that

$$2\phi(a,b) = \phi[(a,b) \circ (a,b)] = \phi(e) = 0$$

i.e., $|\phi(a,b)| \leq 2$. Thus, $|\phi(a,b)| = 1$. It follows that $\phi(a,b) = 0$ for all $(a,b) \in S_n$. But since a homomorphism is uniquely defined by its action on the generators and the 2-cycles generate $S_n$, this means that $\phi$ is the trivial homomorphism. Therefore, since all homomorphisms from $S_n$ to $\mathbb{Z}/p\mathbb{Z}$ are equal to the trivial one (which is not surjective), we know that there are no surjective homomorphisms from $S_n$ to $\mathbb{Z}/p\mathbb{Z}$, as desired. □